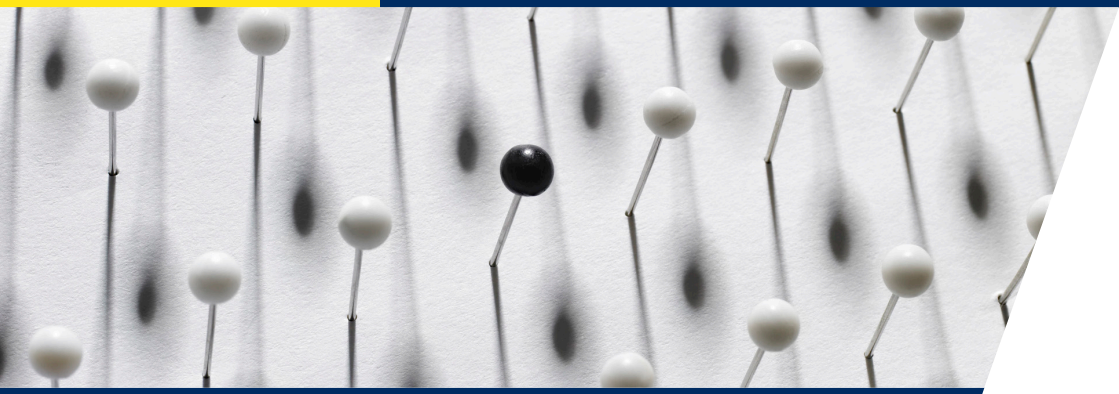
دليـل



# دليـــل قانـــون حمايـــة البيانـــات الأوروبـــي

نسخـــــة 2018

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS
EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
EDPS
EUROPEAN DATA PROTECTION SUPERVISOR

استكمل نص هذا الدليل في أبريل 2018.

ستصبح التحديثات متاحة مستقبلاً على موقع وكالة الاتحاد الأوروبي للحقوق الأساسية على عنوان fra.europa.eu، وموقع مجلس أوروبا الإلكتروني coe.int/dataprotection، وموقع المحكمة الأوروبية لحقوق الإنسان ضمن قائمة السوابق القضائية على عنوان echr.coe.int، وعلى موقع المشرف الأوروبي على حماية البيانات على عنوان edps.europa.eu.

مصدر الصور (الغلاف والداخل): ©iStock.com/jonathansloane.



إن المزيد من المعلومات المتعلقة بالاتحاد الأوروبي متاحة على الإنترنت (http://europa.eu).

تمت ترجمة هذه الوثيقة من اللغة الإنجليزية («Handbook on European data protection law - 2018 edition») من قبل مجلس أوروبا. وكالة الإتحاد الأوروبي للحقوق الأساسية لا تتحمل مسؤولية هذه الترجمة.

تمت صياغة هذا الدليل باللغة الإنجليزية. لا يتحمل مجلس أوروبا والمحكمة الأوروبية لحقوق الإنسان أي مسؤولية عن جودة الترجمات إلى اللغات الأخرى. إن الآراء الواردة في هذا الدليل غير ملزمة لمجلس أوروبا والمحكمة الأوروبية لحقوق الإنسان. يشير الدليل إلى مجموعة مختارة من التعليقات والدلائل، ولا يتحمل مجلس أوروبا والمحكمة الأوروبية لحقوق الإنسان أي مسؤولية عن محتواها، كما لا يمثل إدراجها ضمن هذه القائمة شكلاً من أشكال تأييد هذه المنشورات. هناك المزيد من الإصدارات المعروضة على صفحات الإنترنت الخاصة بمكتبة المحكمة الأوروبية لحقوق الإنسان على عنوان echr.coe.int.

لا يعبر محتوى هذا الدليل عن الموقف الرسمي للمشرف الأوروبي على حماية البيانات ولا يُلزمه في إطار ممارسة اختصاصاته. ولا يتحمل المشرف الأوروبي على حماية البيانات أي مسؤولية عن جودة الترجمات إلى لغات أخرى غير الإنجليزية.

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS
EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
EDPS
European Data Protection Supervisor

# دليل قانون حماية البيانات الأوروبي

# تمهيـــد

أصبحت مجتمعاتنا مجتمعات رقمية بامتياز، حيث تؤثر وتيرة التطورات التكنولوجية وكيفية معالجة البيانات الشخصية على كل واحد منا كل يوم وبشتى الطرق في ضوء هذه التغييرات. لذلك، تمت مؤخراً مراجعة الأطر القانونية الصادرة عن الاتحاد الأوروبي ومجلس أوروبا التي تضمن حماية الخصوصية والبيانات الشخصية.

هذا وتتزعم أوروبا جهود حماية البيانات حول العالم. وتستند معايير حماية البيانات في الاتحاد الأوروبي إلى الاتفاقية 108 التابعة لمجلس أوروبا، وصكوك الاتحاد الأوروبي - بما فيها اللائحة العامة لحماية البيانات والأمر التوجيهي الخاص بحماية البيانات الموجه للشرطة وسلطات العدالة الجنائية - وكذلك السوابق القضائية ذات الصلة للمحكمة الأوروبية لحقوق الإنسان ومحكمة العدل التابعة للاتحاد الأوروبي.

إن الإصلاحات الخاصة بحماية البيانات التي نفذها الاتحاد الأوروبي ومجلس أوروبا شاملة ومعقدة في بعض الأحيان، ولها فوائد وآثار واسعة النطاق على الأفراد والشركات. ويهدف هذا الدليل إلى زيادة الوعي وتحسين المعرفة بقواعد حماية البيانات، خاصة بين صفوف الممارسين القانونيين غير المتخصصين الذين يتعين عليهم التعامل مع مسائل حماية البيانات في إطار عملهم.

تم إعداد الدليل من قبل وكالة الاتحاد الأوروبي للحقوق الأساسية، بالتعاون مع مجلس أوروبا (الذي تعاون بدوره مع سجل المحكمة الأوروبية لحقوق الإنسان) والمشرف الأوروبي على حماية البيانات. يقوم هذا الدليل بتحديث نسخة 2014، وهو جزء من سلسلة من الدلائل القانونية التي شاركت في إنتاجها وكالة الاتحاد الأوروبي للحقوق الأساسية ومجلس أوروبا.

نعرب عن شكرنا لهيئات حماية البيانات في بلجيكا وإستونيا وفرنسا وجورجيا والمجر وأيرلندا وإيطاليا وموناكو وسويسرا والمملكة المتحدة على ملاحظاتهم المفيدة بخصوص مسودة الدليل. إضافة إلى ذلك، نعرب عن تقديرنا لوحدة حماية البيانات ووحدة تدفقات وحماية البيانات الدولية التابعتين للمفوضية الأوروبية. كما نشكر محكمة العدل التابعة للاتحاد الأوروبي على الدعم الوثائقي الذي قدمته خلال الأعمال التحضيرية لهذا الدليل.

كريستوس جياكوموبولوس

المدير العام لحقوق الإنسان وسيادة القانون في مجلس أوروبا

جيوفاني بوتاريلي

المشرف الأوروبي على حماية البيانات

مايكل أو فلاهرتي

مدير وكالة الاتحاد الأوروبي للحقوق الأساسية

# الفهرس

# مسرد

| | |
|---|---|
| Binding corporate rule (BCR) | قواعد الشركات الملزمة |
| Closed circuit television (CCTV) | كاميرات المراقبة |
| Council of Europe Treaty Series (CETS) | سلسلة معاهدات مجلس أوروبا |
| Charter of Fundamental Rights of the European Union | ميثاق الحقوق الأساسية للاتحاد الأوروبي |
| Customs information system (CIS) | نظام المعلومات الجمركي |
| Court of Justice of the European Union (CJEU) (prior to December 2009, European Court of Justice, ECJ) | محكمة العدل للاتحاد الأوروبي (المعروفة إلى حدود ديسمبر 2009 باسم محكمة العدل الأوروبية) |
| Council of Europe (CoE) | مجلس أوروبا |
| Convention 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe).<br>The amending Protocol (CETS No. 223) to Convention 108 ("Modernised Convention 108") was adopted by the Committee of Ministers of the Council of Europe on the occasion of its 128th session held in Elsinore, Denmark (17-18 May 2018). References to the "Modernised Convention 108" refer to the Convention as amended by Protocol CETS No. 223. | الاتفاقية 108: اتفاقية لحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية (مجلس أوروبا).<br>تم اعتماد البروتوكول المعدّل (سلسلة معاهدات مجلس أوروبا رقم 223) للاتفاقية 108 (الاتفاقية 108 المحدثة) من قبل لجنة الوزراء التابعة لمجلس أوروبا بمناسبة دورتها 128 المنعقدة في هيلسينجور بالدانمارك (17 18- مايو 2018). الاشارة الى «الاتفاقية 108 المحدثة» يقصد بها الاتفاقية كما تم تعديلها بموجب بروتوكول سلسلة معاهدات مجلس أوروبا رقم 223. |
| Customer relations management (CRM) | إدارة علاقات العملاء |
| Central Schengen Information System (C-SIS) | نظام معلومات شنغن المركزي |
| Data Protection Officer (DPO) | المسؤول عن حماية البيانات |
| Data Protection Authority (DPA) | هيئة حماية البيانات |
| European Arrest Warrant )EAW) | مذكرة التوقيف الأوروبية |
| European Data Protection Board (EDPB) | المجلس الأوروبي لحماية البيانات |
| European Community (EC) | الجماعة الأوروبية |
| European Convention on Human Rights (ECHR) | الاتفاقية الأوروبية لحقوق الإنسان |
| European Court of Human Rights (ECtHR) | المحكمة الأوروبية لحقوق الإنسان |
| European Data Protection Supervisor (EDPS) | المشرف الأوروبي على حماية البيانات |
| European Economic Area (EEA) | المنطقة الاقتصادية الأوروبية |
| European Food and Safety Authority (EFSA) | الهيئة الأوروبية لسلامة الأغذية |
| European Free Trade Association (EFTA) | رابطة التجارة الحرة الأوروبية |
| European Network and Information Security Agency (ENISA) | الوكالة الأوروبية لأمن الشبكات والمعلومات |
| Europol National Unit (ENU( | وحدة اليوروبول الوطنية |
| European Prosecutor's Office (EPPO) | مكتب المدعي العام الأوروبي |

| | |
|---|---|
| European Securities and Markets Authority (ESMA) | الهيئة الأوروبية للأوراق المالية والأسواق |
| Trans-European Telecommunication Networks (eTEN) | شبكات الاتصالات العابرة لأوروبا |
| European Union (EU) | الاتحاد الأوروبي |
| European Privacy Seal (EuroPriSe) | ختم الخصوصية الأوروبي |
| EU Agency for Large-scale IT Systems (eu-LISA) | وكالة الاتحاد الأوروبي الخاصة بالأنظمة المعلوماتية واسعة النطاق |
| European Union Agency for Fundamental Rights (FRA) | وكالة الاتحاد الأوروبي للحقوق الأساسية |
| General Data Protection Regulation (GDPR) | اللائحة العامة لحماية البيانات |
| Global positioning system )GPS( | نظام تحديد المواقع العالمي |
| International Covenant on Civil and Political Rights (ICCPR) | العهد الدولي الخاص بالحقوق المدنية والسياسية |
| Information and communications technology (ICT) | تكنولوجيا المعلومات والاتصالات |
| Internet service provider (ISP) | مقدم خدمة الإنترنت |
| Joint Supervisory Body (JSB) | الهيئة الإشرافية المشتركة |
| Non-governmental organisation (NGO) | منظمة غير حكومية |
| National Schengen Information System (N-SIS) | نظام معلومات شنغن الوطني |
| Organisation for Economic Co-operation and Development (OECD) | منظمة التعاون الاقتصادي والتنمية |
| Official Journal (OJ) | الجريدة الرسمية |
| Personal identification number (PIN) | رقم التعريف الشخصي |
| Passenger name record (PNR) | سجل اسم المسافر |
| Supervision Coordination Group (SCG) | مجموعة تنسيق الإشراف |
| Single Euro Payments Area (SEPA) | منطقة المدفوعات الأوروبية الموحدة |
| Schengen Information System (SIS) | نظام معلومات شنغن |
| Society for Worldwide Interbank Financial Telecommunication (SWIFT) | جمعية الاتصالات المالية العالمية بين البنوك |
| Treaty on European Union (TEU) | معاهدة الاتحاد الأوروبي |
| Treaty on the Functioning of the European Union (TFEU) | المعاهدة المنظمة لعمل الاتحاد الأوروبي |
| Universal Declaration of Human Rights (UDHR) | الإعلان العالمي لحقوق الإنسان |
| United Nations (UN) | الأمم المتحدة |
| Visa Information System (VIS) | نظام معلومات التأشيرة |

# كيفية استخدام هذا الدليل

يحدد هذا الدليل المعايير القانونية المتعلقة بحماية البيانات التي وضعها الاتحاد الأوروبي ومجلس أوروبا، وهو مصمم لمساعدة الممارسين غير المتخصصين في مجال حماية البيانات، بمن فيهم المحامون والقضاة وغيرهم من مهنيي القانون، إلى جانب الأشخاص العاملين في هيئات أخرى، مثل المنظمات غير الحكومية، والذين قد تصادفهم مسائل قانونية تتعلق بحماية البيانات.

يعتبر هذا الدليل بمثابة مرجع أولي فيما يهم أحكام قانون الاتحاد الأوروبي ذات الصلة والاتفاقية الأوروبية لحقوق الإنسان، فضلاً عن اتفاقية مجلس أوروبا لحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية (الاتفاقية 108) وغيرها من صكوك مجلس أوروبا.

يبدأ كل فصل بجدول يحدد المقتضيات القانونية ذات الصلة بالموضوعات التي يتم التطرق إليها في ذاك الفصل. وتشمل هذه الجداول كلاً من قانون مجلس أوروبا وقانون الاتحاد الأوروبي، وتتضمن سوابق قضائية مختارة من فقه المحكمة الأوروبية لحقوق الإنسان ومحكمة العدل للاتحاد الأوروبي. بعدها يتم استعراض القوانين ذات الصلة ضمن هاتين المنظومتين الأوروبيتين المختلفتين، حسب درجة انطباقها على الموضوعات المحددة التي يتم تناولها، وذلك بشكل تسلسلي. يتيح ذلك للقارئ معرفة أوجه التقارب والاختلاف بين النظامين القانونيين المذكورين، كما من شأنه أن يساعد القراء على العثور بسرعة على المعلومات الأساسية المتعلقة بوضعيتهم ، خاصة إذا كانوا يخضعون لقانون مجلس أوروبا فقط. يُذكر أنه في بعض الفصول قد يختلف ترتيب الموضوعات الواردة في الجداول قليلاً عن الترتيب المتبع في الفصل ذاته، إذا كان ذالك يساعد على الإيجاز في عرض المحتوى. كما يقدم الدليل لمحة عامة موجزة عن إطار عمل منظمة الأمم المتحدة.

يمكن للممارسين في الدول غير الأعضاء في الاتحاد الأوروبي التي هي دول أعضاء في مجلس أوروبا وأطراف في الاتفاقية الأوروبية لحقوق الإنسان والاتفاقية 108 الوصول إلى المعلومات ذات الصلة ببلدهم من خلال الانتقال مباشرة إلى الأجزاء المتعلقة بمجلس أوروبا. كما يجب على الممارسين في الدول غير الأعضاء في الاتحاد الأوروبي أن يأخذوا في الحسبان أنه منذ اعتماد اللائحة العامة لحماية البيانات في الاتحاد الأوروبي، باتت قواعد حماية البيانات في الاتحاد الأوروبي تنطبق على المنظمات والهيئات الأخرى غير المنشأة في الاتحاد الأوروبي، إذا كانت تقوم بمعالجة البيانات الشخصية وتقديم السلع والخدمات لأصحاب البيانات داخل الاتحاد أو تقوم بمراقبة سلوك أصحاب البيانات.

وسيتعين على الممارسين في الدول الأعضاء في الاتحاد الأوروبي الاطلاع على كلا الجزأين، لأن هذه الدول ملزمة بكلا النظامين القانونيين. وتجدر الإشارة إلى أن إصلاحات وتحديث قواعد حماية البيانات في أوروبا، والتي تم تبنيها ضمن إطار مجلس أوروبا (الاتفاقية 108 المحدثة بصيغتها المعدلة بموجب بروتوكول سلسلة معاهدات مجلس أوروبا رقم 223) والاتحاد الأوروبي (اعتماد اللائحة العامة لحماية البيانات والأمر التوجيهي (رقم EU/2016/680)، قد تم تنفيذها بصورة متوازية. وقد أولت الجهات المنظمة في كلا النظامين القانونيين أقصى درجات الحرص لضمان الاتساق والتوافق بين الإطارين القانونيين. وبالتالي، أدت الإصلاحات إلى زيادة التنسيق بين قانون حماية البيانات في الاتحاد الأوروبي ونظيره لدى مجلس أوروبا. وبالنسبة للأشخاص الذين يحتاجون إلى مزيد من المعلومات حول قضية معينة، يمكن العثور على قائمة بمواد أكثر تخصصاً في جزء «مراجع إضافية». وللحصول على معلومات بشأن مقتضيات الاتفاقية 108 وبروتوكولها الإضافي لعام 2001، والتي لا تزال سارية حتى دخول البروتوكول المعدل حيز التنفيذ، ينبغي للقراء الرجوع إلى نسخة 2014 من الدليل.

يتم تقديم قانون مجلس أوروبا من خلال إشارات مرجعية قصيرة لمجموعة مختارة من قضايا المحكمة الأوروبية لحقوق الإنسان، والتي تم انتقاؤها من بين عدد كبير من الأحكام والقرارات الموجودة بشأن قضايا حماية البيانات الصادرة عن هذه المحكمة.

من جهته، يشتمل قانون الاتحاد الأوروبي ذي الصلة على التدابير التشريعية التي تم اعتمادها، والمقتضيات ذات الصلة من المعاهدات وميثاق الحقوق الأساسية للاتحاد الأوروبي، كما هي مفسرة في السوابق القضائية لمحكمة العدل للاتحاد الأوروبي. إضافة إلى ذلك، يعرض الدليل الآراء والمبادئ التوجيهية التي اعتمدها فريق عمل المادة 29، وهو الهيئة الاستشارية المكلفة بموجب الأمر التوجيهي الخاص بحماية البيانات بتقديم مشورة الخبراء للدول الأعضاء في الاتحاد الأوروبي، والتي سيحل محلها المجلس الأوروبي لحماية البيانات بدءاً من 25 مايو 2018. كما توفر آراء المشرف الأوروبي على حماية البيانات إضاءات مهمة حول تفسير قانون الاتحاد الأوروبي، وبالتالي تم إدراجها في هذا الدليل.

تقدم الحالات التي يتم وصفها أو ذكرها في هذا الدليل أمثلة على مجموعة مهمة من السوابق القضائية للمحكمة الأوروبية لحقوق الإنسان ومحكمة العدل التابعة للاتحاد الأوروبي. وتهدف الإرشادات الموجودة في نهاية الدليل إلى مساعدة القراء في البحث عن السوابق القضائية عبر الإنترنت. إن السوابق القضائية الخاصة بمحكمة العدل التي تم عرضها تتعلق بالأمر التوجيهي السابق الخاص بحماية البيانات. ومع ذلك، تظل تفسيرات محكمة العدل التابعة للاتحاد الأوروبي قابلة للتطبيق على الحقوق والالتزامات المقابلة المنصوص عليها في اللائحة العامة لحماية البيانات.

علاوة على ذلك، يتم تقديم أمثلة توضيحية عملية مع سيناريوهات افتراضية في خانات النصوص ذات الخلفية الزرقاء. توضح هذه الأخيرة بشكل أكبر تطبيق قواعد حماية البيانات الأوروبية في الممارسة العملية، لا سيما في حال عدم وجود سوابق قضائية ذات صلة للمحكمة الأوروبية لحقوق الإنسان أو لمحكمة العدل التابعة للاتحاد الأوروبي. وتقدم خانات نصوص أخرى - ذات خلفية رمادية - أمثلة مأخوذة من مصادر أخرى غير السوابق القضائية للمحكمة الأوروبية لحقوق الإنسان ومحكمة العدل التابعة للاتحاد الأوروبي، مثل التشريعات والآراء الصادرة عن فريق عمل المادة 29.

يبدأ الدليل بوصف موجز لدور النظامين القانونيين على النحو المنصوص عليه في الاتفاقية الأوروبية لحقوق الإنسان وقانون الاتحاد الأوروبي (الفصل 1). تتطرق الفصول من 2 إلى 10 المسائل التالية:

- مصطلحات حماية البيانات؛
- المبادئ الأساسية لقانون حماية البيانات الأوروبي؛
- قواعد قانون حماية البيانات الأوروبي؛
- الإشراف المستقل؛
- حقوق أصحاب البيانات وإنفاذها؛
- عمليات نقل وتدفق البيانات الشخصية عبر الحدود؛
- حماية البيانات في سياق الشرطة والعدالة الجنائية؛
- قواعد أخرى لحماية البيانات الأوروبية في مجالات محددة؛
- التحديات الحديثة في مجال حماية البيانات الشخصية.

# 1 سيـــاق قانـــون حمايـــة البيانـــات الأوروبـــي وخلفياتـــه

| الاتحاد الأوروبي | المسائل المتناولة | مجلس أوروبا |
|---|---|---|
| **الحق في حماية البيانات** | | |
| المعاهدة المنظِّمة لعمل الاتحاد الأوروبي، المادة 16<br>ميثاق الحقوق الأساسية للاتحاد الأوروبي (الميثاق)، المادة 8 (الحق في حماية البيانات الشخصية) | | الاتفاقية الأوروبية لحقوق الإنسان، المادة 8 (الحق في احترام الحياة الخاصة وحرمة العائلة والمسكن والمراسلات) |
| الأمر التوجيهي رقم EC/95/46 الخاص بحماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية و حرية حركة هذه البيانات (الأمر التوجيهي الخاص بحماية البيانات)، 281 L 1995 OJ (ساري المفعول حتى مايو 2018)<br>القرار الإطار JHA/2008/977 الصادر عن المجلس بشأن حماية البيانات الشخصية المعالجة في إطار التعاون الشرطي و القضائي في المسائل الجنائية،350 L 2008 OJ (ساري المفعول حتى مايو 2018)<br>اللائحة (الاتحاد الأوروبي) رقم 679/2016 بشأن حماية الأشخاص الذاتيين فيما يتعلق بمعالجة البيانات الشخصية والحركة الحرة لهذه البيانات، وإلغاء الأمر التوجيهي رقم EC/95/46 (اللائحة العامة لحماية البيانات)، 119 L 2016 OJ<br>الأمر التوجيهي (الاتحاد الأوروبي) رقم 2016/680 بشأن حماية الأشخاص الذاتيين فيما يتعلق بمعالجة البيانات الشخصية من قبل الهيئات المختصة لأغراض منع الجرائم الجنائية أو التحقيق فيها أو الكشف عنها أو متابعة مرتكبيها أو تنفيذ العقوبات الجنائية في حقهم، وبشأن حرية حركة هذه البيانات، وإلغاء القرار الإطار JHA/2008/977 الصادر عن المجلس (حماية البيانات بالنسبة للشرطة والسلطات القضائية)، 119 L 2016 OJ | | الاتفاقية المحدثة لحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية (الاتفاقية 108 المحدثة) |

| | | |
|---|---|---|
| الأمر التوجيهي رقم EC/2002/58 بشأن معالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الإلكترونية (الأمر التوجيهي الخاص بالخصوصية والاتصالات الإلكترونية)، OJ L 201 2002<br>اللائحة (الجماعة الأوروبية) رقم 45/2001 بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية من قبل المؤسسات والهيئات الأوروبية وبشأن حرية حركة هذه البيانات (لائحة حماية بيانات مؤسسات الاتحاد الأوروبي)، OJ L 8 2001 | | |
| **القيود المفروضة على الحق في حماية البيانات الشخصية** | | |
| الميثاق، المادة 52 (1)<br>اللائحة العامة لحماية البيانات، المادة 23<br>محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-92/09 وC-93/09، شركة «فولكر وماركوس تشيكه» وهارتموت أيفرت ضد ولاية هيسن [الغرفة الكبرى]، 2010 | | الاتفاقية الأوروبية لحقوق الإنسان، المادة 8 (2)<br>الاتفاقية 108 المحدثة، المادة 11<br>المحكمة الأوروبية لحقوق الإنسان، «س. ومارير ضد المملكة المتحدة» [الغرفة الكبرى]، رقم 30562/04 ورقم 30566/04، 2008 |
| **الموازنة بين الحقوق** | | |
| محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-92/09 وC-93/09، شركة «فولكر وماركوس تشيكه» وهارتموت أيفرت ضد ولاية هيسن [الغرفة الكبرى]، 2010 | بشكل عام | |
| محكمة العدل التابعة للاتحاد الأوروبي، C-73/07، قضية «المفوض الفنلندي المعني بحماية البيانات ضدSatakunnan Markkinapörssi Oy وSatamedia Oy» [الغرفة الكبرى]، 2008<br>محكمة العدل التابعة للاتحاد الأوروبي، C-131/12، قضية «غوغل إسبانيا وشركة غوغل ضد الوكالة الإسبانية لحماية البيانات وماريو كوستيخا غونزاليس» [الغرفة الكبرى]، 2014 | حرية التعبير | المحكمة الأوروبية لحقوق الإنسان، قضية «أكسيل سبرينغر' ضد ألمانيا» [الغرفة الكبرى]، رقم 39954/08، 2012<br>المحكمة الأوروبية لحقوق الإنسان، قضية «موزلي ضد المملكة المتحدة»، رقم 48009/08، 2011<br>المحكمة الأوروبية لحقوق الإنسان، قضية «بوهلين ضد ألمانيا»، رقم 53495/09، 2015 |
| محكمة العدل التابعة للاتحاد الأوروبي، C-28/08 P، قضية «المفوضية الأوروبية ضد شركة 'بافاريان لاغر' المحدودة»، 2010<br>محكمة العدل التابعة للاتحاد الأوروبي، C-615/13P، قضية «ClientEarth و PAN Europeضد الهيئة الأوروبية لسلامة الأغذية»، 2015 | الوصول إلى الوثائق | المحكمة الأوروبية لحقوق الإنسان، قضية «لجنة هيلسنكي المجرية ضد المجر» [الغرفة الكبرى]، رقم 18030/11، 2016 |
| اللائحة العامة لحماية البيانات، المادة 90 | السرية المهنية | المحكمة الأوروبية لحقوق الإنسان، قضية «بروتيانو ضد رومانيا»، رقم 30181/05، 2015 |

| | | |
|---|---|---|
| اللائحة العامة لحماية البيانات، المادة 91 | حرية الديانة والمعتقد | |
| | حرية الفنون والعلوم | لمحكمة الأوروبية لحقوق الإنسان، قضية «نقابة الفنانين التشكيليين النمساويين ضد النمسا»، رقم 68354/01، 2007 |
| محكمة العدل التابعة للاتحاد الأوروبي، C-275/06، قضية «منظمة 'منتجو الموسيقى في إسبانيا' ضد شركة 'تيليفونيكا دي إسبانيا'» [الغرفة الكبرى]، 2008 | حماية الملكية | |
| محكمة العدل التابعة للاتحاد الأوروبي، C-131/12، قضية «غوغل إسبانيا وشركة غوغل ضد الوكالة الإسبانية لحماية البيانات وماريو كوستيخا غونزاليس» [الغرفة الكبرى]، 2014<br>محكمة العدل التابعة للاتحاد الأوروبي، C-398/15، قضية «غرفة التجارة والصناعة والحرف اليدوية والزراعة في ليتشي ضد سالفاتوري ماني»، 2017 | الحقوق الاقتصادية | |

# 1.1. الحق في حماية البيانات الشخصية

## النقـــاط الرئيسيـــة

- وفقاً للمادة 8 من الاتفاقية الأوروبية لحقوق الإنسان، يعتبر حق الشخص في الحماية فيما يتعلق بمعالجة البيانات الشخصية جزءاً من الحق في احترام الحياة الخاصة وحرمة العائلة والمسكن والمراسلات.
- إن الاتفاقية 108 التابعة لمجلس أوروبا هي أول صك دولي ملزم قانوناً يتناول حماية البيانات، وهي الوحيدة من نوعها حتى الآن. وقد خضعت الاتفاقية لعملية تحديث اكتملت باعتماد بروتوكول سلسلة معاهدات مجلس أوروبا رقم 223 المعدّل.
- بموجب قانون الاتحاد الأوروبي، تم الاعتراف بحماية البيانات كحق أساسي متميز. وتم التأكيد عليه في المادة 16 من المعاهدة المنظمة لعمل الاتحاد الأوروبي، وكذلك في المادة 8 من ميثاق الحقوق الأساسية للاتحاد الأوروبي.
- بموجب قانون الاتحاد الأوروبي، تم تنظيم حماية البيانات لأول مرة بواسطة الأمر التوجيهي الخاص بحماية البيانات في عام 1995.
- في ضوء التطورات التكنولوجية المتسارعة، اعتمد الاتحاد الأوروبي تشريعات جديدة في سنة 2016 لتكييف قواعد حماية البيانات مع العصر الرقمي. وقد دخلت اللائحة العامة لحماية البيانات حيز التنفيذ في مايو 2018، ملغية بذلك الأمر التوجيهي الخاص بحماية البيانات.
- إلى جانب اللائحة العامة لحماية البيانات، اعتمد الاتحاد الأوروبي تشريعا بشأن معالجة البيانات الشخصية من قبل الهيئات الوطنية لأغراض إنفاذ القانون. ويحدد الأمر التوجيهي (الاتحاد الأوروبي) رقم 2016/680 قواعد ومبادئ حماية البيانات التي تحكم معالجة البيانات الشخصية لأغراض منع الجرائم الجنائية أو التحقيق فيها أو الكشف عنها أو متابعة مرتكبيها أو تنفيذ عقوبات جنائية في حقهم.

## 1.1.1. الحق في احترام الحياة الخاصة والحق في حماية البيانات الشخصية: مقدمة موجزة

إن الحق في احترام الحياة الخاصة والحق في حماية البيانات الشخصية حقان مختلفان، على الرغم من ارتباطهما الوثيق. فقد ظهر الحق في الخصوصية - المشار إليه في القانون الأوروبي على أنه الحق في احترام الحياة الخاصة - في القانون الدولي لحقوق الإنسان ضمن الإعلان العالمي لحقوق الإنسان، الذي تم تبنيه في عام 1948، باعتباره أحد حقوق الإنسان الأساسية المحمية. وبعد فترة وجيزة من اعتماد الإعلان العالمي لحقوق الإنسان، أكدت أوروبا بدورها على هذا الحق في الاتفاقية الأوروبية لحقوق الإنسان، وهي معاهدة ملزمة قانوناً لأطرافها المتعاقدة، تمت صياغتها في عام 1950. وتنص الاتفاقية الأوروبية لحقوق الإنسان على أن لكل شخص الحق في احترام حياته الخاصة والعائلية ومسكنه ومراسلاته. هذا ويَحظر تدخل السلطة العامة في هذا الحق، إلا في الحالات التي يكون فيها التدخل وفقاً للقانون، ويهدف إلى تحقيق مصالح عامة مهمة ومشروعة، ويكون ضرورياً في مجتمع ديمقراطي.

تم اعتماد الإعلان العالمي لحقوق الإنسان والاتفاقية الأوروبية لحقوق الإنسان قبل فترة طويلة من تطور أجهزة الكمبيوتر والإنترنت وبروز مجتمع المعلومات. وقد جلبت هذه التطورات منافع كبيرة للأفراد والمجتمع، كما ساهمت في تحسين جودة الحياة والكفاءة والإنتاجية. وفي الوقت نفسه، تولدت عن هذه التطورات مخاطر جديدة تهدد الحق في احترام الحياة الخاصة. واستجابة للحاجة إلى قواعد محددة تحكم جمع المعلومات الشخصية واستخدامها، ظهر مفهوم جديد للخصوصية، يُعرف في بعض الولايات القضائية باسم «الخصوصية المعلوماتية»، وفي ولايات قضائية أخرى باسم «الحق في تقرير المصير المعلوماتي».[1] وقد أدى هذا المفهوم إلى إحداث لوائح قانونية خاصة توفر الحماية للبيانات الشخصية.

[1] أكدت المحكمة الدستورية الاتحادية الألمانية على الحق في تقرير المصير المعلوماتي في حكم صدر عام 1983 في قانون التعداد الألماني (Volkszählungsurteil, BVerfGE Bd. 65, S. 1ff). وقد اعتبرت المحكمة أن تقرير المصير المعلوماتي مستمد من الحق الأساسي في احترام الشخصية، المحمي في الدستور الألماني. وأقرت المحكمة الأوروبية لحقوق الإنسان في حكم صدر عام 2017 بأن المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان «تنص على الحق في شكل من أشكال تقرير المصير المعلوماتي». انظر المحكمة الأوروبية لحقوق الإنسان، قضية « Satakunnan Markkinapörssi Oy وSatamedia Oy ضد فنلندا»، رقم 931/13، 27 يونيو 2017، الفقرة 137.

وقد بدأت حماية البيانات في أوروبا في سبعينات القرن الماضي، مع اعتماد تشريعات - من قبل بعض الدول - لمراقبة معالجة المعلومات الشخصية التي تقوم بها السلطات العامة والشركات الكبرى.[2] بعد ذلك، تمت صياغة صكوك حماية البيانات على المستوى الأوروبي.[3] ومع مرور السنين، تطورت حماية البيانات لتصبح قيمة مميزة لا يشملها الحق في احترام الحياة الخاصة. ففي النظام القانوني للاتحاد الأوروبي، تعتبر حماية البيانات حقاً أساسياً منفصلاً عن الحق الأساسي في احترام الحياة الخاصة. هذا الفصل يثير تساؤلا حول العلاقة والاختلافات بين هذين الحقين.

ويرتبط الحق في احترام الحياة الخاصة ارتباطاً وثيقاً بالحق في حماية البيانات الشخصية. فكلاهما يسعى إلى حماية قيم متشابهة، أي الاستقلال الذاتي والكرامة الإنسانية للأفراد، من خلال منحهم مجالاً شخصياً يمكنهم من خلاله تطوير شخصياتهم والتفكير وتشكيل آرائهم بحرية. وبالتالي، فهما شرطان أساسيان مسبقان لممارسة الحريات الأساسية الأخرى، مثل حرية التعبير، وحرية التجمع السلمي وتكوين الجمعيات، وحرية الديانة.

ويختلف الحقان في صياغتهما ونطاقهما. إذ ينطوي الحق في احترام الحياة الخاصة على منع عام للتدخل، مع مراعاة بعض معايير المصلحة العامة التي يمكن أن تبرر التدخل في حالات معينة. من جهته، يُنظر إلى حماية البيانات الشخصية على أنه حق حديث ونشط،[4] حيث ينطوي على وضع نظام من الضوابط والتوازنات لحماية الأفراد عند معالجة بياناتهم الشخصية. هذا ويجب أن تمتثل المعالجة للمكونات الأساسية لحماية البيانات الشخصية، لا سيما الإشراف المستقل واحترام حقوق صاحب البيانات.[5]

لا تؤكد المادة 8 من ميثاق الحقوق الأساسية للاتحاد الأوروبي (الميثاق) على الحق في حماية البيانات الشخصية فحسب، بل توضح كذلك القيم الأساسية المرتبطة بهذا الحق. حيث تنص على أن معالجة البيانات الشخصية يجب أن تكون عادلة، ولأغراض محددة، ومستندة إلى موافقة الشخص المعني أو أساس شرعي ينص عليه القانون. ويجب أن يكون للأفراد الحق في الوصول إلى بياناتهم الشخصية وتصحيحها، كما يجب أن يخضع الامتثال لهذا الحق لمراقبة هيئة مستقلة.

يصبح الحق في حماية البيانات الشخصية ذا صلة عند أي معالجة للبيانات الشخصية. وبالتالي فهو أوسع من الحق في احترام الحياة الخاصة. هذا وتخضع أي عملية معالجة للبيانات الشخصية للحماية المناسبة. وتهم حماية البيانات جميع أنواع البيانات الشخصية ومعالجة البيانات، بغض النظر عن علاقتها بالخصوصية والأثر المترتب على هذه الأخيرة. كما قد تنتهك معالجة البيانات الشخصية الحق في الحياة الخاصة، كما هو موضح في الأمثلة أدناه. غير أنه ليس من الضروري إثبات وجود انتهاك للحياة الخاصة لتفعيل قواعد حماية البيانات.

ويهم الحق في الخصوصية الحالات التي يتم فيها المساس بمصلحة خاصة أو بـ»الحياة الخاصة» للفرد. وكما هو موضح في هذا الدليل، تم تقديم تفسير واسع لمفهوم «الحياة الخاصة» في السوابق القضائية، ويشمل المواقف الحميمية، والمعلومات الحساسة أو السرية، والمعلومات التي يمكن أن تلحق الضرر بنظرة الجمهور إلى الفرد، وحتى جوانب من الحياة المهنية للفرد وسلوكه العام. ومع ذلك، فإن تقييم ما إذا كان هناك تدخل في «الحياة الخاصة» يعتمد على سياق وحقائق كل حالة على حدة.

في مقابل ذلك، يمكن أن تندرج أي عملية تنطوي على معالجة البيانات الشخصية ضمن نطاق قواعد حماية البيانات، و تؤدي إلى تفعيل الحق في حماية البيانات الشخصية. وعلى سبيل المثال، عندما يسجل صاحب العمل المعلومات المتعلقة بأسماء الموظفين والرواتب المدفوعة لهم، فإن مجرد تسجيل هذه المعلومات لا يمكن اعتباره تدخلاً في الحياة الخاصة. في المقابل، إذا قام صاحب العمل، على سبيل المثال، بنقل المعلومات الشخصية للموظفين إلى أطراف ثالثة، فإن ذلك يمكن أن يعتبر تدخلاً في الحياة الخاصة. ويجب على أصحاب العمل في كل الأحوال الامتثال لقواعد حماية البيانات لأن تسجيل معلومات الموظفين هو بمثابة معالجة للبيانات.

---

[2] اعتمدت ولاية هيسن الألمانية أول قانون لحماية البيانات في عام 1970،والذي تم تطبيقه فقط في تلك الولاية. وفي عام 1973، اعتمدت السويد أول قانون وطني لحماية البيانات في العالم. وبنهاية الثمانينات، تبنت العديد من الدول الأوروبية (فرنسا وألمانيا وهولندا والمملكة المتحدة) أيضاً تشريعات تتعلق بحماية البيانات.

[3] تم اعتماد اتفاقية مجلس أوروبا لحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية (الاتفاقية 108) في عام 1981. واعتمد الاتحاد الأوروبي أول صك شامل لحماية البيانات في عام 1995: الأمر التوجيهي رقم EC/95/46 الخاص بحماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وحرية حركة هذه البيانات.

[4] وصف النائب العام شاربستون القضية بأنها تنطوي على حقين منفصلين: الحق «الكلاسيكي» في حماية الخصوصية، وحق «أكثر حداثة» هو الحق في حماية البيانات. انظر محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-92/09 وC-93/02، قضية «شركة Volker und Markus Schecke GbR ضد ولاية هيسن»، رأي النائب العام شاربستون، 17 يونيو 2010، الفقرة 71.

[5] هاستينيك ب.، خطابات ومقالات المشرف الأوروبي على حماية البيانات، قانون حماية البيانات في الاتحاد الأوروبي: مراجعة الأمر التوجيهي رقم EC/46/95 واللائحة العامة المقترحة لحماية البيانات، يوليو 2013.

مثال: في قضية «ديجيتال رايتس آيرلاند»،[6] كان على محكمة العدل التابعة للاتحاد الأوروبي اتخاذ قرار بشأن صلاحية الأمر التوجيهي رقم EC/2006/24 في ضوء الحقين الأساسيين المتمثلين في حماية البيانات الشخصية واحترام الحياة الخاصة، واللذين تم التأكيد عليهما في ميثاق الحقوق الأساسية للاتحاد الأوروبي. وقد فرض الأمر التوجيهي على مقدمي خدمات الاتصالات الإلكترونية المتاحة للجمهور أو شبكات الاتصالات العامة الاحتفاظ ببيانات اتصالات المواطنين لمدة تصل إلى سنتين، وذلك لضمان توفر البيانات لأغراض منع الجرائم الخطيرة والتحقيق فيها ومتابعة مرتكبيها. وقد كان هذا التدبير يتعلق فقط بالبيانات الوصفية وبيانات الموقع والبيانات اللازمة لتحديد هوية المشترك أو المستخدم، ولم يكن ينطبق على محتوى الاتصالات الإلكترونية.

اعتبرت محكمة العدل التابعة للاتحاد الأوروبي أن الأمر التوجيهي تدخل في الحق الأساسي المتمثل في حماية البيانات الشخصية» لأنه ينص على معالجة البيانات الشخصية».[7] إضافة إلى ذلك، خلصت المحكمة إلى أن الأمر التوجيهي يتدخل في الحق في احترام الحياة الخاصة.[8] فعند النظر إليها في مجملها ، يمكن للبيانات الشخصية المحتفظ بها وفقاً للأمر التوجيهي، والتي يمكن الوصول إليها من قبل الهيئات المختصة، أن تسمح بـ «استخلاص استنتاجات دقيقة للغاية فيما يتعلق بالحياة الخاصة للأشخاص الذين تم الاحتفاظ ببياناتهم، مثل عادات الحياة اليومية، وأماكن الإقامة الدائمة أو المؤقتة، والتحركات اليومية أو غيرها، والأنشطة التي يتم القيام بها، والعلاقات الاجتماعية لهؤلاء الأشخاص، والبيئات الاجتماعية التي يرتادونها بها».[9] إن التدخل في هذين الحقين كان واسع النطاق وخطيراً.

وقد قضت محكمة العدل التابعة للاتحاد الأوروبي بعدم صلاحية الأمر التوجيهي رقم EC/2006/24، وخلصت إلى أنه على الرغم من سعيه إلى تحقيق هدف مشروع فإن التدخل في الحق في حماية البيانات الشخصية والحق في الحياة الخاصة كان خطيراً ولم يقتصر على ما هو ضروري فقط.

## 2.1.1. الإطار القانوني الدولي: الأمم المتحدة

لا يعترف إطار عمل الأمم المتحدة بحماية البيانات الشخصية كحق أساسي، على الرغم من أن الحق في الخصوصية هو حق أساسي راسخ منذ زمن بعيد في النظام القانوني الدولي. فقد كانت المادة 12 من الإعلان العالمي لحقوق الإنسان والمتعلقة باحترام الحياة الخاصة **والعائلية**[10] هي المرة الأولى التي ينص فيها صك دولي على حق الفرد في حماية مجاله الخاص من تدخل الآخرين، وخاصة الدولة. وعلى الرغم من كونه غير ملزم، فإن الإعلان العالمي لحقوق الإنسان يتمتع بمكانة كبيرة باعتباره الصك التأسيسي للقانون الدولي لحقوق الإنسان، وقد أثر في صياغة باقي مواثيق حقوق الإنسان في أوروبا. من جهته، دخل العهد الدولي الخاص بالحقوق المدنية والسياسية حيز التنفيذ في عام 1976. وينص على أنه لا يجوز أن يتعرض أي شخص للتدخل التعسفي أو غير القانوني في خصوصيته أو مسكنه أو مراسلاته، أو لاعتداءات غير قانونية على شرفه وسمعته. إن العهد الدولي الخاص بالحقوق المدنية والسياسية هو معاهدة دولية تلزم أطرافها البالغ عددهم 169 باحترام وضمان ممارسة الحقوق المدنية للأفراد، بما في ذلك الخصوصية.

ومنذ عام 2013، اعتمدت الأمم المتحدة قرارين بشأن قضايا الخصوصية بعنوان «الحق في الخصوصية في العصر الرقمي»[11] استجابة لتطور التكنولوجيا الحديثة ولما تم كشفه بشأن تدابير المراقبة الجماعية التي تتخذ في بعض الدول (تسريبات سنودن). ويدين القراران بشدة المراقبة الجماعية ويسلطان الضوء على الأثر الذي يمكن أن تحدثه هذه المراقبة على الحقوق الأساسية في الخصوصية وحرية التعبير، وعلى سير مجتمع نشيط وديمقراطي. وعلى الرغم من كونهما غير ملزمين قانوناً، فقد أثار القراران نقاشاً سياسياً رفيع المستوى وبالغ الأهمية على المستوى الدولي حول الخصوصية والتكنولوجيا الحديثة والمراقبة. كما أديا إلى تعيين مقرر خاص معني بالحق في الخصوصية، مكلف

[6] محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-293/12 وC-594/12، قضية «شركة 'ديجيتال رايتس آيرلاند' المحدودة ضد وزير الاتصالات والموارد البحرية والطبيعية وآخرين» وضد حكومة كيرنتن وآخرين [الغرفة الكبرى]، 8 أبريل 2014.

[7] نفس المرجع السابق، الفقرة 36.

[8] نفس المرجع السابق، الفقرات 35-32.

[9] نفس المرجع السابق، الفقرة 27.

[10] الأمم المتحدة، الإعلان العالمي لحقوق الإنسان، 10 ديسمبر 1948.

[11] انظر الأمم المتحدة، الجمعية العامة، قرار بشأن الحق في الخصوصية في العصر الرقمي، A/RES/68/167، نيويورك، 18 ديسمبر 2013؛ الأمم المتحدة، الجمعية العامة، مشروع قرار منقح بشأن الحق في الخصوصية في العصر الرقمي، A/C.3/69/L.26/Rev.1، نيويورك، 19 نوفمبر 2014.

بتعزيز هذا الحق وحمايته. وتشمل المهام المحددة للمقرر جمع المعلومات المتعلقة بالممارسات والتجارب الوطنية فيما يتعلق بالخصوصية والتحديات الناشئة عن التكنولوجيا الحديثة، وتبادل أفضل الممارسات والترويج لها، وتحديد العقبات المحتملة.

وبينما ركزت القرارات السابقة على الآثار السلبية للمراقبة الجماعية ومسؤولية الدول في تقييد سلطات أجهزة الاستخبارات، تعكس آخر القرارات تطوراً رئيسياً في النقاش حول الخصوصية على مستوى الأمم المتحدة.[12] وتؤكد القرارات التي تم اعتمادها في عامي 2016 و2017 على ضرورة الحد من سلطات وكالات الاستخبارات وتدين المراقبة الجماعية. ومن جهة أخرى، فإنها تنص صراحة على أن «القدرات المتزايدة للشركات التجارية فيما يتعلق بجمع البيانات الشخصية ومعالجتها واستخدامها يمكن أن تشكل خطراً على التمتع بالحق في الخصوصية في العصر الرقمي». وبالتالي، إلى جانب مسؤولية هيئات الدولة، تشير القرارات إلى مسؤولية القطاع الخاص فيما يخص احترام حقوق الإنسان، وتدعو الشركات إلى إبلاغ المستخدمين بشأن جمع البيانات الشخصية واستخدامها مشاركتها والاحتفاظ بها، ووضع سياسات معالجة شفافة.

## 3.1.1. الاتفاقية الأوروبية لحقوق الإنسان

تم تشكيل مجلس أوروبا في أعقاب الحرب العالمية الثانية ليجمع دول أوروبا بغية تعزيز سيادة القانون والديمقراطية وحقوق الإنسان والتنمية الاجتماعية. ولهذا الغرض، تم في عام 1950 تبني الاتفاقية الأوروبية لحقوق الإنسان التي دخلت حيز التنفيذ سنة 1953.

يقع على الأطراف المتعاقدة التزام دولي بالامتثال للاتفاقية الأوروبية لحقوق الإنسان. وقد قامت جميع الدول الأعضاء في مجلس أوروبا بإدراج الاتفاقية الأوروبية لحقوق الإنسان أو تفعيل مقتضياتها ضمن قوانينها الوطنية، الأمر الذي يقتضي من هذه الدول التصرف وفقاً لمقتضيات الاتفاقية. ويجب على الأطراف المتعاقدة احترام الحقوق المنصوص عليها في الاتفاقية عند ممارسة أي نشاط أو سلطة، ويشمل ذلك الأنشطة التي تقتضيها حماية الأمن الوطني. وقد أدرجت أحكام بارزة للمحكمة الأوروبية لحقوق الإنسان أنشطة الدولة ضمن المجالات الحساسة لقانون وممارسات الأمن الوطني.[13] ولم تتردد المحكمة في التأكيد على أن أنشطة المراقبة تشكل تدخلاً في احترام الحياة الخاصة.[14]

ولضمان امتثال الأطراف المتعاقدة لالتزاماتها بموجب الاتفاقية الأوروبية لحقوق الإنسان، تم إنشاء المحكمة الأوروبية لحقوق الإنسان في مدينة ستراسبورغ الفرنسية في عام 1959. وتحرص المحكمة الأوروبية لحقوق الإنسان على امتثال الدول لالتزاماتها بموجب الاتفاقية من خلال النظر في الشكايات المقدمة من الأفراد أو مجموعات الأفراد أو المنظمات غير الحكومية أو الأشخاص الاعتباريين يزعمون حدوث انتهاك لمقتضيات الاتفاقية. ويمكن للمحكمة الأوروبية لحقوق الإنسان أيضاً دراسة القضايا الناشئة بين الدول والتي ترفعها دولة واحدة أو أكثر من أعضاء مجلس أوروبا ضد دولة عضو أخرى.

واعتباراً من سنة 2018، أصبح مجلس أوروبا يضم 47 طرفاً متعاقداً، 28 منهم هم أيضاً دول أعضاء في الاتحاد الأوروبي. ولا يتعين على المدعي أمام المحكمة الأوروبية لحقوق الإنسان أن يكون من مواطني أحد الأطراف المتعاقدة، إلا أن الانتهاكات المزعومة يجب أن تكون قد وقعت داخل نطاق السيادة الترابية والقانونية (أي الولاية القضائية) لأحد الأطراف المتعاقدة.

إن الحق في حماية البيانات الشخصية هو من الحقوق المحمية بموجب المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان، والتي تضمن الحق في احترام الحياة الخاصة وحرمة العائلة والمسكن والمراسلات، وتضع الشروط التي بموجبها يُسمح بفرض قيود على هذا الحق.[15]

---

[12] الأمم المتحدة، الجمعية العامة، مشروع قرار منقح بشأن الحق في الخصوصية في العصر الرقمي، A/C.3/71/L.39/Rev.1، نيويورك، 16 نوفمبر 2016؛ الأمم المتحدة، مجلس حقوق الإنسان، الحق في الخصوصية في العصر الرقمي،22 ، A/HRC/34/L.7/Rev.1 مارس 2017.

[13] انظر على سبيل المثال: المحكمة الأوروبية لحقوق الإنسان، قضية «'كلاس' وآخرون ضد ألمانيا»، رقم 5029/71، 6 سبتمبر 1978؛ المحكمة الأوروبية لحقوق الإنسان، قضية «'روتارو' ضد رومانيا» [الغرفة الكبرى]، رقم 28341/95، 4 مايو 2000؛ المحكمة الأوروبية لحقوق الإنسان، قضية «'شابو' و'فيسي' ضد المجر»، رقم 37138/14، 12 يناير 2016.

[14] نفس المرجع السابق.

[15] مجلس أوروبا، الاتفاقية الأوروبية لحقوق الإنسان، سلسلة معاهدات مجلس أوروبا رقم 005، 1950.

وقد بتت المحكمة الأوروبية لحقوق الإنسان في العديد من الحالات التي تنطوي على قضايا حماية البيانات. وتشمل هذه الحالات اعتراض الاتصالات،[16] ومختلف أشكال المراقبة من قبل كل من القطاعين العام والخاص،[17] والحماية من تخزين البيانات الشخصية من قبل السلطات العامة.[18] تجدر الإشارة إلى أن احترام الحياة الخاصة ليس حقاً مطلقاً، لأن ممارسة الحق في الخصوصية يمكن أن تمس بحقوق أخرى، مثل حرية التعبير والوصول إلى المعلومات والعكس صحيح. ومن ثم، تسعى المحكمة جاهدة لإيجاد توازن بين مختلف الحقوق المعنية . وقد أوضحت المحكمة أن المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان لا تلزم الدول فقط بالامتناع عن أي أعمال قد تنتهك هذا الحق المنصوص عليه في الاتفاقية، وإنما تخضع هذه الدول أيضاً في ظروف معينة لالتزامات إيجابية تتعلق بالعمل من أجل ضمان الاحترام الفعلي للحياة الخاصة والعائلية.[19] هذا وتصف الفصول ذات الصلة العديد من هذه الحالات بالتفصيل.

## 4.1.1. الاتفاقية 108 التابعة لمجلس أوروبا

مع ظهور تكنولوجيا المعلومات في ستينات القرن الماضي، كانت هناك حاجة متزايدة لوضع قواعد أكثر تفصيلاً لصون حقوق الأفراد من خلال حماية بياناتهم الشخصية. وبحلول منتصف السبعينات، اعتمدت لجنة الوزراء التابعة لمجلس أوروبا مجموعة متنوعة من القرارات الخاصة بحماية البيانات الشخصية، والتي تشير إلى المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان.[20] وفي عام 1981، فتح باب التوقيع على اتفاقية لحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية (الاتفاقية 108).[21] وكانت الاتفاقية 108، ولا تزال، الصك الدولي الوحيد الملزم قانوناً في مجال حماية البيانات.

تنطبق الاتفاقية 108 على جميع عمليات معالجة البيانات التي يقوم بها كل من القطاعين العام والخاص، بما في ذلك معالجة البيانات من قبل السلطة القضائية وسلطات إنفاذ القانون. وتحمي الاتفاقية الأفراد من الانتهاكات التي قد تصاحب معالجة البيانات الشخصية، كما تسعى في الوقت ذاته إلى تقنين تدفقات البيانات الشخصية عبر الحدود. وفيما يتعلق بمعالجة البيانات الشخصية، تهم المبادئ المنصوص عليها في الاتفاقية، على وجه الخصوص، جمع البيانات ومعالجتها آلياً بصورة عادلة وقانونية، ولأغراض مشروعة ومحددة. هذا يعني أنه لا ينبغي استخدام البيانات لغايات لا تتوافق مع هذه الأغراض وينبغي الاحتفاظ بها لمدة لا تزيد عن اللازم. كما تهم هذه المبادئ جودة البيانات، ولا سيما ضرورة أن تكون ملائمة وذات صلة و صحيحة وألا تكون مفرطة (التناسب).

وإلى جانب تقديم ضمانات بشأن معالجة البيانات الشخصية والالتزامات المتعلقة بأمن البيانات، فإنها تحظر، في غياب ضمانات قانونية مناسبة، معالجة البيانات «الحساسة» - مثل عرق الشخص أو توجهاته السياسية أو صحته أو ديانته أو حياته الجنسية أو سجله الجنائي.

وتكرس الاتفاقية أيضاً حق الفرد في معرفة أن هناك معلومات مخزنة تتعلق به، وإذا لزم الأمر، فإن له الحق كذلك في تصحيحها. إن القيود التي تفرض على الحقوق المنصوص عليها في الاتفاقية ممكنة فقط عندما تكون مصالح عليا، مثل أمن الدولة أو الدفاع عنها، على المحك. إضافة إلى ذلك، تنص الاتفاقية على التدفق الحر للبيانات الشخصية بين الأطراف المتعاقدة وتفرض بعض القيود على التدفقات إلى الدول التي لا يوفر فيها التنظيم القانوني حماية مماثلة.

---

[16] انظر على سبيل المثال: المحكمة الأوروبية لحقوق الإنسان، قضية «مالون ضد المملكة المتحدة»، رقم 8691/79، 2 أغسطس 1984؛ المحكمة الأوروبية لحقوق الإنسان، قضية «كوبلاند ضد المملكة المتحدة»، رقم 62617/00، 3 أبريل 2007؛ أو المحكمة الأوروبية لحقوق الإنسان، قضية « مصطفى سيزغين تانريكولو ضد تركيا»، رقم 27473/06، 18 يوليو 2017.

[17] انظر على سبيل المثال: المحكمة الأوروبية لحقوق الإنسان، قضية «كلاس وآخرون ضد ألمانيا»، رقم 5029/71، 6 سبتمبر 1978؛ المحكمة الأوروبية لحقوق الإنسان، قضية «أوزون ضد ألمانيا»، رقم 35623/05، 2 سبتمبر 2010.

[18] انظر على سبيل المثال: المحكمة الأوروبية لحقوق الإنسان، قضية «رومان زاخاروف ضد روسيا»، رقم 47143/06، 4 ديسمبر 2015؛ المحكمة الأوروبية لحقوق الإنسان، قضية «شابو وفيسي ضد المجر»، رقم 37138/14، 12 يناير 2016.

[19] انظر على سبيل المثال: المحكمة الأوروبية لحقوق الإنسان، قضية «ا ضد فنلندا»، رقم 20511/03، 17 يوليو 2008؛ المحكمة الأوروبية لحقوق الإنسان، قضية «ك. أ. ضد فنلندا»، رقم 2872/02، 2 ديسمبر 2008.

[20] مجلس أوروبا، لجنة الوزراء (1973)، القرار (73) 22 بشأن حماية خصوصية الأفراد فيما يتعلق بنوك البيانات الإلكترونية في القطاع الخاص، 26 سبتمبر 1973؛ مجلس أوروبا، لجنة الوزراء (1974)، القرار (74) 29 بشأن حماية خصوصية الأفراد فيما يتعلق بنوك البيانات الإلكترونية في القطاع العام، 20 سبتمبر 1974.

[21] مجلس أوروبا، اتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية، سلسلة معاهدات مجلس أوروبا رقم 108، 1981.

وتجدر الإشارة إلى أن الاتفاقية 108 ملزمة للدول التي صادقت عليها. وهي لا تخضع للإشراف القضائي للمحكمة الأوروبية لحقوق الإنسان، ولكن تم أخذها بعين الاعتبار في السوابق القضائية لهذه المحكمة في سياق المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان. ومع مرور السنين، قضت المحكمة بأن حماية البيانات الشخصية هي جزء مهم من الحق في احترام الحياة الخاصة (المادة 8)، واسترشدت بمبادئ الاتفاقية 108 في تحديد ما إذا كان هناك تدخل أم لا في هذا الحق الأساسي.[22]

وللمضي قدماً في تطوير المبادئ والقواعد العامة المنصوص عليها في الاتفاقية 108، اعتمدت لجنة الوزراء التابعة لمجلس أوروبا عدة توصيات غير ملزمة قانوناً. وقد أثرت هذه الأخيرة على تطور قانون حماية البيانات في أوروبا. فعلى سبيل المثال، لسنوات عديدة، كان الصك الوحيد في أوروبا الذي يوفر إرشادات حول استخدام البيانات الشخصية في قطاع الشرطة هو «توصية الشرطة».[23] وبالتالي، فإن المبادئ الواردة في التوصية، مثل وسائل الاحتفاظ بملفات البيانات وضرورة تنفيذ قواعد واضحة بشأن الأشخاص المسموح لهم بالوصول إلى هذه الملفات، قد تم تطويرها بشكل أكبر وتم إدراجها في التشريعات اللاحقة للاتحاد الأوروبي.[24] وتسعى آخر التوصيات إلى معالجة تحديات العصر الرقمي - على سبيل المثال، فيما يتعلق بمعالجة البيانات في سياق التوظيف (انظر الفصل 9).

للإشارة فإن جميع الدول الأعضاء في الاتحاد الأوروبي قد صادقت على الاتفاقية 108، وفي عام 1999، تم اقتراح تعديلات على الاتفاقية 108 لتمكين الاتحاد الأوروبي من أن يصبح طرفاً ولكنها لم تدخل حيز التنفيذ.[25] وفي عام 2001، تم اعتماد بروتوكول إضافي للاتفاقية 108، حيث أضاف مقتضيات بشأن تدفقات البيانات عبر الحدود إلى الدول غير الأطراف، أو ما يسمى بالبلدان الثالثة، وبشأن إلزامية إحداث هيئات إشرافية لحماية البيانات الوطنية.[26]

إن الاتفاقية 108 مفتوحة للانضمام أمام الدول غير الأعضاء في مجلس أوروبا ي. وتشكل إمكانات الاتفاقية كمعيار عالمي، إلى جانب طابعها المفتوح، أساساً لتعزيز حماية البيانات على المستوى العالمي. وحتى الآن ، هناك 51 دولة طرف في الاتفاقية 108، و تشمل كافة الدول الأعضاء في مجلس أوروبا (47 دولة)؛ وأوروغواي، التي كانت أول دولة غير أوروبية تنضم في أغسطس 2013؛ ودول موريشيوس والسنغال وتونس التي انضمت في 2016 و2017.

وقد خضعت الاتفاقية مؤخراً لعملية تحديث. حيث أكدت استشارة عامة أجريت في عام 2011 الهدفين الرئيسيين لهذا العمل: تعزيز حماية الخصوصية في الساحة الرقمية وتقوية آلية المتابعة الخاصة بالاتفاقية. وقد ركزت عملية التحديث على هذين الهدفين، واكتملت باعتماد البروتوكول المعدل للاتفاقية 108 (بروتوكول سلسلة معاهدات مجلس أوروبا رقم 223). وقد تم تنفيذ هذا الإجراء بالتوازي مع إصلاحات أخرى لأدوات حماية البيانات الدولية، إلى جانب إصلاح قواعد حماية البيانات في الاتحاد الأوروبي، والذي تم إطلاقه في عام 2012. وقد أولى المنظمون في مجلس أوروبا والاتحاد الأوروبي أقصى درجات العناية لضمان الاتساق والتوافق بين الإطارين القانونيين. هذا ويحافظ التحديث على الطابع العام والمرن للاتفاقية ويعزز إمكاناتها كصك عالمي بشأن قانون حماية البيانات، كما أنه يعيد تأكيد المبادئ الهامة ويثبتها ويتيح حقوقاً جديدة للأفراد، مع زيادة مسؤوليات الجهات التي تعالج البيانات الشخصية وضمان قدر أكبر من المساءلة. وعلى سبيل المثال، يحق للأفراد الذين تتم معالجة بياناتهم الشخصية معرفة منطق معالجة هذه البيانات كما يحق لهم الاعتراض على تلك المعالجة. ولمواجهة الاستخدام المتزايد للتنميط في عالم الإنترنت، تنص الاتفاقية أيضاً على حق الفرد في عدم الخضوع لقرارات تستند فقط إلى المعالجة الآلية دون أخذ وجهات نظره بعين الاعتبار. ويعد الإنفاذ الفعال لقواعد حماية البيانات من قبل الهيئات الإشرافية المستقلة لدى الأطراف المتعاقدة أمراً أساسياً للتنفيذ العملي للاتفاقية. ولهذه الغاية، تؤكد الاتفاقية المحدثة على الحاجة إلى أن تُمنح الهيئات الإشرافية صلاحيات ووظائف فعالة وأن تتمتع باستقلالية حقيقية عند قيامها بمهمتها.

---

[22] انظر على سبيل المثال: المحكمة الأوروبية لحقوق الإنسان، قضية «ز ضد فنلندا»، رقم 22009/93، 25 فبراير 1997.

[23] مجلس أوروبا، لجنة الوزراء (1987)، التوصية (87) 15 للدول الأعضاء التي تنظم استخدام البيانات الشخصية في قطاع الشرطة، ستراسبورغ، 17 سبتمبر 1987.

[24] مجلس أوروبا، لجنة الوزراء (1987)، التوصية (87) 15 للدول الأعضاء التي تنظم استخدام البيانات الشخصية في قطاع الشرطة، ستراسبورغ، 17 سبتمبر 1987. وحرية حركة هذه البيانات، الجريدة الرسمية23 ، 281 L 0J نوفمبر 1995.

[25] مجلس أوروبا، تعديلات على اتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية (سلسلة المعاهدات الأوروبية رقم 108) اعتمدتها لجنة الوزراء بستراسبورغ، في 15 يونيو 1999.

[26] مجلس أوروبا، البروتوكول الإضافي لاتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية، بخصوص الهيئات الإشرافية وتدفقات البيانات عبر الحدود، سلسلة معاهدات مجلس أوروبا رقم 181، 2001. بعد تحديث الاتفاقية 108، لم يعد هذا البروتوكول مطبقاً حيث تم تحديث مقتضياته وإدماجها في الاتفاقية 108 المحدثة.

## 5.1.1. قانون حماية البيانات الأوروبي

يتألف قانون الاتحاد الأوروبي من قانون الاتحاد الأوروبي الأساسي والثانوي. وقد تمت المصادقة على المعاهدات، ولا سيما معاهدة الاتحاد الأوروبي والمعاهدة المنظمة لعمل الاتحاد الأوروبي، من قبل جميع الدول الأعضاء في الاتحاد الأوروبي؛ وبالتالي فإنها تمثل «قانون الاتحاد الأوروبي الأساسي». أما لوائح الاتحاد الأوروبي وأوامره التوجيهية وقراراته فقد تم اعتمادها من قبل مؤسسات الاتحاد الأوروبي التي مُنحت هذه الصلاحية بموجب المعاهدات؛ وهي بالتالي تمثل «قانون الاتحاد الأوروبي الثانوي».

### حماية البيانات في قانون الاتحاد الأوروبي الأساسي

لم تتضمن المعاهدات الأصلية للجماعات الأوروبية أي إشارة إلى حقوق الإنسان أو حمايتها، نظراً إلى أن الجماعة الاقتصادية الأوروبية كانت تعتبر في البداية بمثابة منظمة إقليمية تركز بالأساس على التكامل الاقتصادي وإنشاء سوق مشتركة. إن أحد المبادئ الأساسية التي يقوم عليها إنشاء الجماعات الأوروبية وتنميتها - وهو مبدأ صالح حتى يومنا هذا - هو مبدأ التخويل. وفقاً لهذا المبدأ، يعمل الاتحاد الأوروبي فقط في حدود الاختصاصات المخولة له من قبل الدول الأعضاء، على النحو المبين في معاهدات الاتحاد الأوروبي. وعلى عكس مجلس أوروبا، لا تتضمن معاهدات الاتحاد الأوروبي أي اختصاص صريح بشأن مسائل الحقوق الأساسية.

لكن عندما عُرضت على محكمة العدل التابعة للاتحاد الأوروبي قضايا تزعم حدوث انتهاكات لحقوق الإنسان في مسائل تقع ضمن نطاق قانون الاتحاد الأوروبي، قدمت المحكمة تفسيراً مهماً للمعاهدات، فلتوفير حماية للأفراد، قامت بإدراج الحقوق الأساسية ضمن ما يسمى بالمبادئ العامة للقانون الأوروبي. ووفقاً لمحكمة العدل التابعة للاتحاد الأوروبي، تعكس هذه المبادئ العامة المحتوى الخاص بحماية حقوق الإنسان الموجود في الدساتير الوطنية ومعاهدات حقوق الإنسان، ولا سيما الاتفاقية الأوروبية لحقوق الإنسان. وقد صرحت المحكمة أنها ستحرص على امتثال قانون الاتحاد الأوروبي لهذه المبادئ.

وإقراراً منه بأن سياساته يمكن أن يكون لها أثر على حقوق الإنسان، وفي سعيه لجعل المواطنين يشعرون «بأنهم أقرب» إلى الاتحاد الأوروبي، أعلن هذا الأخير في سنة 2000 عن ميثاق الحقوق الأساسية للاتحاد الأوروبي (الميثاق). ويشتمل الميثاق على مجموعة كاملة من الحقوق المدنية والسياسية والاقتصادية والاجتماعية الخاصة بالمواطنين الأوروبيين، من خلال توليف التقاليد الدستورية والالتزامات الدولية المشتركة بين الدول الأعضاء. وتنقسم الحقوق الواردة في الميثاق إلى ستة أجزاء: الكرامة، والحريات، والمساواة، والتضامن، وحقوق المواطنين، والعدالة.

وبعدما كان في الأصل مجرد وثيقة سياسية، أصبح الميثاق ملزماً قانوناً[27] باعتباره قانون الاتحاد الأوروبي الأساسي (انظر المادة 6 (1) من معاهدة الاتحاد الأوروبي) عندما دخلت معاهدة لشبونة حيز التنفيذ في 1 ديسمبر 2009. [28] وتتوجه مقتضيات الميثاق إلى مؤسسات وهيئات الاتحاد الأوروبي بحيث تلزمها باحترام الحقوق الواردة فيه عند تأدية مهامها. كما أن مقتضيات الميثاق ملزمة للدول الأعضاء عند تنفيذها لقانون الاتحاد الأوروبي.

لا يضمن الميثاق احترام الحياة الخاصة والعائلية (المادة 7) فحسب، بل ينص أيضاً على الحق في حماية البيانات الشخصية (المادة 8). ويرفع الميثاق صراحة مستوى هذه الحماية إلى مستوى حق أساسي في قانون الاتحاد الأوروبي. ويجب على مؤسسات وهيئات الاتحاد الأوروبي أن تضمن هذا الحق وتحترمه، وكذلك الدول الأعضاء عند تنفيذ قانون الاتحاد (المادة 51 من الميثاق). هذا ويجب فهم المادة 8 من الميثاق، والتي تمت صياغتها بعد الأمر التوجيهي الخاص بحماية البيانات بعدة سنوات، على أنها تجسد قانون حماية البيانات الموجود مسبقاً في الاتحاد الأوروبي. لذلك، لا يشير الميثاق صراحةً فقط إلى الحق في حماية البيانات في المادة 8 (1)، ولكنه يشير أيضاً إلى مبادئ حماية البيانات الرئيسية في المادة 8 (2). وأخيراً، تقتضي المادة 8 (3) من الميثاق وجود هيئة مستقلة تتولى مراقبة تنفيذ هذه المبادئ.

[27] الاتحاد الأوروبي (2012)، ميثاق الحقوق الأساسية للاتحاد الأوروبي، الجريدة الرسمية 326 C 2012 OJ.

[28] انظر النسخ الموحدة الخاصة بالجماعات الأوروبية (2012)، معاهدة الاتحاد الأوروبي، الجريدة الرسمية 326 C 2012 OJ؛ والخاصة بالجماعات الأوروبية (2012)، المعاهدة المنظمة لعمل الاتحاد الأوروبي، الجريدة الرسمية 326 C 2012 OJ.

ويعتبر اعتماد معاهدة لشبونة محطة بارزة في تطور قانون حماية البيانات، ليس فقط من ناحية الارتقاء بالميثاق إلى مكانة وثيقة قانونية ملزمة على مستوى القانون الأساسي، ولكن أيضاً من ناحية توفير الحق في حماية البيانات الشخصية. هذا الحق منصوص عليه بالتحديد في المادة 16 من المعاهدة المنظمة لعمل الاتحاد الأوروبي، في الجزء مخصص للمبادئ العامة للاتحاد الأوروبي. وتضع المادة 16 كذلك أساساً قانونياً جديداً يمنح الاتحاد الأوروبي صلاحية التشريع بشأن مسائل حماية البيانات. ويعد هذا الأمر تطوراً مهماً لأن قواعد حماية البيانات في الاتحاد الأوروبي - ولا سيما الأمر التوجيهي الخاص بحماية البيانات - كانت تستند في البداية إلى الأساس القانوني للسوق الداخلية، وإلى الحاجة إلى إحداث تقارب بين القوانين الوطنية بحيث لا تعرقل حرية حركة البيانات داخل الاتحاد الأوروبي. وتوفر المادة 16 من المعاهدة المنظمة لعمل الاتحاد الأوروبي حاليا أساساً قانونياً مستقلاً لمقاربة حديثة وشاملة لحماية البيانات، يشمل كافة المسائل التي تدخل ضمن اختصاص الاتحاد الأوروبي، بما في ذلك التعاون الشرطي والقضائي في المسائل الجنائية. كما تؤكد المادة 16 من المعاهدة المنظمة لعمل الاتحاد الأوروبي أن الامتثال لقواعد حماية البيانات المعتمدة وفقاً لها يجب أن يخضع لمراقبة هيئات إشرافية مستقلة. هذا وقد شكلت المادة 16 أساساً قانونياً لاعتماد الإصلاح الشامل لقواعد حماية البيانات في عام 2016، أي اللائحة العامة لحماية البيانات والأمر التوجيهي الخاص بحماية البيانات الموجه للشرطة وسلطات العدالة الجنائية (انظر أدناه).

**اللائحة العامة لحماية البيانات**

منذ عام 1995 وحتى مايو 2018، كان الأمر التوجيهي رقم EC/95/46، الصادر عن البرلمان الأوروبي والمجلس بتاريخ 24 أكتوبر 1995 بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وحرية حركة هذه البيانات (الأمر التوجيهي الخاص بحماية البيانات)،[29] الصك القانوني الرئيسي للاتحاد الأوروبي بشأن حماية البيانات. وقد تم اعتماده في عام 1995، في وقت اعتمدت فيه العديد من الدول الأعضاء بالفعل قوانين حماية البيانات الوطنية.[30] وقد انبثقت فكرة هذا الأمر التوجيهي من الحاجة إلى المواءمة بين هذه القوانين لضمان مستوى عالٍ من الحماية والتدفق الحر للبيانات الشخصية بين مختلف الدول الأعضاء. فقد كانت حرية حركة السلع ورأس المال والخدمات والأشخاص داخل السوق الداخلية تتطلب التدفق الحر للبيانات، وهو ما لم يكن ممكناً ما لم تتمكن الدول الأعضاء من الاعتماد على إطار رفيع المستوى وموحد لحماية البيانات.

لقد كان الأمر التوجيهي الخاص بحماية البيانات يعكس مبادئ حماية البيانات الواردة بالفعل في القوانين الوطنية وفي الاتفاقية 108، مع توسيعها في كثير من الأحيان. وقد استند إلى إمكانية إضافة صكوك حماية، كما هو منصوص عليه في المادة 11 من الاتفاقية 108. وقد تبين أن إدراج الإشراف المستقل على وجه الخصوص في الأمر التوجيهي كأداة لتحسين الامتثال لقواعد حماية البيانات هو بمثابة مساهمة مهمة في الأداء الفعال لقانون حماية البيانات الأوروبي. وبالتالي، تمت إضافة هذه الميزة إلى قانون مجلس أوروبا في عام 2001 من خلال البروتوكول الإضافي للاتفاقية 108. ويوضح هذا الأمر التفاعل الوثيق بين الصكين والتأثير الإيجابي المتبادل بينهما على مر السنين.

وقد أنشأ الأمر التوجيهي الخاص بحماية البيانات نظام حماية بيانات مفصل وشامل في الاتحاد الأوروبي. لكن وفقاً للنظام القانوني للاتحاد الأوروبي، لا تنطبق الأوامر التوجيهية بشكل مباشر ويجب اعتمادها ضمن القوانين الوطنية للدول الأعضاء. وبالتالي، فإن تمتع الدول الأعضاء بهامش تقدير في اعتماد مقتضيات الأمر التوجيهي هو أمر حتمي. وعلى الرغم من أن الأمر التوجيهي كان يهدف إلى توفير اتساق كامل[31] (ومستوى حماية كاملة)، فقد تم اعتماده عملياً بشكل مختلف في الدول الأعضاء. وقد أدى ذلك إلى إحداث قواعد متنوعة في مجال حماية البيانات في مختلف بلدان الاتحاد الأوروبي، كما اختلف تفسير التعاريف والقواعد في القوانين الوطنية. وتباينت كذلك مستويات الإنفاذ وشدة العقوبات بين الدول الأعضاء. وأخيراً، طرأت تغييرات كبيرة في مجال تكنولوجيا المعلومات منذ صياغة الأمر التوجيهي في منتصف التسعينات. وقد عجلت هذه الأسباب مجتمعة بإصلاح تشريعات حماية البيانات في الاتحاد الأوروبي.

---

[29] الأمر التوجيهي رقم EC/95/46 الصادر عن البرلمان الأوروبي والمجلس بتاريخ 24 أكتوبر 1995 بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وحرية حركة هذه البيانات، الجريدة الرسمية L 281 1995 OJ.

[30] اعتمدت ولاية هيسن الألمانية أول قانون لحماية البيانات في العالم سنة 1970، والذي كان ينطبق فقط على تلك الولاية. واعتمدت السويد القانون المعروف باسم «Datalagen» سنة 1973؛ واعتمدت ألمانيا قانون «Bundesdatenschutzgestez» سنة 1976؛ فيما اعتمدت فرنسا القانون المتعلق بالمعلوميات والملفات والحريات (Loi relatif à l'informatique, aux fichiers et aux libertés) سنة 1977. وفي المملكة المتحدة، تم اعتماد قانون حماية البيانات سنة 1984. وأخيرًا، اعتمدت هولندا التشريع المعروف بمسمى «Wet Persoonregistraties» سنة 1989.

[31] محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-468/10 وC-469/10، قضية «الرابطة الوطنية للمؤسسات المالية الائتمانية واتحاد التجارة الإلكترونية والتسويق المباشر ضد إدارة الدولة»، 24 نوفمبر 2011، الفقرة 29.

وقد أسفر الإصلاح عن اعتماد اللائحة العامة لحماية البيانات في أبريل 2016، بعد سنوات من النقاش المكثف. وكانت المناقشات حول الحاجة إلى تحديث قواعد حماية البيانات في الاتحاد الأوروبي قد بدأت سنة 2009، عندما أطلقت المفوضية مشاورة عامة حول الإطار القانوني المستقبلي للحق الأساسي في حماية البيانات الشخصية. وتم نشر مقترح اللائحة من قبل المفوضية في يناير 2012، لتنطلق بذلك عملية تشريعية طويلة من المفاوضات بين البرلمان الأوروبي ومجلس الاتحاد الأوروبي. وبعد اعتمادها، نصت اللائحة العامة لحماية البيانات على فترة انتقالية لمدة عامين. وقد أصبحت اللائحة مطبقة بالكامل في 25 مايو 2018، عندما تم إلغاء الأمر التوجيهي الخاص بحماية البيانات.

ونجم عن اعتماد اللائحة العامة لحماية البيانات في عام 2016 تحديث تشريعات حماية البيانات في الاتحاد الأوروبي، بصورة تجعلها مناسبة لحماية الحقوق الأساسية في سياق التحديات الاقتصادية والاجتماعية للعصر الرقمي. إن اللائحة العامة لحماية البيانات تحفظ وتطور المبادئ والحقوق الأساسية لصاحب البيانات المنصوص عليها في الأمر التوجيهي الخاص بحماية البيانات. علاوة على ذلك، فإنها قد أضافت التزامات جديدة تقتضي من المنظمات تطبيق إجراءات حماية البيانات منذ التصميم وتلقائياً؛ وتعيين مسؤول عن حماية البيانات في ظروف معينة؛ والامتثال للحق الجديد في إمكانية نقل البيانات؛ والامتثال لمبدأ المساءلة. وبموجب قانون الاتحاد الأوروبي، فإن اللوائح قابلة للتطبيق مباشرة، وليست هناك حاجة للتنفيذ الوطني. وبالتالي، تنص اللائحة العامة لحماية البيانات على مجموعة واحدة من قواعد حماية البيانات تنطبق على كافة دول الاتحاد الأوروبي. هذا الأمر يؤدي إلى وضع قواعد متسقة في مجال حماية البيانات في مختلف أنحاء الاتحاد الأوروبي، ما ينجم عنه إنشاء بيئة تتسم باليقين القانوني يمكن أن يستفيد منها المشغلون الاقتصاديون والأفراد بصفتهم «أصحاب البيانات».

لكن على الرغم من أن اللائحة العامة لحماية البيانات قابلة للتطبيق بشكل مباشر، من المتوقع أن تقوم الدول الأعضاء بتحديث قوانين حماية البيانات الوطنية الحالية الخاصة بها لتوائم اللائحة بشكل كامل، وتعكس في الوقت ذاته هامش تقدير لمقتضيات محددة في الحيثية 10. هذا وتشكل القواعد والمبادئ الرئيسية المنصوص عليها في اللائحة، إلى جانب الحقوق القوية التي تمنحها للأفراد، جزءاً كبيراً من الدليل، وسيتم عرضها في الفصول التالية. وتتوفر اللائحة على قواعد شاملة بشأن النطاق الإقليمي، وتنطبق على الشركات المنشأة في الاتحاد الأوروبي، وأيضاً على المراقبين والمعالجين غير الموجودين في الاتحاد الأوروبي والذين يقدمون سلعاً أو خدمات لأصحاب البيانات في الاتحاد الأوروبي أو يراقبون سلوكهم. ونظراً إلى أن العديد من شركات التكنولوجيا خارج حدود الاتحاد الأوربي لها حصة رئيسية في السوق الأوروبية وملايين العملاء داخل الاتحاد، فإن إخضاع هذه المنظمات لقواعد حماية البيانات في الاتحاد الأوروبي أمر مهم لضمان حماية الأفراد وتكافؤ الفرص.

**حماية البيانات في مجال إنفاذ القانون - الأمر التوجيهي رقم 680/2016**

قدم الأمر التوجيهي المتعلق بحماية البيانات الملغى نظاماً شاملاً لحماية البيانات. وقد تعزز هذا النظام الآن باعتماد اللائحة العامة لحماية البيانات. فبالرغم من كونه شاملاً، كان نطاق تطبيق الأمر التوجيهي المتعلق بحماية البيانات الملغى محدوداً، فقد اقتصر على الأنشطة التي تتم داخل السوق الداخلية، إلى جانب أنشطة السلطات العامة غير تلك المختصة في مجال إنفاذ القانون. وعليه، كان من الضروري اعتماد صكوك خاصة بغية تحقيق الوضوح اللازم والتوازن بين حماية البيانات والمصالح المشروعة الأخرى والتصدي للتحديات المرتبطة بشكل خاص بقطاعات محددة. وينطبق هذا الأمر على القواعد التي تنظم معالجة البيانات الشخصية من قبل سلطات إنفاذ القانون.

وكان القرار الإطار JHA/2008/977 الصادر عن المجلس بشأن حماية البيانات الشخصية المعالجة في إطار التعاون الشرطي والقضائي في المسائل الجنائية أول صك قانوني في الاتحاد الأوروبي ينظم هذه المسألة. لكن قواعده لا تسري إلا على بيانات الشرطة والقضاء عند تبادلها بين الدول الأعضاء. المعالجة المحلية للبيانات الشخصية من قبل سلطات إنفاذ القانون لا تندرج ضمن نطاق تطبيقه.

وقد جاء الأمر التوجيهي رقم 680/2016 الخاص بحماية الأشخاص الذاتيين فيما يتعلق بمعالجة البيانات الشخصية من قبل السلطات المختصة لأغراض منع الجرائم الجنائية أو التحقيق فيها أو كشفها أو متابعة مرتكبيها أو تنفيذ العقوبات الجنائية، والمتعلق أيضاً بحرية نقل

هذه البيانات،[32] المشار إليه بالأمر التوجيهي الخاص بحماية البيانات الموجه للشرطة وسلطات العدالة الجنائية، لتدارك هذا الوضع. فهذا الأمر التوجيهي الذي تم اعتماده بموازاة اللائحة العامة لحماية البيانات، قد ألغى القرار الإطار JHA/2008/977 ووضع نظاماً شاملاً لحماية البيانات الشخصية في سياق إنفاذ القانون، كما أقر بخصوصيات معالجة البيانات المتعلقة بالأمن العام. وفي الوقت الذي تحدد فيه اللائحة العامة لحماية البيانات القواعد العامة لحماية الأفراد فيما يتعلق بمعالجة بياناتهم الشخصية وضمان حرية حركة هذه البيانات داخل الاتحاد الأوروبي، يضع الأمر التوجيهي قواعد خاصة بشأن حماية البيانات في مجالي التعاون القضائي في المسائل الجنائية وتعاون الشرطة. وبالتالي، ينطبق الأمر التوجيهي رقم 680/2016 عند قيام سلطة مختصة بمعالجة البيانات لأغراض منع الجرائم الجنائية أو التحقيق فيها أو كشفها أو متابعة مرتكبيها أو تنفيذ العقوبات الجنائية. وعندما تقوم السلطات المختصة بمعالجة البيانات الشخصية لأغراض غير تلك الواردة أعلاه، ينطبق النظام العام للائحة العامة لحماية البيانات. وبخلاف سابقه (القرار الإطار JHA/2008/977 الصادر عن المجلس)، يمتد نطاق تطبيق الأمر التوجيهي رقم 2016/680 ليشمل المعالجة المحلية للبيانات الشخصية من قبل سلطات إنفاذ القانون ولا يقتصر على تبادل هذه البيانات بين الدول الأعضاء. علاوة على ذلك، يسعى الأمر التوجيهي إلى تحقيق توازن بين حقوق الأفراد والأهداف المشروعة للمعالجة المتعلقة بالجانب الأمني.

ولهذا الغرض، يؤكد الأمر التوجيهي على الحق في حماية البيانات الشخصية والمبادئ الأساسية التي ينبغي أن تشمل معالجة البيانات، مع الحرص على اتباع القواعد والمبادئ المنصوص عليها في اللائحة العامة لحماية البيانات. وتتشابه حقوق الأفراد والمسؤوليات المفروضة على المراقبين – على سبيل المثال، فيما يتعلق بأمن البيانات وحماية البيانات منذ التصميم وتلقائياً والإشعارات المتعلقة بخروقات البيانات – مع الحقوق والمسؤوليات المنصوص عليها في اللائحة العامة لحماية البيانات. هذا ويأخذ الأمر التوجيهي أيضاً بعين الاعتبار التحديات التكنولوجية الناشئة والخطيرة والتي يمكن أن يكون لها أثر سلبي شديد على الأفراد، كاستعمال سلطات إنفاذ القانون لتقنيات التنميط، ويسعى أيضاً إلى التصدي لها. فمن حيث المبدأ، يجب حظر القرارات المستندة إلى المعالجة الآلية فقط، بما في ذلك التنميط.[33] بالإضافة إلى ذلك، لا يجب أن ترتكز القرارات على بيانات حساسة. هذا وتخضع هذه المبادئ لبعض الاستثناءات التي ينص عليها الأمر التوجيهي. كما أن هذه المعالجة لا يجب أن تتسبب في تمييز ضد أي شخص.[34]

ويضم الأمر التوجيهي أيضاً قواعد تضمن مساءلة المراقبين، الذين يتعين عليهم اختيار مسؤول عن حماية البيانات لمراقبة الامتثال لقواعد حماية البيانات، مع إبلاغ الجهة المعنية والموظفين الذين يباشرون أعمال المعالجة بالتزاماتهم وإسداء المشورة لهم، والتعاون مع الهيئة الإشرافية. وتخضع كل من معالجة البيانات الشخصية في أجهزة الشرطة وقطاع العدالة الجنائية الآن لإشراف هيئات مستقلة. هذا ويجب أن يمتثل كل من النظام القانوني العام لحماية البيانات ونظام حماية البيانات الخاص بإنفاذ القانون والمسائل الجنائية بالتساوي مع متطلبات ميثاق الحقوق الأساسية للاتحاد الأوروبي.

يصف الفصل 8 بشكل مفصل النظام الخاص لمعالجة البيانات في سياق التعاون الشرطي والقضائي المنصوص عليه في الأمر التوجيهي الخاص بحماية البيانات الموجه للشرطة وسلطات العدالة الجنائية.

**الأمر التوجيهي المتعلق بالخصوصية والاتصالات الإلكترونية**

لقد كان وضع قواعد خاصة لحماية البيانات ضرورياً أيضا في قطاع الاتصالات الإلكترونية. فمع تطور الإنترنت وخطوط الهواتف الأرضية والمتنقلة، كان من المهم ضمان احترام حق المستخدمين في الخصوصية وفي السرية. ويحدد الأمر التوجيهي رقم 2002/58/0EC I35 المتعلق بمعالجة البيانات

[32] الأمر التوجيهي (الاتحاد الأوروبي) رقم 680/2016 الصادر عن البرلمان الأوروبي والمجلس بتاريخ 27 أبريل 2016 بشأن حماية الأشخاص الذاتيين فيما يتعلق بمعالجة البيانات الشخصية من قبل السلطات المختصة لأغراض منع الجرائم الجنائية أو التحقيق فيها أو الكشف عنها أو متابعة مرتكبيها أو تنفيذ العقوبات الجنائية، والمتعلق أيضاً بحرية حركة هذه البيانات، الجريدة الرسمية 4 ،119 L OJ I مايو 2016.

[34] نفس المرجع السابق، المادة 11 (2) و(3).

[35] الأمر التوجيهي رقم EC/2002/58 الصادر عن البرلمان الأوروبي والمجلس بتاريخ 12 يوليو 2002 المتعلق بمعالجة البيانات الشخصية وحماية الخصوصية في الاتصالات الإلكترونية، الجريدة الرسمية 201 L OJ (الأمر التوجيهي المتعلق بالخصوصية والاتصالات الإلكترونية أو الأمر التوجيهي المتعلق بالخصوصية الإلكترونية).

[36] الأمر التوجيهي المتعلق بالخصوصية والاتصالات الإلكترونية، المادة 4 (1).

الشخصية وحماية الخصوصية في الاتصالات الإلكترونية (الأمر التوجيهي المتعلق بالخصوصية والاتصالات الإلكترونية أو الأمر التوجيهي المتعلق بالخصوصية الإلكترونية) قواعد تخص أمن البيانات الشخصية في هذه الشبكات، وإشعار الأشخاص بخروقات البيانات، وسرية الاتصالات.

وفيما يتعلق بالجانب الأمني، يجب على مشغلي خدمات الاتصالات الإلكترونية، ضمن جملة من الأمور، الحرص على اقتصار الوصول إلى البيانات الشخصية فقط على الأشخاص المصرح لهم بذلك، كما يتعين عليهم اتخاذ تدابير لمنع إتلاف البيانات الشخصية أو ضياعها أو تضررها عن طريق الخطأ.36 وعند وجود خطر الإخلال بأمن شبكة الاتصالات العامة، يجب على المشغلين إبلاغ المشتركين بهذا الخطر،[37] وفي حال وقوع اختراق أمني بالرغم من التدابير الأمنية المتخذة، يجب على المشغلين إشعار الهيئة الوطنية المختصة المكلفة بتنفيذ وإنفاذ الأمر التوجيهي الخاص بخرق البيانات الشخصية. ويتعين على المشغلين أحياناً إشعار الأفراد باختراقات البيانات الشخصية، لا سيما في حال تأثير الاختراق سلباً على بياناتهم الشخصية أو خصوصيتهم.[38] وتقتضي سرية الاتصالات، من حيث المبدأ، حظر الاستماع للاتصالات أو التنصت عليها أو تخزينها أو أي شكل من أشكال مراقبة الاتصالات والبيانات الوصفية أو اعتراضها. هذا ويحظر الأمر التوجيهي أيضاً الاتصالات غير المرغوب فيها (يشار إليها غالباً باسم «البريد العشوائي»)، إلا إذا منح المستخدمون موافقتهم على ذلك، كما يتضمن قواعد حول تخزين «ملفات تعريف الارتباط» («كوكيز») على الكمبيوتر والأجهزة. وتشير هذه الالتزامات السلبية الأساسية بوضوح إلى أن سرية الاتصالات مرتبطة بشكل كبير بحماية الحق في احترام الحياة الخاصة المنصوص عليه في المادة 7 من الميثاق والحق في حماية البيانات الشخصية المنصوص عليه في المادة 8 من الميثاق.

في يناير من عام 2017، نشرت المفوضية مقترحاً بشأن لائحة تخص احترام الحياة الخاصة وحماية البيانات الشخصية فيما يتعلق بالاتصالات الإلكترونية، والتي كان الغرض منها استبدال الأمر التوجيهي المتعلق بالخصوصية الإلكترونية. ويهدف الإصلاح إلى مواءمة القواعد المنظمة للاتصالات الإلكترونية مع النظام الجديد لحماية البيانات الشخصية المنشأ بموجب اللائحة العامة لحماية البيانات. وسيتم تطبيق اللائحة الجديدة مباشرة في مختلف أنحاء الاتحاد الأوروبي؛ حيث سيتمتع جميع الأفراد بنفس المستوى من الحماية فيما يتعلق باتصالاتهم الإلكترونية، فيما سيستفيد مشغلو شبكات الاتصالات والشركات من الوضوح واليقين القانوني ووجود مجموعة واحدة من القوانين في مختلف أنحاء الاتحاد الأوروبي. وستُطبق القواعد المقترحة بشأن سرية الاتصالات الإلكترونية أيضاً على الجهات الفاعلة الجديدة التي تقدم خدمات الاتصالات الإلكترونية و التي لا يشملها الأمر التوجيهي المتعلق بالخصوصية الإلكترونية، حيث لا يشمل هذا الأخير سوى مقدمي خدمات الاتصالات التقليدية. وبفعل الانتشار الهائل لاستخدام خدمات مثل «سكايب» و«واتساب» و«فيسبوك ماسنجر» و«ڤايبر» لتبادل الرسائل أو إجراء الاتصالات، ستدخل الآن خدمات الاتصال المباشر عبر الإنترنت هذه ضمن نطاق سريان اللائحة وسيتعين عليها الامتثال لمتطلبات هذه الأخيرة فيما يتعلق بحماية البيانات والخصوصية والأمن. وحتى تاريخ نشر هذا الدليل، كان مسار تشريعي خاص بوضع قواعد الخصوصية الإلكترونية ما يزال جارياً.

**اللائحة رقم 45/2001**

ونظراً لأن الأمر التوجيهي الخاص بحماية البيانات لا يمكن أن يسري إلا على الدول الأعضاء في الاتحاد الأوروبي، فقد كانت هناك حاجة إلى صك قانوني إضافي للتنصيص على حماية البيانات عند معالجة البيانات الشخصية من قبل مؤسسات الاتحاد الأوروبي وهيئاته. وهكذا فإن اللائحة (الجماعة الأوروبية) رقم 45/2001 بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية من قبل مؤسسات الاتحاد وهيئاته وحرية حركة هذه البيانات (لائحة حماية بيانات مؤسسات الاتحاد الأوروبي) تؤدي هذه المهمة.[39]

تتقيد اللائحة رقم 45/2001 بمبادئ نظام الاتحاد الأوروبي العام لحماية البيانات، وتطبق هذه المبادئ على معالجة البيانات من قبل مؤسسات وهيئات الاتحاد الأوروبي أثناء ممارسة وظائفها. إضافة إلى ذلك، فإنها تحدث هيئة إشرافية مستقلة لتتبع تطبيق مقتضياتها، تتمثل في المشرف الأوروبي على حماية البيانات الذي توكل له صلاحيات إشرافية ومهمة تتبع معالجة البيانات الشخصية في مؤسسات الاتحاد الأوروبي وهيئاته، والاستماع للشكايات المتعلقة بالخروقات المزعومة لقواعد حماية البيانات والتحقيق فيها. كما يقدم المشورة لمؤسسات وهيئات الاتحاد الأوروبي

[37] نفس المرجع السابق، المادة 4 (2).

[38] نفس المرجع السابق، المادة 4 (3).

[39] اللائحة (الجماعة الأوروبية) رقم 45/2001 الصادرة عن البرلمان الأوروبي والمجلس بتاريخ 18 ديسمبر 2000 بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية من قبل مؤسسات الاتحاد وهيئاته وحرية حركة هذه البيانات، الجريدة الرسمية L 8 2001 0J.

بشأن جميع الأمور المتعلقة بحماية البيانات الشخصية، بدءاً من المقترحات التي تخص التشريعات الجديدة ووصولاً إلى صياغة القواعد الداخلية المتعلقة بمعالجة البيانات.

وفي يناير من سنة 2017، قدمت المفوضية الأوروبية مقترحاً بخصوص اللائحة الجديدة المتعلقة بمعالجة البيانات من قبل مؤسسات الاتحاد الأوروبي، والتي ستلغي اللائحة الحالية. وكما كان الحال بالنسبة لإصلاح الأمر التوجيهي المتعلق بالخصوصية الإلكترونية، سيقوم إصلاح اللائحة رقم 45/2001 بتحديث ومواءمة قواعدها مع النظام الجديد لحماية البيانات المحدث بموجب اللائحة العامة لحماية البيانات.

**دور محكمة العدل التابعة للاتحاد الأوروبي**

إن الاختصاص القضائي لمحكمة العدل التابعة للاتحاد الأوروبي يشمل تحديد ما إذا كانت دولة عضو قد أوفت بالتزاماتها بموجب قانون حماية البيانات الخاص بالاتحاد الأوروبي، وتفسير تشريعات الاتحاد الأوروبي لضمان تطبيقها بصورة فعالة وموحدة في مختلف الدول الأعضاء. ومنذ اعتماد الأمر التوجيهي الخاص بحماية البيانات في 1995، تراكم عدد كبير من السوابق القضائية التي توضح نطاق ومعنى مبادئ حماية البيانات والحق الأساسي في حماية البيانات الشخصية على النحو المنصوص عليه في المادة 8 من الميثاق. وعلى الرغم من إلغاء الأمر التوجيهي وتعويضه بصك قانوني جديد، وهو اللائحة العامة لحماية البيانات، فإن السوابق القضائية التي سبقت هذا الأخير تظل ذات صلة وصالحة لتفسير وتطبيق مبادئ حماية البيانات في الاتحاد الأوروبي، وذلك في حدود المبادئ والمفاهيم الأساسية للأمر التوجيهي الخاص بحماية البيانات التي أبقت عليها اللائحة العامة لحماية البيانات.

## 2.1. القيود المفروضة على الحق في حماية البيانات الشخصية

### النقـــاط الرئيسيـــة

- إن الحق في حماية البيانات ليس حقاً مطلقاً؛ فقد يتم تقييده عند الضرورة من أجل تحقيق مصلحة عامة أو حماية حقوق الآخرين وحرياتهم.
- تمت الإشارة إلى شروط تقييد الحق في احترام الحياة الشخصية والحق في حماية البيانات الشخصية في المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان والمادة 52 (1) من الميثاق. وقد تم التوسع فيها وتفسيرها من خلال السوابق القضائية للمحكمة الأوروبية لحقوق الإنسان ومحكمة العدل التابعة للاتحاد الأوروبي.
- بمقتضى قانون حماية البيانات الصادر عن مجلس أوروبا، تعد معالجة البيانات الشخصية تدخلاً قانونياً في الحق في احترام الحياة الخاصة ولا يمكن القيام بها إلا إذا كانت:
  - وفقاً للقانون؛
  - تسعى لتحقيق هدف مشروع؛
  - تحترم جوهر الحقوق والحريات الأساسية؛
  - ضرورية ومتناسبة في مجتمع ديمقراطي لتحقيق غرض مشروع.

- يضع النظام القانوني للاتحاد الأوروبي شروطاً مماثلة على القيود المفروضة على ممارسة الحقوق الأساسية التي يكفلها الميثاق. لا يكون أي تقييد مفروض على أي حق أساسي، بما في ذلك حماية البيانات الشخصية، قانونياً إلا إذا كان:
  - وفقاً للقانون؛
  - يحترم جوهر الحق؛
  - يخضع لمبدأ التناسبية، عند الاقتضاء؛
  - يسعى إلى تحقيق هدف يهم المصلحة العامة معترف به من قبل الاتحاد الأوروبي، أو إلى حماية حقوق الآخرين.

إن الحق الأساسي في حماية البيانات بمقتضى المادة 8 من الميثاق ليس حقاً مطلقاً، «وإنما يجب النظر إليه في إطار وظيفته في المجتمع».[40] وبالتالي، فإن المادة 52 (1) من الميثاق تقر بأنه يمكن فرض قيود على ممارسة الحقوق كتلك الواردة في المادتين 7 و8 من الميثاق، إذا كان القانون ينص على هذه القيود، وكانت تحترم جوهر هذه الحقوق والحريات، وتخضع لمبدأ التناسبية، وتعد ضرورية، وتحقق فعلاً أهداف المصلحة العامة التي يقرها الاتحاد الأوروبي أو تستجيب لضرورة حماية حقوق الآخرين وحرياتهم.[41] وعلى نحو مماثل، في نظام الاتفاقية الأوروبية لحقوق الإنسان، تكفل المادة 8 حماية البيانات، لكن قد يتم تقييد ممارسة هذا الحق عند الضرورة لتحقيق غرض مشروع. ويشير هذا الجزء إلى الشروط الخاصة بالتدخل بمقتضى الاتفاقية الأوروبية لحقوق الإنسان، كما تم تفسيرها في السوابق القضائية للمحكمة الأوروبية لحقوق الإنسان، والشروط المتعلقة بالقيود القانونية بموجب المادة 52 من الميثاق.

## 1.2.1. متطلبات التدخل المبرر بمقتضى الاتفاقية الأوروبية لحقوق الإنسان

قد تشكل معالجة البيانات الشخصية تدخلاً في حق احترام الحياة الخاصة لصاحب البيانات الذي تكفله المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان.[42] وكما تم توضيحه أعلاه (انظر الجزء 1.1.1 والجزء 4.1.1.)، خلافاً للنظام القانوني للاتحاد الأوروبي، لا تقر الاتفاقية الأوروبية لحقوق الإنسان بكون حماية البيانات الشخصية حقاً أساسياً منفردا، بل ترى أنها جزء من الحقوق المكفولة بموجب الحق في احترام الحياة الخاصة. لذلك، فإنه لا يمكن إدراج كل عملية تنطوي على معالجة البيانات الشخصية ضمن نطاق المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان. ولإعمال المادة 8، يجب أولاً تحديد ما إذا تم المس بمصلحة خاصة أو بالحياة الخاصة لشخص ما. ومن خلال السوابق القضائية، تناولت المحكمة الأوروبية لحقوق الإنسان مفهوم «الحياة الخاصة» باعتباره مفهوماً واسعا، يتسع ليشمل حتى الجوانب المتعلقة بالحياة المهنية والسلوك في المجال العام. كما أصدرت قراراً يقضي بأن حماية البيانات الشخصية جزء مهم من الحق في احترام الحياة الخاصة. إلا أنه بالرغم من التفسير الواسع للحياة الخاصة، لا تمس جميع أنواع المعالجة في حد ذاتها بالحقوق المكفولة بموجب المادة 8.

وعندما ترى المحكمة الأوروبية لحقوق الإنسان أن عملية المعالجة تؤثر على حق الأفراد في احترام الحياة الخاصة، فإنها ستتبين ما إذا كان التدخل مبرراً. إن الحق في احترام الحياة الخاصة ليس حقاً مطلقاً، وإنما يجب موازنته مع المصالح والحقوق المشروعة الأخرى والتوفيق فيما بينها، سواء كانت تخص أشخاصاً آخرين (المصالح الخاصة) أو المجتمع ككل (المصالح العامة).

الشروط التراكمية التي يمكن بموجبها تبرير التدخل هي:

#### أن يكون وفقاً للقانون

وفقاً للسوابق القضائية للمحكمة الأوروبية لحقوق الإنسان، يكون التدخل وفقاً للقانون إذا كان يستند إلى أحد مقتضيات القانون الوطني الذي يتصف بسمات معينة. يجب أن يكون القانون «في متناول الأشخاص المعنيين ويمكن توقع آثاره».[43] ويمكن توقع قاعدة معينة «إذا تمت صياغتها بدقة كافيةلتمكين أي شخص من تنظيم سلوكه - مع المشورة المناسبة إذا لزم الأمر».[44] علاوة على ذلك، «ستعتمد درجة الدقة المطلوبة من 'القانون' في هذا الصدد على الموضوع.»[45]

---

[40] انظر على سبيل المثال، محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-92/09وC-93/09، شركة «فولكر وماركوس تشيكه» وهارتموت أيفرت ضد ولاية هيسن [الغرفة الكبرى]، 9 نوفمبر 2010، الفقرة 48.

[41] نفس المرجع السابق، الفقرة 50.

[42] المحكمة الأوروبية لحقوق الانسان، قضية «س. ومارب ضد المملكة المتحدة» [الغرفة الكبرى]، رقم 30562/04 ورقم 30566/04، 8 ديسمبر 2008، الفقرة 67.

[43] المحكمة الأوروبية لحقوق الإنسان، قضية «أمان ضد سويسرا» [الغرفة الكبرى]، رقم 27798/95، 16 فبراير 2000، الفقرة 50؛ انظر أيضاً المحكمة الأوروبية لحقوق الإنسان، قضية «كوب ضد سويسرا»، رقم 23224/94، 25 مارس 1998، الفقرة 55، والمحكمة الأوروبية لحقوق الإنسان، قضية «إيوردانشي وآخرون ضد مولدوفا»، رقم 25198/02، 10 فبراير 2009، الفقرة 50.

[44] المحكمة الأوروبية لحقوق الإنسان، قضية «أمان ضد سويسرا» [الغرفة الكبرى]، رقم 27798/95، 16 فبراير 2000، الفقرة 56؛ انظر أيضاً المحكمة الأوروبية لحقوق الإنسان، قضية «مالون ضد المملكة المتحدة»، رقم 8691/79، 2 أغسطس 1984، الفقرة 66؛ المحكمة الأوروبية لحقوق الإنسان، قضية «سيلفر وآخرون ضد المملكة المتحدة»، رقم5947/72 ، ورقم 6205/73، ورقم 7052/75، ورقم 7061/75 ورقم 7107/75 ورقم 7113/75، 25 مارس 1983، الفقرة 88.

[45] المحكمة الأوروبية لحقوق الإنسان، قضية «'ذا صنداي تايمز' ضد المملكة المتحدة»، رقم 6538/74، 26 أبريل1979، الفقرة 49؛ أنظر أيضاً المحكمة الأوروبية لحقوق الإنسان، قضية «سيلفر وآخرون ضد المملكة المتحدة»، رقم5947/72 ، ورقم 6205/73، ورقم 7052/75، ورقم 7061/75 ورقم 7107/75 ورقم 7113/75، 25 مارس 1983، الفقرة 88.

أمثلة: في قضية «روتارو ضد رومانيا»،[46] زعم المدعي انتهاك حقه في احترام حياته الخاصة بسبب احتفاظ جهاز المخابرات الروماني بملف يحتوي على معلوماته الشخصية واستخدامه. ووجدت المحكمة الأوروبية لحقوق الإنسان أنه في الوقت الذي يسمح فيه القانون الوطني بجمع المعلومات التي تمس بالأمن الوطني وتسجيلها وأرشفتها في ملفات سرية، فإنه لم يفرض أي قيود على ممارسة هذه الصلاحيات، والتي ظلت خاضعة للسلطة التقديرية للسلطات. وعلى سبيل المثال، لم يحدد القانون الوطني نوع المعلومات التي يمكن معالجتها، أو فئات الأشخاص الذين يمكن اتخاذ تدابير المراقبة في حقهم، أو الظروف التي يمكن فيها اتخاذ مثل هذه التدابير، أو الإجراء الواجب اتباعه. وبناءً عليه، خلصت المحكمة إلى أن القانون الوطني لم يمتثل لشرط التوقعية (أي إمكانية توقع الشيء) المنصوص عليه في المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان وأن هذه المادة قد انتهكت.

في قضية «'تايلور-سابوري' ضد المملكة المتحدة»،[47] كان المدعي خاضعاً لمراقبة الشرطة. وباستخدام «نسخة» من جهاز استدعاء المدعي، تمكنت الشرطة من اعتراض الرسائل المرسلة إليه. وقد ألقي القبض على المدعي ووجهت إليه تهمة التآمر لتوريد مخدر خاضع للمراقبة. وكان جزء من الدعوى المرفوعة ضده يتألف من ملاحظات مكتوبة تتزامن مع رسائل جهاز الاستدعاء، قامت الشرطة بتدوينها. ومع ذلك، أثناء محاكمة المدعي، لم يكن هناك مقتضى في القانون البريطاني ينظم اعتراض الاتصالات المنقولة عبر نظام اتصالات خاص. ولذلك فإن التدخل في حقوقه لم يكن «وفقاً للقانون». وخلصت المحكمة الأوروبية لحقوق الإنسان إلى أن هذا الأمر ينتهك المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان.

تتعلق قضية «'فوكوتا-بويتش' ضد سويسرا»[48] بالمراقبة السرية لمطالبة بالتأمين الاجتماعي من قبل محققين خاصين بتكليف من شركة التأمين الخاصة بها. وقد رأت المحكمة الأوروبية لحقوق الإنسان أنه في الوقت الذي أمرت فيه شركة تأمين خاصة باتخاذ إجراء المراقبة الوارد في الشكاية، فإن الدولة قد منحت الشركة الحق في تقديم المزايا الناشئة عن التأمين الطبي الإلزامي وتحصيل أقساط التأمين. ولا يمكن لدولة أن تعفي نفسها من المسؤولية بموجب الاتفاقية من خلال تفويض التزاماتها إلى هيئات خاصة أو أفراد. ويجب أن يوفر القانون الوطني الضمانات الكافية ضد التجاوزات لكي يكون التدخل في الحقوق المنصوص عليها في المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان «طبقاً للقانون». في هذه القضية، خلصت المحكمة الأوروبية لحقوق الإنسان إلى أن المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان قد انتهكت لأن القانون الوطني لم يوضح بشكل كاف نطاق وطريقة ممارسة السلطة التقديرية الممنوحة لشركات التأمين بصفتها سلطات عمومية في المنازعات المتعلقة بالتأمين من أجل القيام بمراقبة شخص مؤمن بشكل سري. كما أنه لم يتضمن على وجه الخصوص الضمانات الكافية ضد التجاوزات.

**أن يحقق هدفاً مشروعا**

قد يكون الهدف المشروع عبارة عن إحدى المصالح العامة المذكورة أو حماية حقوق الآخرين وحرياتهم. وتتمثل الأهداف المشروعة التي يمكن أن تبرر التدخل وفقاً للمادة 8 (2) من الاتفاقية الأوروبية لحقوق الإنسان في مصالح الأمن الوطني والسلامة العامة أو الرفاه الاقتصادي لبلد ما، ومنع الفوضى أو الجريمة، وحماية الصحة أو الآداب العامة، وحماية حقوق الأشخاص الآخرين وحرياتهم.

مثال: في قضية «'بيك' ضد المملكة المتحدة»،[49] حاول المدعي الانتحار في الشارع بقطع شرايين معصميه، وكان غير مدرك بأن كاميرا مراقبة كانت تصوره. وبعد أن أنقذته عناصر الشرطة، التي كانت تتابع كاميرات المراقبة، سلمت التسجيل لوسائل الإعلام، التي نشرته دون إخفاء وجه المدعي. وقد رأت المحكمة الأوروبية لحقوق الإنسان أنه لا توجد أسباب وجيهة أو كافية تبرر الكشف المباشر عن اللقطات للعموم من قبل السلطات دون الحصول على موافقة المدعي أو إخفاء هويته. وخلصت المحكمة إلى أنه كان هناك انتهاك للمادة 8 من الاتفاقية الأوروبية لحقوق الإنسان.

[46] المحكمة الأوروبية لحقوق الإنسان، قضية «روتارو ضد رومانيا» [الغرفة الكبرى]، رقم 28341/95، 4 مايو 2000، الفقرة 57؛ انظر أيضاً المحكمة الأوروبية لحقوق الإنسان، قضية «جمعية التكامل الأوروبي وحقوق الإنسان وإكيمزييف ضد بلغاريا»، رقم 62540/00، 28 يونيو 2007؛ المحكمة الأوروبية لحقوق الإنسان، قضية «شيموفولوس ضد روسيا»، رقم 30194/09، 21 يونيو 2011؛ والمحكمة الأوروبية لحقوق الإنسان، قضية «فيتر ضد فرنسا»، رقم 59842/00، 31 مايو 2005.

[47] المحكمة الأوروبية لحقوق الإنسان، قضية «تايلور-سابوري ضد المملكة المتحدة»، رقم 47114/99، 22 أكتوبر 2002.

[48] المحكمة الأوروبية لحقوق الإنسان، قضية «فوكوتا-بويتش ضد سويسرا»، رقم القضية 61838/10، 18 أكتوبر 2016، الفقرة 77.

[49] المحكمة الأوروبية لحقوق الإنسان، قضية «بيك ضد المملكة المتحدة»، رقم 44647/98، 28يناير 2003، الفقرة 85.

**أن يكون ضرورياً في مجتمع ديمقراطي**

أشارت المحكمة الأوروبية لحقوق الإنسان أن «مفهوم الضرورة يعني ضمناً أن التدخل يتوافق مع حاجة اجتماعية ملحة، وعلى وجه الخصوص، أنه يتناسب مع الهدف المشروع المنشود»،[50] وعند تقييم ما إذا كان التدبير ضرورياً للاستجابة لحاجة اجتماعية ملحة، تدرس المحكمة الأوروبية لحقوق الإنسان مدى أهميته وملاءمته فيما يتعلق بالهدف المنشود. وتحقيقا لهذه الغاية، قد تأخذ بعين الاعتبار ما إذا كان التدخل يحاول معالجة مسألة إذا لم تتم معالجتها يمكن أن يكون لها تأثير ضار على المجتمع، وما إذا كان هناك دليل على أن التدخل قد يخفف من هذا التأثير الضار، وما هي وجهات النظر المجتمعية الأوسع بشأن هذه المسألة بعينها.[51] على سبيل المثال، يعد جمع الأجهزة الأمنية وتخزينها للبيانات الشخصية لأفراد معينين تبيّن أن لهم صلات بحركات إرهابية تدخلاً في حق الأفراد في احترام الحياة الخاصة، لكنه يستجيب لضرورة اجتماعية خطيرة وملحة: الأمن الوطني ومكافحة الإرهاب. وليتوافق مع معيار الضرورة، يجب أن يكون التدخل أيضاً متناسباً. ففي السوابق القضائية للمحكمة الأوروبية لحقوق الإنسان، يتم تناول التناسبية ضمن مفهوم الضرورة. وتقتضي التناسبية ألا يصل التدخل في الحقوق المحمية بموجب الاتفاقية الأوروبية لحقوق الإنسان إلى أبعد مما هو مطلوب لتحقيق الهدف المشروع المنشود. ولعل أحد العوامل المهمة التي يجب مراعاتها عند إجراء اختبار التناسبية هو نطاق التدخل، ولا سيما عدد الأشخاص المتأثرين، والضمانات أو التحفظات الموضوعة للحد من نطاقه أو آثاره الضارة على حقوق الأفراد.[52]

مثال: في قضية «'خليلي' ضد سويسرا»،[53] خلال بحث أجرته الشرطة، تبين لهذه الأخيرة أن المدعية تحمل بطاقات دعوة كتب عليها: «امرأة لطيفة وجميلة، في أواخر الثلاثين من العمر، ترغب في لقاء رجل لاحتساء مشروب أو الخروج معاً من وقت لآخر. رقم الهاتف [...]». وقد زعمت المدعية أنه بعد هذا الاكتشاف، أدخلت الشرطة اسمها في السجلات باعتبارها مومساً، وهو الأمر الذي أنكرته باستمرار. وطلبت المدعية أن تتم إزالة كلمة «مومس» من السجلات الحاسوبية للشرطة. وقد أقرت المحكمة الأوروبية لحقوق الإنسان من حيث المبدأ بأن الاحتفاظ بالبيانات الشخصية لشخص ما على أساس أن هذا الشخص قد يرتكب مخالفة أخرى قد يكون متناسباً في ظل ظروف معينة. لكن في قضية المدعية، كان الادعاء بممارسة الدعارة غير القانونية يبدو مبهما وواسعا بشكل مفرط، وغير مدعم بحقائق واقعية بما أنه لم تتم إدانتها قط بممارسة الدعارة غير القانونية، وبالتالي لا يمكن اعتبار هذا الأمر «ضرورة اجتماعية ملحة» بالمعنى الذي جاء في المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان. واعتباراً منها بأن عبء إثبات صحة البيانات المخزنة المتعلقة بالمدعية يقع على السلطات، ونظراً إلى خطورة التدخل في حقوق المدعية، قضت المحكمة بأن الإبقاء على كلمة «مومس» في ملفات الشرطة لسنوات لم يكن ضرورياً في مجتمع ديمقراطي. وخلصت المحكمة إلى أنه كان هناك انتهاك للمادة 8 من الاتفاقية الأوروبية لحقوق الإنسان.

مثال: في قضية «س. ومارير ضد المملكة المتحدة»،[54] ألقي القبض على المدعيان واتهما بارتكاب جرائم جنائية. وقد أخذت الشرطة بصماتهما وعينات من حمضهما النووي، كما هو منصوص عليه في قانون الشرطة والأدلة الجنائية. إلا أنه لم تتم إدانة المدعيان بهذه الجرائم، حيث تمت تبرئة أحدهما وإيقاف الإجراءات الجنائية في حق المدعي الثاني. غير أنه تم الاحتفاظ ببصماتهما وملفي حمضهما النووي وعيناتهما الخلوية وتخزينها من قبل الشرطة في قاعدة بيانات، كما أن التشريع الوطني سمح بالاحتفاظ بها بدون وضع مهلة محددة قابلة للتطبيق. وبينما اعتبرت المملكة المتحدة أن الاحتفاظ بالبيانات يساعد في تحديد المجرمين في المستقبل، وبالتالي سعت وراء تحقيق الهدف المشروع المتمثل في منع الجريمة والكشف عنها، اعتبرت المحكمة الأوروبية لحقوق الإنسان أن التدخل في حق المدعيين في احترام الحياة الخاصة غير مبرر، وأشارت إلى أن المبادئ الأساسية لحماية البيانات تقتضي أن يكون الاحتفاظ بالبيانات الشخصية متناسباً مع غرض الجمع وأن فترات الاحتفاظ يجب أن تكون محدودة. وأيدت المحكمة فكرة أن توسيع قاعدة البيانات لتشمل ملفات تعريف الحمض النووي الخاصة بالأشخاص المدانين إضافة إلى جميـع الأفـراد المشتبه بهم وغير المدانين، كان من الممكـن أن

[50] المحكمة الأوروبية لحقوق الإنسان، قضية «لينجر ضد السويد»، رقم 9248/81، 26 مارس 1987، الفقرة 58.

[51] فريق عمل المادة 29 المعني بحماية البيانات (2014)، رأي حول تطبيق مفهومي الضرورة والتناسبية وحماية البيانات في قطاع إنفاذ القانون، WP 211، بروكسل، 27 فبراير 2014، ص.8-7.

[52] نفس المرجع السابق، ص. 11-9.

[53] المحكمة الأوروبية لحقوق الإنسان، قضية «خليلي ضد سويسرا»، رقم 16188/07، 18 أكتوبر 2011.

[54] المحكمة الأوروبية لحقوق الإنسان، قضية «س. ومارير ضد المملكة المتحدة» [الغرفة الكبرى]، رقم 30562/04 ورقم 30566/04، 4 ديسمبر 2008.

يساهم في الكشف عن الجرائم ومنعها في المملكة المتحدة. إلا أنها «استغربت الطبيعة الشاملة والعشوائية لصلاحية الاحتفاظ»،[55] ونظراً لكون العينات الخلوية غنية بالمعلومات الوراثية والصحية، كان التدخل في حق المدعيين في الحياة الخاصة سافراً. إذ يمكن أخذ البصمات والعينات من الأشخاص الموقوفين، والاحتفاظ بها إلى أجل غير مسمى في قاعدة بيانات الشرطة، بغض النظر عن طبيعة وخطورة المخالفة، وحتى بالنسبة للجرائم البسيطة التي لا يعاقب عليها بالسجن.

علاوة على ذلك، كانت فرص نجاح الأفراد الذين تمت تبرئتهم في إزالة بياناتهم من قاعدة البيانات محدودة. وأخيراً، أولت المحكمة الأوروبية لحقوق الإنسان اهتماماً خاصاً لحقيقة أن أحد المدعين كان يبلغ 11 عاماً عند القبض عليه. فمن شأن الاحتفاظ بالبيانات الشخصية لقاصر غير مدان أن يكون بالغ الضرر نظراً لهشاشته وأهمية تطوره واندماجه في المجتمع.[56] ورأت المحكمة، بالإجماع، أن الاحتفاظ بالبيانات يشكل تدخلاً غير متناسب مع الحق في الحياة الخاصة لا يمكن اعتباره ضرورياً في مجتمع ديمقراطي.

مثال: في قضية «'لايندر' ضد السويد»،[57] قضت المحكمة الأوروبية لحقوق الإنسان بأن التدقيق السري بشأن المتقدمين لشغل مناصب ذات أهمية بالنسبة للأمن الوطني لا يتعارض في حد ذاته مع شرط الضرورة في مجتمع ديمقراطي. وقد أدت الضمانات الخاصة المنصوص عليها في القانون الوطني لحماية مصالح صاحب البيانات - على سبيل المثال، تدابير المراقبة التي ينفذها البرلمان ووزير العدل - إلى استنتاج المحكمة الأوروبية لحقوق الإنسان بأن نظام مراقبة الموظفين السويدي يستجيب لمتطلبات المادة 8 (2) من الاتفاقية الأوروبية لحقوق الإنسان. وبالنظر إلى هامش التقدير الواسع المتاح لها، كان من حق الدولة المدعى عليها أن تعتبر أنه في حالة هذا المدعي كانت لمصالح الأمن القومي الغلبة على المصالح الفردية. وخلصت المحكمة إلى أن المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان لم تنتهك.

## 2.2.1. شروط فرض قيود مشروعة بمقتضى ميثاق الحقوق الأساسية للاتحاد الأوروبي

تختلف بنية وصياغة الميثاق مقارنة بالاتفاقية الأوروبية لحقوق الإنسان. فهو لا يستخدم مفهوم التدخل في الحقوق المضمونة، ولكنه يشتمل على مقتضى بشأن القيود المفروضة على ممارسة الحقوق والحريات التي يقرها الميثاق.

ووفقاً للمادة 52 (1)، لا يتم قبول القيود المفروضة على ممارسة الحقوق والحريات المنصوص عليها في الميثاق، وبالتالي على ممارسة الحق في حماية البيانات الشخصية، إلا في الحالات التالية:

- ينص عليها في القانون؛
- تحترم جوهر الحق في حماية البيانات؛
- تخضع لمبدأ التناسبية وتعد ضرورية؛[58]
- تحقق أهداف المصلحة العامة التي يقرها الاتحاد أو تستجيب لضرورة حماية حقوق الآخرين وحرياتهم.

ونظراً لكون حماية البيانات الشخصية حقاً أساسياً متميزاً وقائماً بذاته في النظام القانوني للاتحاد الأوروبي، تكرسه المادة 8 من الميثاق، فإن أي معالجة للبيانات الشخصية في حد ذاتها تشكل تدخلاً في هذا الحق. وليس مهماً ما إذا كانت البيانات الشخصية المعنية تتعلق بالحياة الخاصة للفرد، أو بيانات حساسة، أو ما إذا كان أصحاب البيانات قد تعرضوا للمتاعب بأي شكل من الأشكال. ولكي يكون التدخل قانونياً، يجب أن يمتثل لجميع الشروط المذكورة في المادة 52 (1) من الميثاق.

[55] نفس المرجع السابق، الفقرة 119.

[56] نفس المرجع السابق، الفقرة 124.

[57] المحكمة الأوروبية لحقوق الإنسان، قضية «لايندر ضد السويد»، رقم 9248/81، 26 مارس 1987، الفقرتان 59 و67.

[58] تقييم ضرورة التدابير المقيدة للحق الأساسي في حماية البيانات، انظر: المشرف الأوروبي على حماية البيانات (2017)، «مجموعة الأدوات المتعلقة بالضرورة»، بروكسل، 11 أبريل 2017.

**التنصيص القانوني**

يجب أن ينص القانون على القيود المتعلقة بالحق في حماية البيانات الشخصية. هذا الشرط يعني ضمناً أن القيود يجب أن تستند إلى أساس قانوني يسهل الوصول إليه ويمكن توقعه، وتتم صياغته بدقة كافية لتمكين الأفراد من فهم التزاماتهم وتنظيم سلوكهم. ويجب أن يحدد الأساس القانوني بوضوح نطاق الصلاحية المخولة وطريقة ممارستها من قبل السلطات المختصة لحماية الأفراد من التدخل التعسفي. ويشبه هذا التفسير شرط «التدخل القانوني» بمقتضى السوابق القضائية للمحكمة الأوروبية لحقوق الإنسان،[59] وقد قيل إن معنى عبارة «المنصوص عليها في القانون» المستخدمة في الميثاق يجب أن يكون هو نفسه المعنى المنسوب لها فيما يتعلق بالمحكمة الأوروبية لحقوق الإنسان.[60] وتعد السوابق القضائية للمحكمة الأوروبية لحقوق الإنسان، ولا سيما مفهوم «جودة القانون» الذي طورته مع مرور السنوات، أحد الاعتبارات ذات الصلة التي يجب أن تؤخذ بالحسبان من قبل محكمة العدل التابعة للاتحاد الأوروبي عند تفسير نطاق المادة 52 (1) من الميثاق.[61]

**احترام جوهر الحق**

في النظام القانوني للاتحاد الأوروبي فإن أية قيود مفروضة على الحقوق الأساسية المحمية بموجب الميثاق يجب أن تحترم جوهر هذه الحقوق. وهذا يعني أنه لا يمكن إيجاد أي تبرير للقيود التي تصل بفعل سعة نطاقها وشدة تدخلها إلى حد تجريد حق أساسي من مغزاه الجوهري. وإذا تم المساس بجوهر الحق، يتعين عندها اعتبار القيد المفروض غير قانوني، دونما حاجة إلى القيام بمزيد من التقييم فيما إذا كان يخدم هدفاً من أهداف المصلحة العامة ويستوفي معايير الضرورة والتناسبية

مثال: تتمحور قضية «شريمز»[62] حول حماية الأفراد من نقل بياناتهم الشخصية إلى دول أخرى، ويتعلق الأمر في هذه الحالة بالولايات المتحدة. فقد تقدم السيد شريمز، وهو مواطن نمساوي كان يستخدم موقع «فيسبوك» لعدة سنوات، بشكاية لدى هيئة مراقبة حماية البيانات الإيرلندية لشجب نقل بياناته الشخصية من فرع «فيسبوك» الأيرلندي إلى شركة «فيسبوك» والخوادم الموجودة في الولايات المتحدة حيث تمت معالجتها. وقد جاء في شكايته أنه بالنظر إلى المعلومات التي تم الكشف عنها من قبل المُبلِّغ عن المخالفات الأمريكي إدوارد سنودن في 2013 بشأن أنشطة التجسس التي تقوم بها أجهزة المراقبة الأمريكية، لم يوفر القانون ولا الممارسة في الولايات المتحدة حماية كافية للبيانات الشخصية المنقولة إلى الأراضي الأمريكية. وقد كشف سنودن بأن وكالة الأمن القومي قامت باختراق خوادم شركات من قبيل «فيسبوك» بشكل مباشر، وكان بإمكانها قراءة المحتوى والدردشات والرسائل الخاصة. لقد ارتكزت عمليات نقل البيانات إلى الولايات المتحدة على قرار ملائمة تبنته المفوضية سنة 2000 ، حيث سمح هذا القرار بإجراء عمليات نقل البيانات إلى شركات أمريكية أشهدت على نفسها بأنها ستسهر على حماية البيانات الشخصية الواردة من الاتحاد الأوروبي والامتثال لما يسمى بـ «مبادئ الملاذ الآمن». وعندما عُرضت القضية على محكمة العدل التابعة للاتحاد الأوروبي، بتت هذه الأخيرة في صحة قرار المفوضية استناداً إلى الميثاق. وقد ذكرت بأن حماية الحقوق الأساسية في الاتحاد الأوروبي تتطلب فرض استثناءات وقيود على تلك الحقوق لتطبيقها فقط بما تقتضيه الضرورة. وقد اعتبرت محكمة العدل التابعة للاتحاد الأوروبي أن التشريع الذي يسمح للسلطات العامة بالوصول، بشكل عام، إلى محتوى الاتصالات الإلكترونية «يضر بجوهر الحق الأساسي في احترام الحياة الخاصة، على النحو الذي تضمنه المادة 7 من الميثاق».

وقد يصبح هذا الحق بلا معنى إذا تم السماح للسلطات العامة الأمريكية بالوصول إلى الاتصالات كيفما شاءت، دون أي مبرر موضوعي قائم على اعتبارات محددة تتعلق بالأمن القومي أو منع الجريمة وتخص فرداً معيناً، ودون أن تكون ممارسات المراقبة هذه مصحوبة بضمانات مناسبة ضد الشطط في استعمال السلطة.

[59] المشرف الأوروبي على حماية البيانات (2017)، «مجموعة الأدوات المتعلقة بالضرورة»، 11 أبريل 2017، ص. 4؛ انظر أيضاً محكمة العدل التابعة للاتحاد الأوروبي، رأي المحكمة 15/1 (الغرفة الكبرى)، 26 يوليو 2017.

[60] محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان رقم C-203/15 ورقم C-698/15، قضية «تيلي 2 السويد المحدودة' ضد الإدارة السويدية للبريد والاتصالات»، وقضية «وزير الدولة المكلف بالشؤون الداخلية ضد توم واتسون وبيتر برايس وجيفري لويس»، رأي النائب العام سوغماندسفارد أوي، الصادر في 19 يوليو 2016، الفقرة 140.

[61] محكمة العدل التابعة للاتحاد الأوروبي، رقم C-70/10، قضية «شركة المساهمة 'سكارليت إكستانديد' ضد الشركة البلجيكية للمؤلفين والملحنين والموزعين الموسيقيين»، رأي النائب العام كروز فيالون، الصادر في 14 أبريل 2011، الفقرة 100.

[62] محكمة العدل التابعة للاتحاد الأوروبي، رقم C-362/14، قضية «ماكسيميليان شريمز ضد مفوض حماية البيانات» [الغرفة الكبرى]، 6 أكتوبر 2015.

علاوة على ذلك، لاحظت محكمة العدل عدم توافق «التشريع [الذي] لا ينص على أي إمكانية للجوء الفرد إلى سبل الانتصاف القانونية من أجل الوصول إلى البيانات الشخصية المتعلقة به أو تصحيحها أو محوها» مع الحق الأساسي في الحماية القضائية الفعالة (المادة 47 من الميثاق). وبالتالي، فإن قرار الملاذ الآمن قد فشل في ضمان الولايات المتحدة لمستوى حماية الحقوق الأساسية مساو لما يضمنه الاتحاد الأوروبي بمقتضى الأمر التوجيهي الذي يقرأ في ضوء الميثاق. وبذلك، قررت محكمة العدل التابعة للاتحاد الأوروبي إبطال القرار.[63]

مثال: في قضية «ديجيتال رايتس آيرلاند»،[64] نظرت محكمة العدل التابعة للاتحاد الأوروبي في مدى توافق الأمر التوجيهي رقم2006/24/EC (الأمر التوجيهي المتعلق بالاحتفاظ بالبيانات) مع المادتين 7 و8 من الميثاق. حيث ألزم الأمر التوجيهي مقدمي خدمات الاتصالات الإلكترونية بالاحتفاظ ببيانات الحركة والموقع لمدة تتراوح بين ستة أشهر على الأقل و24 شهراً كحد أقصى، وبالسماح للهيئات الوطنية المختصة بالوصول إلى تلك البيانات بغرض منع الجرائم الخطيرة والتحقيق فيها والكشف عنها ومتابعة مرتكبيها. ولم يسمح الأمر التوجيهي بالاحتفاظ بمحتوى الاتصالات الإلكترونية. وقد أشارت محكمة العدل التابعة للاتحاد الأوروبي إلى أن البيانات التي يتعين على مقدمي الخدمات الاحتفاظ بها وفقاً للأمر التوجيهي شملت البيانات اللازمة لتتبع وتحديد مصدر الاتصال ووجهته وتاريخه ووقته ومدته والرقم المتصل والأرقام المتصَل بها وعناوين بروتوكول الإنترنت. إن هذه البيانات، «في مجملها، قد تسمح باستخلاص استنتاجات دقيقة للغاية بشأن الحياة الخاصة للأشخاص الذين تم الاحتفاظ ببياناتهم، مثل عادات الحياة اليومية، وأماكن الإقامة الدائمة أو المؤقتة، والتحركات اليومية أو غيرها، والأنشطة التي يتم القيام بها والعلاقات الاجتماعية لهؤلاء الأشخاص والبيئات الاجتماعية التي يرتادونها».

وبالتالي، فإن الاحتفاظ بالبيانات الشخصية بموجب الأمر التوجيهي شكل تدخلاً خطيراً جداً في حقي الخصوصية وحماية البيانات الشخصية. غير أن محكمة العدل اعتبرت أن التدخل لم يؤثر سلباً على جوهر تلك الحقوق. وفيما يتعلق بالحق في الخصوصية، لم يتم المساس بجوهره لأن الأمر التوجيهي لم يسمح بمعرفة محتوى الاتصالات الإلكترونية، كما لم يتم المساس بجوهر الحق في حماية البيانات الشخصية، حيث ألزم الأمر التوجيهي مقدمي خدمات الاتصالات الإلكترونية باحترام مبادئ معينة لحماية البيانات وأمن البيانات وتفعيل التدابير التقنية والتنظيمية المناسبة لهذا الغرض.

### الضرورة والتناسبية

تنص المادة 52 (1) من الميثاق على أنه لا يجوز وضع قيود على ممارسة الحقوق والحريات الأساسية التي يقرها الميثاق إلا إذا اقتضت الضرورة ذلك، مع مراعاة مبدأ التناسبية.

وقد يكون التقييد **ضرورياً** إذا كانت هناك حاجة لاعتماد تدابير لتحقيق هدف المصلحة العامة المنشود - ولكن الضرورة، كما تفسرها محكمة العدل التابعة للاتحاد الأوروبي، كذلك تعني ضمناً أن التدابير المعتمدة يجب أن تكون أقل تدخلاً مقارنة بالخيارات الأخرى المتاحة لتحقيق نفس الهدف. وبالنسبة للقيود المفروضة على حقي احترام الحياة الخاصة وحماية البيانات الشخصية، تستند محكمة العدل التابعة للاتحاد الأوروبي لمعيار الضرورة الصارم، معتبرة أن «الاستثناءات والقيود يجب أن تنطبق فقط بما تقتضيه الضرورة القصوى». وإذا تم اعتبار التقييد ضرورة قصوى، فهذا الأمر يستدعي أيضاً تقييم ما إذا كان متناسباً.

تعني **التناسبية** أن المزايا الناتجة عن التقييد يجب أن تفوق الأضرار التي يسببها الأخير فيما يتعلق بممارسة الحقوق الأساسية المعنية.[65] ولتقليل الأضرار والمخاطر التي تهدد التمتع بالحق في الخصوصية والحق في حماية البيانات، من المهم أن تحمل القيود معها ضمانات مناسبة.

---

[63] إن قرار محكمة العدل التابعة للاتحاد الأوروبي الخاص بإبطال قرار المفوضية EC/520/2000 كان يستند أيضاً إلى أسس أخرى سيتم تناولها في أجزاء أخرى من هذا الدليل. الجدير بالذكر أن محكمة العدل اعتبرت أن القرار قيد بشكل غير قانوني صلاحيات الهيئات الإشرافية الوطنية المعنية بحماية البيانات. إضافة إلى ذلك، افتقر الأفراد في ظل نظام الملاذ الآمن إلى سبل الانتصاف القضائي في حال رغبتهم في الوصول إلى البيانات الشخصية المتعلقة بهم و/أو تصحيحها أو محوها. وبالتالي، فإنه قد تم المس بجوهر الحق الأساسي في الحماية القضائية الفعالة، المنصوص عليه في المادة 47 من الميثاق.

[64] محكمة العدل التابعة لمحكمة للاتحاد الأوروبي، القضيتان المضمومتان رقم C-293/12 و C-594/1، قضية «شركة 'ديجيتال رايتس آيرلاند' المحدودة ضد وزير الاتصالات والموارد البحرية والطبيعية وآخرين، وضد حكومة مقاطعة كيرنتن وآخرين» [الغرفة الكبرى]، 8 أبريل 2014.

[65] المشرف الأوروبي على حماية البيانات، «مجموعة الأدوات المتعلقة بالضرورة»، ص. 5.

مثال: في قضية «شركة فولكر وماركوس تشيكه»،[66] خلصت محكمة العدل التابعة للاتحاد الأوروبي إلى أنه من خلال فرض نشر البيانات المتعلقة بكل شخص طبيعي مستفيد من دعم بعض الصناديق الفلاحية دون تمييز مبني على معايير مناسبة، مثل الفترات التي تلقى فيها هؤلاء الأشخاص هذه المساعدة ووتيرتها وطبيعتها وقدرها، فإن المجلس والمفوضية قد تجاوزا القيود التي يفرضها مبدأ التناسبية.

لذلك، تبين لمحكمة العدل التابعة للاتحاد الأوروبي أنه من الضروري القضاء ببطلان بعض مقتضيات لائحة المجلس (الجماعة الأوروبية) رقم 1290/2005 والقضاء ببطلان اللائحة رقم 259/2008 برمتها.[67]

مثال: في قضية «ديجيتال رايتس آيرلاند»، اعتبرت محكمة العدل التابعة للاتحاد الأوروبي أن التدخل في الحق في الخصوصية الناتج عن الأمر التوجيهي المتعلق بالاحتفاظ بالبيانات لم يمس بجوهر هذا الحق لأنه كان يحظر الاحتفاظ بمحتوى الاتصالات الإلكترونية. ومع ذلك، فقد خلصت إلى أن الأمر التوجيهي لا يتوافق مع المادتين 7 و8 من الميثاق، وقضت ببطلانه. ونظراً لأن بيانات الحركة والموقع، إذا جمعت وتم النظر إليها في مجملها، يمكن أن تحلّل وتعطي صورة مفصلة عن حياة الأفراد الخاصة، فقد شكّل ذلك تدخلاً خطيراً في هذه الحقوق. وقد أخذت محكمة العدل بعين الاعتبار أن الأمر التوجيهي يقتضي الاحتفاظ بجميع البيانات الوصفية المتعلقة بالهاتف الثابت والهاتف المحمول والوصول إلى الإنترنت والبريد الإلكتروني والاتصال الهاتفي عبر الإنترنت بشكل ينطبق على جميع وسائل الاتصال الإلكتروني - التي ينتشر استخدامها على نطاق واسع في حياة الناس اليومية. ومن الناحية العملية، فقد شكل الأمر التوجيهي تدخلاً أثر على جميع سكان أوروبا. وبالنظر إلى حجم هذا التدخل وخطورته، ترى محكمة العدل التابعة للاتحاد الأوروبي أنه لا يمكن تبرير الاحتفاظ ببيانات الحركة والموقع إلا لغرض مكافحة الجرائم الخطيرة. إضافة إلى ذلك، لم يضع الأمر التوجيهي أي معايير موضوعية من شأنها أن تضمن اقتصار وصول السلطات الوطنية المختصة على ما هو ضروري من البيانات المحتفظ بها، كما أنه لم يتضمن الشروط الموضوعية والإجرائية التي تنظم وصول السلطات الوطنية إلى البيانات المحتفظ بها واستخدامها، والتي لم يتم إخضاعها لمراجعة مسبقة من قبل محكمة أو هيئة مستقلة أخرى.

وتوصلت محكمة العدل التابعة للاتحاد الأوروبي إلى استنتاج مماثل في القضيتين المضمومتين «تيلي 2 السويد المحدودة' ضد الإدارة السويدية للبريد والاتصالات» و«وزير الدولة المكلف بالشؤون الداخلية ضد توم واتسون وآخرين»،[69] وتتعلق هذه القضايا بالاحتفاظ ببيانات الحركة وبيانات الموقع «لجميع المشتركين والمستخدمين المسجلين وجميع وسائل الاتصال الإلكتروني إلى جانب البيانات الوصفية» دون «تمييز أو تقييد أو استثناء وفقاً للهدف المنشود»،[70] وفي القضية قيد النظر، لا يعد كون الشخص مرتبطاً بشكل مباشر أو غير مباشر بجرائم جنائية خطيرة، أو أن اتصالاته متعلقة بالأمن الوطني، شرطاً للاحتفاظ ببياناته. وفي ضوء عدم وجود الصلة المطلوبة بين البيانات المحتفظ بها وتهديد الأمن العام أو قيود على الفترة الزمنية أو المنطقة الجغرافية، خلصت محكمة العدل التابعة للاتحاد الأوربي إلى أن التشريعات الوطنية تجاوزت حدود ما كان ضرورياً لغرض مكافحة الجريمة الخطيرة.[71]

---

[66] محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان رقم C-92/09 وC-93/09، «شركة 'فولكر وماركوس تشيكه' وهارتموت أيفرت ضد ولاية هيسن» [الغرفة الكبرى]، 9 نوفمبر 2010، الفقرتان 89 و86.

[67] لائحة المجلس (الجماعة الأوروبية) رقم 1290/2005 المؤرخة في 21 يونيو 2005 بشأن تمويل السياسة الفلاحية المشتركة، الجريدة الرسمية L 209 2005 OJ؛ لائحة المفوضية (الجماعة الأوروبية) رقم 259/2008 المؤرخة في 18 مارس 2008 التي تحدد قواعد مفصلة لتطبيق لائحة المجلس (الجماعة الأوروبية) رقم 1290/2005 فيما يتعلق بنشر المعلومات عن المستفيدين من الأموال المتأتية من الصندوق الأوروبي للضمان الفلاحي (EAGF) والصندوق الفلاحي الأوروبي للتنمية القروية(EAFRD) ، الجريدة الرسمية L 76 2008 OJ.

[68] محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان رقم C-293/12 وC-594/12، «شركة 'ديجيتال رايتس آيرلاند' المحدودة ضد وزير الاتصالات والموارد البحرية والطبيعية وآخرين، وضد حكومة مقاطعة كيرنتن وآخرين» [الغرفة الكبرى]، 8 أبريل 2014، الفقرة 39.

[69] محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان رقم C-203/15 وC-698/15، قضية «'تيلي 2 السويد المحدودة' ضد الإدارة السويدية للبريد والاتصالات»، وقضية «وزير الدولة المكلف بالشؤون الداخلية ضد توم واتسون وآخرين» [الغرفة الكبرى]، 21 ديسمبر 2016، الفقرتان 106-105.

[70] نفس المرجع السابق، الفقرة 105.

[71] نفس المرجع السابق، الفقرة 107.

فيما يتعلق بالضرورة، يتبع المشرف الأوروبي على حماية البيانات مقاربة مماثلة في «مجموعة الأدوات المتعلقة بالضرورة» الخاصة به.[72] وتهدف مجموعة الأدوات هذه إلى المساعدة على تقييم مدى امتثال التدابير المقترحة لقانون الاتحاد الأوروبي المتعلق بحماية البيانات. وقد تم إعدادها لدعم صناع السياسات والمشرعين في الاتحاد الأوروبي المسؤولين عن إعداد أو افتحاص الإجراءات التي تنطوي على معالجة للبيانات الشخصية وعلى تقييد للحق في حماية البيانات الشخصية والحقوق والحريات الأخرى المنصوص عليها في الميثاق.

**أهداف المصلحة العامة**

لكي يكون التقييد على ممارسة الحقوق المنصوص عليها في الميثاق مبرراً، يجب أن يستجيب كذلك فعليا لأهداف المصلحة العامة التي يقرها الاتحاد أو الحاجة إلى حماية حقوق الأشخاص الآخرين وحرياتهم. وفيما يتعلق بضرورة حماية حقوق الآخرين وحرياتهم، غالباً ما يتفاعل الحق في حماية البيانات الشخصية مع حقوق أساسية أخرى. ويقدم الجزء 3.1 تحليلاً مفصلاً لمثل هذه التفاعلات. أما بالنسبة لأهداف المصلحة العامة، فهي تشمل الأهداف العامة للاتحاد الأوروبي التي تم التأكيد عليها في المادة 3 من معاهدة الاتحاد الأوروبي، مثل تعزيز السلام ورفاهية شعوب الاتحاد والعدالة الاجتماعية والحماية وخلق فضاء ينعم بالحرية والأمن والعدالة حيث تكون حرية حركة الأشخاص مضمونة، وذلك بالاقتران مع التدابير المناسبة لمنع الجريمة ومكافحتها، وكذلك الأهداف والمصالح الأخرى التي تكفلها مقتضيات محددة من المعاهدات.[73] في هذا الصدد، تفصل اللائحة العامة لحماية البيانات بشكل أكبر المادة 52 (1) من الميثاق؛ إذ تحدد المادة 23 (1) من اللائحة سلسلة من أهداف المصلحة العامة التي تعتبر مشروعة لتقييد حقوق الأفراد، شريطة أن يحترم التقييد جوهر الحق في حماية البيانات الشخصية وأن يكون ضرورياً ومتناسباً. ويعد الأمن والدفاع الوطنيين، ومنع الجريمة، وحماية المصالح الاقتصادية والمالية المهمة للاتحاد الأوروبي أو الدول الأعضاء، والصحة العامة، والضمان الاجتماعي من بين أهداف المصلحة العامة المشار إليها في اللائحة.

من المهم تحديد وشرح هدف المصلحة العامة الذي يسعى إليه التقييد بشكل مفصل بما يكفي، حيث سيتم تقييم ضرورة التقييد بناء على هذه الأساس. فالوصف الواضح والتفصيلي لهدف التقييد والتدابير المقترحة مهم لتقييم ما إذا كان ضرورياً.[74] هذا ويرتبط الهدف المنشود ارتباطاً وثيقاً بضرورة التقييد وتناسبه.

مثال: تتعلق قضية «'شوارتز' ضد مدينة بوخوم»[75] بالقيود المفروضة على الحق في احترام الحياة الخاصة والحق في حماية البيانات الشخصية الناشئة عن أخذ البصمات وتخزينها عند إصدار سلطات الدول الأعضاء جوازات السفر.[76] وقد تقدم المدعي بطلب لمدينة بوخوم بغرض الحصول على جواز سفر، لكنه رفض أخذ بصماته؛ وعلى إثر ذلك، رفضت المدينة طلبه. فقام برفع دعوى أمام محكمة ألمانية للحصول على جواز سفر دون أخذ البصمات. وقد أحالت المحكمة الألمانية القضية إلى محكمة العدل التابعة للاتحاد الأوروبي، متسائلة عما إذا كانت المادة 1 (2) من اللائحة2252/2004 المتعلقة بمعايير الخصائص الأمنية والقياسات الحيوية في جوازات السفر ووثائق السفر الصادرة عن الدول الأعضاء تعتبر صالحة.

وقد أشارت محكمة العدل التابعة للاتحاد الأوروبي إلى أن بصمات الأصابع **هي بمثابة بيانات شخصية**، لأنها تتضمن موضوعياً معلومات فريدة عن الأفراد تسمح بتحديد هويتهم بدقة، فيما تعتبر عملية أخذ بصمات الأصابع وتخزينها عملية معالجة. هذه المعالجة، التي تنظمها المادة 1 (2) من اللائحة رقم 2252/2004، تشكل تهديداً للحق في احترام الحياة الخاصة والحق في حماية البيانات الشخصية.[77] ومع ذلك، تسمح المادة 52 (1) من الميثاق بفرض قيود على ممارسة هذين الحقين، طالما أن هذه القيود منصوص عليها في القانون، وتحترم جوهر تلك الحقوق، وتعتبر ضرورية، بما يتوافق مع مبدأ التناسبية، وتستجيب فعلاً لأهداف المصلحة العامة التي أقرها الاتحاد أو للحاجة إلى حماية حقوق الآخرين وحرياتهم.

في هذه القضية، أشارت محكمة العدل التابعة للاتحاد الأوروبي أولاً إلى أنه يجب اعتبار التقييد الناشئ عن أخذ البصمات وتخزينها عند إصدار جوازات السفر **منصوصاً عليه في القانون** لأن هذه العمليات منصوص عليها في المادة 1 (2) من اللائحة رقم 2252/2004. وثانياً، أن هذه

[71] نفس المرجع السابق، الفقرة 107.
[72] المشرف الأوروبي على حماية البيانات، «مجموعة الأدوات المتعلقة بالضرورة»، بروكسل، 11 أبريل 2017.
[73] التفسيرات المتعلقة بميثاق الحقوق الأساسية(303/02/2007 C) ، الجريدة الرسمية 303 C 2007 ،0J، ص.35-17.
[74] المشرف الأوروبي على حماية البيانات، «مجموعة الأدوات المتعلقة بالضرورة»، بروكسل، 11 أبريل 2017، ص. 4.
[75] محكمة العدل التابعة للاتحاد الأوروبي، رقم C-291/12، قضية «مايكل شوارتز ضد مدينة بوخوم»، 17 أكتوبر 2013.
[76] نفس المرجع السابق، الفقرات من 33 إلى 36.
[77] نفس المرجع السابق، الفقرات من 27 إلى 30.

اللائحة قد تم تصميمها لمنع تزوير جوازات السفر واستخدامها بطريقة احتيالية. وبالتالي، فإن المادة 1 (2) موجودة لمنع الدخول غير القانوني إلى الاتحاد الأوروبي، ضمن جملة من الأمور، وبالتالي تسعى إلى تحقيق هدف المصلحة العامة الذي يقره الاتحاد الأوروبي. وثالثاً، أنه لم يتضح من الأدلة المتاحة لمحكمة العدل التابعة للاتحاد الأوروبي، كما لم يُزعم، أن القيود المفروضة على ممارسة هذين الحقين في هذه القضية لم تحترم جوهر الحقين. ورابعاً، أن تخزين بصمات الأصابع على أحد وسائط التخزين الآمنة للغاية على النحو المنصوص عليه في هذا المقتضى يتطلب تكنولوجيا متطورة. ومن المرجح أن يقلل هذا التخزين من مخاطر تزوير جوازات السفر ويسهل عمل السلطات المسؤولة عن التحقق من صحة جوازات السفر على حدود الاتحاد الأوروبي. إن كون هذه الطريقة غير موثوق بها بالكامل ليس حاسماً. إذ على الرغم من أنها لا تمنع قبول جميع الأشخاص غير المرخص لهم، فهي كافية لتقليل احتمالية هذا القبول بشكل كبير. وفي ضوء ما سبق، اعتبرت محكمة العدل التابعة للاتحاد الأوروبية أن أخذ وتخزين بصمات الأصابع المشار إليهما في المادة 1 (2) من اللائحة رقم 2252/2004 كانا متناسبين مع تحقيق الأهداف التي تسعى إليها تلك اللائحة، إلى جانب الهدف المتمثل في منع الدخول غير القانوني إلى الاتحاد الأوروبي.[78]

قامت محكمة العدل التابعة للاتحاد الأوروبي بعد ذلك بتقييم ما إذا كانت هذه المعالجة **ضرورية**، مشيرةً إلى أن الإجراء قيد النظر لا يتعدى أخذ البصمات لإصبعين لا غير، وأنه علاوةً على ذلك تم على مرأى من الجميع عموماً، وهو ما يعني أن هذه العملية ليست ذات طابع حميمي، كما أنها لا تسبب أي إزعاج جسدي أو نفسي للشخص المعني، فهي شبيهة بالتقاط صورة لوجه هذا الشخص. وتجدر الإشارة أيضاً إلى أن البديل الحقيقي الوحيد لأخذ بصمات الأصابع والذي تمت الإشارة إليه أمام المحكمة هو فحص قزحية العين. ولم يشر أي شيء في ملف القضية المعروض على المحكمة إلى أن هذا الإجراء من شأنه أن يكون أقل تدخلاً في الحقوق المنصوص عليها في المادتين 7 و8 من الميثاق من أخذ بصمات الأصابع. علاوة على ذلك، فيما يتعلق بفعالية هاتين الطريقتين، معروف أن تقنية التعرف على قزحية العين ليست بنفس تقدم تقنية التعرف على بصمات الأصابع، كما أن تكلفتها تفوق بكثير تكلفة مقارنة بصمات الأصابع. ولهذا السبب، فهي أقل ملاءمة للاستخدام العام. وبناءً على ذلك، لم يتم إخطار محكمة العدل التابعة للاتحاد الأوروبي بأي تدابير من شأنها أن تكون فعالة بما فيه الكفاية في المساعدة على تحقيق هدف الحماية من الاستخدام الاحتيالي لجوازات السفر، و في نفس الوقت أقل تهديداً للحقوق المنصوص عليها في المادتين 7 و8 من الميثاق مقارنة مع التدابير المستمدة من الطريقة القائمة على استخدام بصمات الأصابع.[79].

وقد أشارت محكمة العدل التابعة للاتحاد الأوروبي إلى أن المادة 4 (3) من اللائحة رقم 2252/2004 تنص صراحة على أنه لا يجوز استخدام بصمات الأصابع إلا للتحقق من صحة جواز السفر وهوية حامله، في حين أن المادة 1 (2) من اللائحة لا تنص على تخزين بصمات الأصابع ماعدا داخل جواز السفر نفسه الذي يخص حامله وحده. وبالتالي، لم تقدم اللائحة أساساً قانونيا للتخزين المركزي للبيانات التي يتم جمعها بموجبها أو لاستخدام هذه البيانات لأغراض أخرى غير منع الدخول غير القانوني إلى الاتحاد الأوروبي.[80] وفي ضوء جميع الاعتبارات السابقة، خلصت المحكمة إلى أن البت في السؤال المحال إليها لم يكشف عن أي شيء يمكن أن يؤثر على صلاحية المادة 1 (2) من اللائحة رقم 2252/2004.

### العلاقة بين الميثاق والاتفاقية الأوروبية لحقوق الإنسان

على الرغم من الاختلاف في صياغتهما، فإن شروط القيود القانونية المفروضة على الحقوق الواردة في المادة 52 (1) من الميثاق تذكرنا بالمادة 8 (2) من الاتفاقية الأوروبية لحقوق الإنسان المتعلقة بالحق في احترام الحياة الخاصة. وفي السوابق القضائية الخاصة بمحكمة العدل التابعة للاتحاد لأوروبي والمحكمة الأوروبية لحقوق الإنسان، غالبا ما تشير كل محكمة إلى أحكام الأخرى، كجزء من الحوار المستمر بين المحكمتين للبحث عن تفسير متسق لقواعد حماية البيانات. وتنص المادة 52 (3) من الميثاق على أنه «بقدر ما يحتوي هذا الميثاق على حقوق تتوافق مع الحقوق التي تضمنها اتفاقية حماية حقوق الإنسان والحريات الأساسية، فإن معنى ونطاق هذه الحقوق يجب أن يكون هو مطابقاً لما تنص عليه الاتفاقية المذكورة «. ومع ذلك، فإن المادة 8 من الميثاق لا تتوافق بشكل مباشر مع أي مادة في الاتفاقية الأوروبية لحقوق الإنسان.[81] وتتعلق المادة 52 (3) من الميثاق بمحتوى ونطاق الحقوق التي يحميها كل نظام قانوني، وليس بشروط تقييدها. ومع ذلك، في ضوء السياق الأوسع للحوار والتعاون بين المحكمتين، يمكن أن تأخذ محكمة العدل التابعة للاتحاد الأوروبي بعين الاعتبار في تحليلاتها معايير التقييد القانوني المنصوص عليها في المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان، كما تفسرها المحكمة الأوروبية لحقوق الإنسان.

[78] نفس المرجع السابق، الفقرات من 35 إلى 45.

[79] محكمة العدل التابعة للاتحاد الأوروبي، رقم C-291/12، قضية «مايكل شوارتز ضد مدينة بوخوم»، 17 أكتوبر 2013، الفقرات من 46 إلى 53.

[80] نفس المرجع السابق، الفقرات من 56 إلى 61.

[81] المشرف الأوروبي على حماية البيانات(2017) ، «مجموعة الأدوات المتعلقة بالضرورة»، بروكسل، 11 أبريل 2017، ص. 6.

ويُعد السيناريو المعاكس ممكناً أيضاً، وهو الذي قد تستند بموجبه المحكمة الأوروبية لحقوق الإنسان إلى شروط التقييد المشروع بمقتضى ميثاق الحقوق الأساسية للاتحاد الأوروبي. على أي حال، ينبغي أيضاً الأخذ في الاعتبار أنه لا يوجد في الاتفاقية الأوروبية لحقوق الإنسان أي مادة مكافئة تماماً للمادة 8 من الميثاق تشير إلى حماية البيانات الشخصية، ولا سيما إلى حقوق صاحب البيانات، والأسس المشروعة للمعالجة، والإشراف من طرف هيئة مستقلة. هذا ويمكن إيجاد بعض مكونات المادة 8 من الميثاق ضمن السوابق القضائية للمحكمة الأوروبية لحقوق الإنسان التي تم تطويرها على ضوء المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان وبعلاقة مع الاتفاقية 108 [82] ويضمن هذا الارتباط وجود إلهام متبادل بين محكمة العدل التابعة للاتحاد الأوروبي والمحكمة الأوروبية لحقوق الإنسان بشأن المسائل المتعلقة بحماية البيانات.

## 3.1. التفاعل مع باقي الحقوق والمصالح المشروعة

### النقاط الرئيسية

- غالباً ما يتفاعل الحق في حماية البيانات مع حقوق أخرى، مثل حرية التعبير والحق في تلقي المعلومات وإرسالها.
- غالباً ما يكون هذا التفاعل متناقضاً: في حين توجد مواقف يتعارض فيها الحق في حماية البيانات الشخصية مع حق معين، هناك أيضاً حالات يضمن فيها الحق في حماية البيانات الشخصية بشكل فعال احترام نفس ذلك الحق. هذا هو الحال مثلاً بالنسبة لحرية التعبير، بالنظر إلى أن السرية المهنية هي أحد مكونات الحق في احترام الحياة الخاصة.
- تعد الحاجة إلى حماية حقوق وحريات الآخرين أحد المعايير المستخدمة لتقييم التقييد القانوني للحق في حماية البيانات الشخصية.
- عندما تكون هناك حقوق مختلفة على المحك، يجب على المحاكم إجراء عملية موازنة للتوفيق بينها.
- تقتضي اللائحة العامة لحماية البيانات من الدول الأعضاء التوفيق بين الحق في حماية البيانات الشخصية من جهة وحرية التعبير والإعلام من جهة أخرى.
- يمكن أن تتبنى الدول الأعضاء أيضاً قواعد محددة في القانون الوطني للتوفيق بين الحق في حماية البيانات الشخصية من جهة ووصول الجمهور إلى الوثائق الرسمية والتزامات السرية المهنية من جهة أخرى.

إن الحق في حماية البيانات الشخصية ليس حقاً مطلقاً؛ وقد تم تفصيل شروط التقييد القانوني لهذا الحق أعلاه. من بين معايير القيود القانونية على الحقوق المعترف بها بموجب كل من قانون مجلس أوروبا وقانون الاتحاد الأوروبي أن التدخل في حماية البيانات ضروري لحماية حقوق الآخرين وحرياتهم. وقد ذكرت كل من المحكمة الأوروبية لحقوق الإنسان ومحكمة العدل التابعة للاتحاد الأوروبي مراراً وتكراراً في الحالات التي تفاعلت فيها حماية البيانات مع حقوق أخرى أن إجراء الموازنة مع الحقوق الأخرى أمر ضروري عند تطبيق وتفسير المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان والمادة 8 من ميثاق الحقوق الأساسية للاتحاد الأوروبي.[83] ستوضح العديد من الأمثلة المهمة كيفية تحقيق هذا التوازن.

بالإضافة إلى الموازنة التي تقوم بها هذه المحاكم، يجوز للدول، إذا لزم الأمر، اعتماد تشريعات للتوفيق بين الحق في حماية البيانات الشخصية والحقوق الأخرى. لهذا السبب، تنص اللائحة العامة لحماية البيانات على عدد من مجالات الاستثناءات الوطنية.

فيما يتعلق بحرية التعبير، تقتضي اللائحة العامة لحماية البيانات من الدول الأعضاء التوفيق، بموجب القانون، بين «الحق في حماية البيانات الشخصية وفقاً لهذه اللائحة من جهة والحق في حرية التعبير والمعلومات، بما في ذلك المعالجة للأغراض الصحفية وأغراض التعبير الأكاديمي أو الفني أو الأدبي».[84] ويمكن للدول الأعضاء أيضاً اعتماد قوانين للتوفيق بين حماية البيانات ووصول الجمهور إلى الوثائق الرسمية والتزامات السرية المهنية المحمية كشكل من أشكال الحق في احترام الحياة الخاصة.[85]

---

[82] توضيحات بشأن ميثاق الحقوق الأساسية للاتحاد الأوروبي (C 303/02/2007)، المادة 8.

[83] المحكمة الأوروبية لحقوق الإنسان، قضية فون هانوفر ضد ألمانيا (رقم 2)، [الغرفة الكبرى]، رقمي 08/40660 و08/60641,7 فبراير 2012؛ محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-468/10 وC-469/10، الرابطة الوطنية لمؤسسات الائتمان المالي (ASNEF) واتحاد التجارة الإلكترونية والتسويق المباشر (FECEMD) ضد إدارة الدولة، 24 نوفمبر 2011، الفقرة 48؛ محكمة العدل التابعة للاتحاد الأوروبي القضية رقم C-275/06، منتجو الموسيقى إسبانيا (بروموسيكاي) ضد تيليفونيكا إسبانيا (شركة ذات مساهم واحد) [الغرفة الكبرى]، 29 يناير 2008، الفقرة 68.

[84] اللائحة العامة لحماية البيانات، المادة 85.

[85] نفس المرجع السابق، المواد 86 إلى 90.

## 1.3.1. حرية التعبير

يُعد الحق في حرية التعبير أحد الحقوق التي تتفاعل إلى حد كبير مع الحق في حماية البيانات.

إن حرية التعبير محمية بموجب المادة 11 من ميثاق الحقوق الأساسية للاتحاد الأوروبي ('حرية التعبير والمعلومات'). ويشمل هذا الحق «حرية اعتناق الآراء وتلقي ونقل المعلومات والأفكار دون تدخل من السلطة العامة ودون أي اعتبار للحدود». وتحمي حرية المعلومات، وفقاً لكل من المادة 11 من ميثاق الحقوق الأساسية للاتحاد الأوروبي والمادة 10 من الاتفاقية الأوروبية لحقوق الإنسان، ليس فقط الحق في نقل المعلومات ولكن أيضاً في تلقيها.

يجب أن تتوافق القيود المفروضة على حرية التعبير مع المعايير المنصوص عليها في المادة 52 (1) من ميثاق الحقوق الأساسية للاتحاد الأوروبي، الموصوفة أعلاه. بالإضافة إلى ذلك، تناظر المادة 11 من ميثاق الحقوق الأساسية للاتحاد الأوروبي المادة 10 من الاتفاقية الأوروبية لحقوق الإنسان. وعملاً بالمادة 52 (3) من ميثاق الحقوق الأساسية للاتحاد الأوروبي، بقدر ما تحتوي على حقوق تتوافق مع الحقوق التي تضمنها الاتفاقية الأوروبية لحقوق الإنسان، «يجب أن يكون معنى ونطاق تلك الحقوق هو نفسه الذي حددته الاتفاقية المذكورة». وبالتالي، فإن القيود التي يمكن فرضها قانونياً على الحق الذي تضمنه المادة 11 من ميثاق الحقوق الأساسية للاتحاد الأوروبي لا يمكن أن تتجاوز تلك المنصوص عليها في المادة 10 (2) من الاتفاقية الأوروبية لحقوق الإنسان - أي يجب أن ينص عليها القانون وأن تكون ضرورية في مجتمع ديمقراطي «لحماية [...] سمعة أو حقوق الآخرين». وتشمل هذه الحقوق، على وجه الخصوص، الحق في احترام الحياة الخاصة والحق في حماية البيانات الشخصية.

إن العلاقة بين حماية البيانات الشخصية وحرية التعبير محكومة بالمادة 85 من اللائحة العامة لحماية البيانات، تحت عنوان «المعالجة وحرية التعبير والمعلومات». فوفقاً لهذه المادة، يجب على الدول الأعضاء التوفيق بين الحق في حماية البيانات الشخصية والحق في حرية التعبير والمعلومات. وعلى وجه الخصوص، يجب تنفيذ الإعفاءات والاستثناءات من فصول محددة من اللائحة العامة لحماية البيانات للأغراض الصحفية أو لغرض التعبير الأكاديمي أو الفني أو الأدبي، بقدر ما تكون ضرورية للتوفيق بين الحق في حماية البيانات الشخصية وحرية التعبير والمعلومات.

مثال: في قضية «وسيط حماية البيانات ضد شركتي 'ساتاكونان ماركينابورس' و'ساتاميديا' المحدودتين»[86]، طُلب من محكمة العدل التابعة للاتحاد الأوروبي تحديد العلاقة بين حماية البيانات وحرية الصحافة. وكان عليها أن تتحقق من عملية نشر قامت بها شركة معينة، بواسطة خدمة الرسائل القصيرة، همت بيانات ضريبية تخص حوالي 1.2 مليون شخص طبيعي بعد ما تم الحصول عليها بشكل قانوني من السلطات الضريبية الفنلندية. وقد أصدرت هيئة الإشراف على حماية البيانات الفنلندية قراراً يطالب الشركة بالتوقف عن نشر هذه البيانات. ولكن طعنت الشركة في هذا القرار في محكمة وطنية، وطلبت هذه الأخيرة توضيحاً من محكمة العدل التابعة للاتحاد الأوروبي بشأن تفسير الأمر التوجيهي المتعلق بحماية البيانات. وعلى وجه الخصوص، كان على محكمة العدل التابعة للاتحاد الأوروبي التحقق مما إذا كان يجب اعتبار معالجة البيانات الشخصية، التي أتاحتها السلطات الضريبية للسماح لمستخدمي الهاتف المحمول بتلقي البيانات الضريبية المتعلقة بالأشخاص الطبيعيين الآخرين، نشاطاً يتم تنفيذه للأغراض الصحفية فقط. وبعد التوصل إلى أن أنشطة الشركة كانت عبارة عن 'معالجة بيانات شخصية' بالمعنى المقصود في المادة 3 (1) من الأمر التوجيهي المتعلق بحماية البيانات، حللت محكمة العدل التابعة للاتحاد الأوروبي المادة 9 من الأمر التوجيهي (بشأن معالجة البيانات الشخصية وحرية التعبير). وأشارت أولاً إلى أهمية الحق في حرية التعبير في كل مجتمع ديمقراطي ورأت أنه ينبغي تفسير المفاهيم المتعلقة بهذه الحرية، مثل الصحافة، على نطاق واسع. ثم لاحظت أنه لتحقيق توازن بين الحقين الأساسيين، يجب ألا تنطبق الاستثناءات والقيود المفروضة على الحق في حماية البيانات إلا بالقدر الذي يُعتبر ضرورياً تماماً. في هذه الظروف، رأت محكمة العدل التابعة للاتحاد الأوروبي أن الأنشطة مثل تلك التي تقوم بها الشركات فيما يتعلق بالبيانات الواردة في المستندات المتاحة في المجال العام بموجب التشريع الوطني يمكن تصنيفها على أنها 'أنشطة صحفية' إذا كان هدفها هو الكشف عن المعلومات أو الآراء أو الأفكار للجمهور، بغض النظر عن الوسيلة المستخدمة لنقلها. كما قضت بأن هذه الأنشطة لا تقتصر على الأعمال الإعلامية ويمكن أن تتم لأغراض الربح. غير أن محكمة العدل التابعة للاتحاد الأوروبي تركت الأمر بيد المحكمة الوطنية للتقرير فيما إذا كان هذا هو الحال مع الوقائع المعينة لهذه القضية.

[86] محكمة العدل التابعة للاتحاد الأوروبي، قضية وسيط حماية البيانات ضد شركتي «ساتاكونان ماركينابورسي» و«ساتاميديا» المحدودتين [الغرفة الكبرى]، 16 ديسمبر 2008، الفقرات 56 و61 و62.

[87] تتعلق القضية بتفسير المادة 9 من المدأ التوجيهي المتعلق بحماية البيانات - التي حلت محلها الآن المادة 85 من اللائحة العامة لحماية البيانات - والتي تنص على ما يلي: «يتعين على الدول الأعضاء التنصيص على استثناءات أو إعفاءات من أحكام هذا الفصل والفصل الرابع والفصل السادس لمعالجة البيانات الشخصية التي يتم إجراؤها فقط للأغراض الصحفية أو لأغراض فنية أو التعبير الأدبي فقط إذا كانت ضرورية للتوفيق بين الحق في الخصوصية والقواعد التي تحكم حرية التعبير».

هذا وقد نظرت المحكمة الأوروبية لحقوق الإنسان في نفس القضية أيضاً، بعد أن قررت المحكمة الوطنية، بناءً على إرشادات من محكمة العدل التابعة للاتحاد الأوروبي، أن أمر الهيئة الإشرافية بوقف نشر جميع المعلومات الضريبية هو تدخل مبرر في حرية الشركة في التعبير. وقد أيدت المحكمة الأوروبية لحقوق الإنسان هذا النهج.[88] حيث وجدت أنه على الرغم من وجود تدخل في حق الشركات في نقل المعلومات، فإن هذا التدخل كان متوافقاً مع القانون، وسعى إلى تحقيق هدف مشروع، وكان ضرورياً في مجتمع ديمقراطي.

وأشارت المحكمة إلى معايير السوابق القضائية التي ينبغي أن توجه السلطات الوطنية وأيضاً المحكمة الأوروبية لحقوق الإنسان بنفسها، عند الموازنة بين حرية التعبير والحق في احترام الحياة الخاصة. فعندما يكون خطاب سياسي أو نقاش حول مسألة تتعلق بالمصلحة العامة قيد النظر، يكون هناك مجال ضئيل لتقييد الحق في تلقي المعلومات ونقلها حيث أن للجمهور الحق في الحصول على المعلومات، «وهذا حق أساسي في مجتمع ديمقراطي».[89]

«ولكن لا يمكن اعتبار المقالات الصحفية التي تهدف فقط إلى إرضاء فضول قراء معينين فيما يتعلق بتفاصيل الحياة الخاصة لشخص ما مساهمة في نقاش يتعلق بالمصلحة العامة. ويهدف الاستثناء من قواعد حماية البيانات للأغراض الصحفية إلى السماح للصحفيين بالوصول إلى البيانات وجمعها ومعالجتها حتى يتمكنوا من أداء أنشطتهم الصحفية. وبالتالي، فقد كانت هناك بالفعل مصلحة عامة في منح الشركات المدعية الوصول إلى الكميات الكبيرة من البيانات الضريبية قيد النظر والسماح لها بجمعها ومعالجتها. وعلى النقيض من ذلك، وجدت المحكمة أنه لم تكن هناك مصلحة عامة في نشر مثل هذه البيانات الخام من قبل الصحف بالجملة وفي شكل غير معدل وبدون أي مدخلات تحليلية. إذ يُحتمل أن تكون المعلومات المتعلقة بالضرائب قد مكنت الأفراد الفضوليين من تصنيف الأفراد وفقاً لوضعهم الاقتصادي وأشبعت تعطش الجمهور للحصول على معلومات حول الحياة الخاصة للآخرين، ولا يمكن اعتبار ذلك مساهمة في نقاش متعلق بالمصلحة العامة.

مثال: في قضية «غوغل إسبانيا»،[90] نظرت محكمة العدل التابعة للاتحاد الأوروبي في ما إذا كانت شركة «غوغل» ملزمة بحذف المعلومات المتقادمة حول الصعوبات المالية التي مر منها المدعي من نتائج قائمة البحث الخاصة بها. فعندما كان يتم إجراء بحث على محرك البحث التابع لشركة «غوغل» باستخدام اسم المدعي، كانت نتائج البحث تقدم روابط لمقالات صحفية قديمة تشير إلى علاقته بإجراءات الإفلاس. واعتبر المدعي هذا انتهاكاً لحقيه في احترام الحياة الخاصة وحماية البيانات الشخصية، حيث إن الإجراءات قد تم الانتهاء منها منذ سنوات، مما يجعل هذه الإشارات غير ذات صلة.

أوضحت المحكمة الأوروبية لحقوق الإنسان أولاً أن محركات البحث على الإنترنت ونتائج البحث التي توفر البيانات الشخصية يمكن أن تنشئ ملفاً تفصيلياً للفرد. وفي ضوء مجتمع يصبح أكثر رقمنة بشكل متزايد، فإن شرط أن تكون البيانات الشخصية دقيقة وأن لا يتجاوز نشرها ما هو ضروري، أي توفير المعلومات للجمهور، يعد أمراً أساسياً لضمان مستوىً عالٍ من حماية البيانات للأفراد. ويجب أن يضمن «المراقب فيما يتعلق بهذه المعالجة، في إطار مسؤولياته وصلاحياته وقدراته، أن تلك المعالجة تفي بمتطلبات» قانون الاتحاد الأوروبي، حتى يكون للضمانات القانونية الموضوعة تأثير كامل. وهذا يعني أن حق المرء في أن تُمحى بياناته الشخصية عندما تصبح المعالجة غير ضرورية أو متقادمة يشمل أيضاً على محركات البحث، التي وُجد بأنها تُعد مراقباً، وليست مجرد معالج (انظر الجزء 1.3.2).

عند النظر فيما إذا كانت شركة «غوغل» مطالبة بإزالة الروابط المتعلقة بالمدعي، رأت محكمة العدل التابعة للاتحاد الأوروبي أنه في ظل ظروف معينة، يحق للأفراد الحصول على محو بياناتهم الشخصية من نتائج بحث محرك بحث على الإنترنت. ويمكن المطالبة بهذا الحق عندما تكون المعلومات المتعلقة بالفرد خاطئة أو غير ملائمة أو غير ذات صلة أو مفرطة لأغراض معالجة البيانات. وقد أقرت محكمة العدل التابعة للاتحاد الأوروبي أن هذا الحق ليس مطلقاً؛ بل يجب أن تتم موازنته مع حقوق أخرى، ولا سيما مصلحة الجمهور العام وحقه في الوصول إلى المعلومات.

يجب تقييم كل طلب للمحو على أساس كل حالة على حدة لتحقيق التوازن بين الحقين الأساسيين في حماية البيانات الشخصية والحياة الخاصة لصاحب البيانات من جهة، والمصالح المشروعة لجميع مستخدمي الإنترنت من جهة أخرى. وقد قدمت محكمة العدل التابعة للاتحاد الأوروبي إرشادات بشأن العوامل التي يجب مراعاتها أثناء القيام بعملية الموازنة هذه. وتُعتبر طبيعة المعلومات المعنية عاملاً مهماً بشكل خاص في هذا الصدد. فإذا كانت المعلومات تتعلق بالحياة الخاصة للفرد بصورة حساسة، ولا توجد مصلحة عامة في توفيرها للعموم، فإن حقي حماية البيانات والخصوصية سيطغيان على حق الجمهور العام في الوصول إلى المعلومات. وعلى العكس من ذلك، إذا تبين أن صاحب البيانات هو شخصية عامة، أو أن المعلومات ذات طبيعة تبرر إتاحتها للجمهور العام، فإن ذلك يبرر التدخل في الحقوق الأساسية لصاحب البيانات في حماية البيانات والخصوصية.

بعد صدور الحكم، تبنى فريق عمل المادة 29 مبادئ توجيهية بشأن تنفيذ حكم محكمة العدل التابعة للاتحاد الأوروبي. وتتضمن هذه المبادئ التوجيهية قائمة بالمعايير المشتركة التي يجب أن تستخدمها الهيئات الإشرافية عند التعامل مع الشكاوى المتعلقة بطلبات الأفراد للحذف وإرشادات فيما يخص عملية الموازنة بين الحقوق.[91]

---

[88] المحكمة الأوروبية لحقوق الإنسان، قضية شركتي «ساتاكونان ماركينابورسي» و«ساتاميديا» المحدودتين ضد فنلندا، رقم 13/931، 27 يونيو 2017.

[89] نفس المرجع السابق، الفقرة 169.

[90] لفريق عمل المادة 29 (2014)، المبادئ التوجيهية لتنفيذ حكم محكمة العدل التابعة للاتحاد الأوروبي في قضية «غوغل إسبانيا وشركة غوغل ضد الوكالة الإسبانية لحماية البيانات (AEPD) وماريو كوستيخا جونزاليز» C-131/12، WP 225، بروكسل، 26 نوفمبر 2014.

[91] لفريق عمل المادة 29 (2014)، المبادئ التوجيهية لتنفيذ حكم محكمة العدل التابعة للاتحاد الأوروبي في قضية «غوغل إسبانيا وشركة غوغل ضد الوكالة الإسبانية لحماية البيانات (AEPD) وماريو كوستيخا جونزاليز» C-131/12، WP 225، بروكسل، 26 نوفمبر 2014..

فيما يتعلق بالتوفيق بين الحق في حماية البيانات والحق في حرية التعبير، أصدرت المحكمة الأوروبية لحقوق الإنسان عدداً من الأحكام البارزة.

مثال: في قضية شركة «'أكسل سبينجر' المساهمة ضد ألمانيا»،[92] قضت المحكمة الأوروبية لحقوق الإنسان بأن أمراً احترازياً يمنع الشركة المدعية من نشر مقال عن اعتقال وإدانة ممثل معروف ينتهك المادة 10 من الاتفاقية الأوروبية لحقوق الإنسان. وكررت المحكمة الأوروبية لحقوق الإنسان المعايير التي يجب مراعاتها عند الموازنة بين الحق في حرية التعبير والحق في احترام الحياة الخاصة، على النحو المنصوص عليه في سوابقها القضائية:

- ما إذا كان الحدث الذي يغطيه المقال المنشور ذا أهمية عامة؛
- ما إذا كان الشخص المعني شخصية عامة؛
- كيف تم الحصول على المعلومات وما إذا كانت موثوقة.

وجدت المحكمة الأوروبية لحقوق الإنسان أن حدث اعتقال الممثل وإدانته كان حقيقة قضائية عامة وبالتالي يندرج ضمن المصلحة العامة؛ فقد كان الممثل مشهوراً بما يكفي لتنطبق عليه صفة الشخصية العامة؛ وأن المعلومات بشأن اعتقاله قد قدمها مكتب المدعي العام ولم يكن هناك نزاع حول صحتها بين الأطراف. لذلك، لم تكن قيود النشر المفروضة على الشركة متناسبة بشكل معقول مع الهدف المشروع المتمثل في حماية الحياة الخاصة للمدعي. فخلصت المحكمة إلى أنه تم انتهاك المادة 10 من الاتفاقية الأوروبية لحقوق الإنسان.

مثال: تتعلق قضية «'شركة كوديك وهاشيت فيليباكي' ضد فرنسا»[93] بنشر مجلة أسبوعية فرنسية لمقابلة مع السيدة كوست، والتي ادعت فيها هذه الأخيرة أن الأمير ألبرت، أمير موناكو، هو والد ابنها. ووصفت المقابلة أيضاً علاقة السيدة كوست بالأمير، وطريقة تفاعله مع ولادة الطفل، مصحوبة بصور الأمير رفقة الطفل. رفع الأمير ألبرت دعوى قضائية ضد شركة النشر لانتهاك حقه في حماية حياته الخاصة. ورأت المحاكم الفرنسية أن نشر المقال قد تسبب في ضرر لا رجعة فيه للأمير ألبرت وأمرت الناشر بدفع تعويضات ونشر تفاصيل حكمها على الغلاف الأمامي للمجلة.

بعد ذلك، رفع ناشرو المجلة القضية أمام المحكمة الأوروبية لحقوق الإنسان، زاعمين أن حكم المحاكم الفرنسية يتعارض بشكل غير مبرر مع حقهم في حرية التعبير. كان على المحكمة الأوروبية لحقوق الإنسان أن توازن بين حق الأمير ألبرت في احترام حياته الخاصة من جهة وحق الناشر في التعبير وحق الجمهور العام في الحصول على المعلومات من جهة أخرى. كما كان حق السيدة كوست في مشاركة قصتها مع الجمهور ومصلحة الطفل في أن يُعترف رسمياً بعلاقته بوالده أمرين مهمين يجب أن يؤخذا في الاعتبار أيضاً.

رأت المحكمة الأوروبية لحقوق الإنسان أن نشر المقابلة يشكل تدخلاً في الحياة الخاصة للأمير وتحققت مما إذا كان هذا التدخل ضرورياً. واعتبرت أن المنشور يتعلق بشخصية عامة ومسألة تتعلق بالمصلحة العامة، حيث كان لمواطني موناكو مصلحة في معرفة وجود طفل للأمير، لأن مستقبل الملكية الوراثية «يرتبط ارتباطاً وثيقاً بوجود الخلف»، وبالتالي فإن ذلك يشكل مسألة موضع اهتمام للجمهور.[94] هذا وأشارت المحكمة إلى أن المقال سمح للسيدة كوست وطفلها بممارسة حقهما في حرية التعبير. لم تقم المحاكم المحلية بإيلاء الاعتبار الواجب للمبادئ والمعايير التي تم وضعها من خلال السوابق القضائية للمحكمة الأوروبية لحقوق الإنسان للموازنة بين الحق في احترام الحياة الخاصة والحق في حرية التعبير. وخلصت إلى أن فرنسا انتهكت المادة 10 من الاتفاقية الأوروبية لحقوق الإنسان فيما يتعلق بحرية التعبير.

في السوابق القضائية للمحكمة الأوروبية لحقوق الإنسان، يتمثل أحد المعايير الحاسمة فيما يتعلق بالموازنة بين هذه الحقوق في ما إذا كان التعبير المعني يساهم في إغناء نقاش متعلق بالمصلحة العامة أم لا.

[92] المحكمة الأوروبية لحقوق الإنسان، قضية شركة «أكسل سبينجر المساهمة» ضد ألمانيا [الغرفة الكبرى]، رقم 39954/08، 7 فبراير 2012، الفقرتان 90 و91

[93] المحكمة الأوروبية لحقوق الإنسان، قضية شركة «كوديك وهاشيت فيليباكي» ضد فرنسا [الغرفة الكبرى]، رقم 40454/07، 10 نوفمبر 2015.

[94] نفس المرجع السابق، الفقرات 104-116.

مثال: في قضية «'موزلي' ضد المملكة المتحدة»،[95] نشرت صحيفة أسبوعية وطنية صوراً حميمة للمدعي، وهو شخصية معروفة، وقد نجح فيما بعد في رفع دعوى مدنية ضد الناشر وحصل على تعويضات. إلا أنه على الرغم من التعويض المالي الذي حصل عليه، اشتكى من كونه قد ظل ضحية لانتهاك حقه في الخصوصية لأنه حُرم من فرصة التماس أمر احترازي قبل نشر الصور المذكورة بسبب عدم وجود أي شرط قانوني يرغم الصحيفة على تقديم إشعار مسبق قبل النشر.

وقد سجلت المحكمة الأوروبية لحقوق الإنسان أنه على الرغم من أن نشر مثل هذه المواد قد كان لأغراض الترفيه عموماً وليس التثقيف، إلا أن المواد المنشورة قد استفادت بلا شك من حماية المادة 10 من الاتفاقية الأوروبية لحقوق الإنسان، والتي قد تتصاع إلى متطلبات المادة 8 من نفس الاتفاقية على أساس أن المعلومات كانت ذات طبيعة خاصة وحميمية ولم تكن هناك مصلحة عامة في نشرها. غير أنه كان من الواجب توخي الحذر بشكل خاص عند فحص القيود التي قد تعمل كشكل من أشكال الرقابة قبل النشر. وبالنظر للأثر المثبط الذي قد ينشأ عن اشتراط الإخطار المسبق والشكوك حول فعاليته والهامش الواسع للتقدير في هذا المجال، خلصت المحكمة الأوروبية لحقوق الإنسان إلى أن وجود شرط ملزم قانوناً للإخطار المسبق يبقى أمراً غير مفروض بمقتضى المادة 8. وعليه، خلصت المحكمة إلى أنه لم يكن هناك انتهاك للمادة 8.

مثال: في قضية «'بولين' ضد ألمانيا»،[96] نشر المدعي، وهو مغنٍّ ومنتج فني مشهور، كتاباً عن سيرته الذاتية، ثم أُجبر بعد ذلك على إزالة بعض المقاطع منه بعد صدور أحكام قضائية. وقد تمت تغطية هذا الخبر على نطاق واسع في وسائل الإعلام الوطنية، وأطلقت إحدى شركات التبغ حملة إعلانية فكاهية تشير إلى هذا الحدث، باستخدام الاسم الأول للمدعي دون موافقته. وسعى المدعي دون جدوى للحصول على تعويضات من شركة الإعلانات، مدعياً أنه تم انتهاك حقوقه بموجب المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان. كررت المحكمة الأوروبية لحقوق الإنسان المعايير التي توجه عملية الموازنة بين الحق في احترام الحياة الخاصة والحق في حرية التعبير، ورأت أنه لا يوجد انتهاك للمادة 8. فقد كان المدعي شخصية عامة ولم يشر الإعلان إلى تفاصيل حياته الخاصة ولكن إلى حدث عام سبق أن غطته وسائل الإعلام وشكل جزءاً من نقاش عام. بالإضافة إلى ذلك، كان الإعلان ذا طبيعة فكاهية ولم يحتوِ على أي شيء مهين أو سلبي تجاه بالمدعي.

مثال: في قضية «'بيريوك' ضد ليتوانيا»،[97] جادلت المدعية أمام المحكمة الأوروبية لحقوق الإنسان بأن ليتوانيا قد أخفقت في الوفاء بالتزامها بضمان احترام حقها في الحياة الخاصة. لأنه على الرغم من أن إحدى الصحف الكبرى قد ارتكبت انتهاكاً خطيراً لخصوصيتها، لم تحصل سوى على مبلغ هزيل من التعويضات المالية من قبل المحاكم الوطنية التي نظرت في القضية. وعند منحها التعويضات غير المالية، طبقت المحاكم الوطنية أحكام القانون الوطني بشأن تقديم المعلومات للجمهور، والتي تفرض سقفاً منخفضاً للتعويض عن الضرر غير المالي الناجم عن النشر غير القانوني للمعلومات حول حياة الشخص الخاصة للجمهور من قبل وسائل الإعلام. وقد نشأت هذه القضية عند قيام أكبر صحيفة يومية في ليتوانيا بنشر مقال على صفحتها الأولى يفيد بأن المدعية مصابة بفيروس نقص المناعة البشرية. كما انتقد المقال أيضاً سلوك المدعية وشكك في معاييرها الأخلاقية.

أشارت المحكمة الأوروبية لحقوق الإنسان إلى أن حماية البيانات الشخصية، ولا سيما البيانات الطبية، هي ذات أهمية أساسية للحق في احترام الحياة الخاصة بموجب الاتفاقية الأوروبية لحقوق الإنسان. وتُعتبر سرية بيانات الصحة ذات أهمية خاصة، لأن الكشف عن البيانات الطبية (إصابة المدعية بفيروس نقص المناعة البشرية في هذه الحالة) قد يؤثر بشكل كبير على حياة الشخص الخاصة والعائلية، ووضعه الوظيفي، واندماجه في المجتمع. وعلقت المحكمة أهمية خاصة على حقيقة أنه، وفقاً للخبر المنشور في الصحيفة، قام الطاقم الطبي بالمستشفى بتقديم المعلومات عن حالة المدعية فيما يتعلق بفيروس نقص المناعة البشرية في انتهاك واضح لالتزامهم بالسرية الطبية. وبالتالي لم يكن هذا التدخل في حق المدعية في الحياة الخاصة مشروعاً.

[95] المحكمة الأوروبية لحقوق الإنسان، قضية موزلي ضد المملكة المتحدة، رقم 48009/08، 10 مايو 2011، الفقرتان 129 و130.
[96] المحكمة الأوروبية لحقوق الإنسان، قضية بولين ضد ألمانيا، رقم 53495/09، 19 فبراير 2015، الفقرات 45-60.
[97] المحكمة الأوروبية لحقوق الإنسان، قضية بيريوك ضد ليتوانيا، رقم 23373/03، 25 نوفمبر 2008.

لقد تم نشر المقال من قبل الصحافة، وحرية التعبير هي أيضاً حق أساسي بموجب الاتفاقية الأوروبية لحقوق الإنسان. إلا أنه عند تحقق المحكمة مما إذا كانت توجد مصلحة عامة تبرر نشر هذا النوع من المعلومات حول المدعية، وجدت المحكمة أن الغرض الرئيسي من المنشور هو زيادة مبيعات الصحيفة من خلال إرضاء فضول القراء. ولا يمكن اعتبار هذا الغرض على أنه يساهم في أي نقاش متعلق بالمصلحة العامة للمجتمع. وبما أن هذا الفعل شكل «إساءة استعمال صارخة لحرية الصحافة»، فإن القيود الصارمة في جبر الضرر والقيمة المنخفضة للتعويضات غير المالية المنصوص عليها في القانون الوطني تعني أن ليتوانيا لم تفِ بالتزامها الإيجابي بحماية حق المدعية في حماية حياتها خاصة. ووجدت المحكمة الأوروبية لحقوق الإنسان أنه كان هناك انتهاك للمادة 8 من الاتفاقية الأوروبية لحقوق الإنسان.

لا يتعارض الحق في حرية التعبير والحق في حماية البيانات الشخصية دائمًا. بل هناك حالات تضمن فيها الحماية الفعالة للبيانات الشخصية حرية التعبير.

مثال: ذكرت محكمة العدل التابعة للاتحاد الأوروبي في قضية قناة «تيلي 2 السويد» أن التدخل الناجم عن الأمر التوجيهي 2006/24 (الأمر التوجيهي المتعلق بالاحتفاظ بالبيانات) في الحقوق الأساسية المنصوص عليها في المادتين 7 و8 من ميثاق الحقوق الأساسية للاتحاد الأوروبي كان «واسع النطاق، ويجب اعتباره خطيراً بصورة خاصة. علاوة على ذلك... فإن كون البيانات يتم الاحتفاظ بها واستخدامها لاحقاً دون إبلاغ المشترك أو المستخدم المسجل من المرجح أن يولد في أذهان أصحاب البيانات شعوراً بأن حياتهم الخاصة تخضع للمراقبة المستمرة». ووجدت محكمة العدل التابعة للاتحاد الأوروبي أيضاً أن الاحتفاظ المعمم ببيانات المرور والموقع يمكن أن يكون له تأثير على استخدام الاتصالات الإلكترونية «وبالتالي على ممارسة مستخدميها لحرية التعبير المكفولة في المادة 11 من ميثاق الحقوق الأساسية للاتحاد الأوروبي».[98] وبهذا المعنى، من خلال المطالبة بضمانات صارمة لعدم الاحتفاظ بالبيانات بطريقة معممة، فإن قواعد حماية البيانات تساهم في نهاية المطاف في ممارسة حرية التعبير.

فيما يتعلق بالحق في تلقي المعلومات، والذي يشكل أيضاً جزءاً من حرية التعبير، هناك إدراك متزايد لأهمية شفافية الحكومة لسير عمل مجتمع ديمقراطي. إن الشفافية هدف للمصلحة العامة، ويمكنها بالتالي أن تبرر التدخل في الحق في حماية البيانات، إذا لزم الأمر وكان متناسباً، كما هو موضح في الجزء 1.2. ونتيجة لذلك، في العقدين الماضيين، تم الاعتراف بالحق في الوصول إلى الوثائق التي تحتفظ بها السلطات العامة كحق مهم لكل مواطن في الاتحاد الأوروبي، وأي شخص طبيعي أو اعتباري يقيم في دولة عضو أو لديه مكتب مسجل بها.

**وفق قانون مجلس أوروبا**، يمكن الرجوع إلى المبادئ المنصوص عليها في التوصية بشأن الوصول إلى الوثائق الرسمية، والتي ألهمت واضعي اتفاقية الوصول إلى الوثائق الرسمية (الاتفاقية 205).[99]

**وفق قانون الاتحاد الأوروبي**، يُعد الحق في الوصول إلى الوثائق مكفولاً بموجب اللائحة 1049/2001 فيما يتعلق بوصول الجمهور إلى وثائق البرلمان الأوروبي والمجلس الأوروبي والمفوضية الأوروبية (لائحة الوصول إلى الوثائق).[100] وقد وسعت المادة 42 من ميثاق الحقوق الأساسية للاتحاد الأوروبي والمادة 15 (3) من المعاهدة المتعلقة بسير عمل الاتحاد الأوروبي هذا الحق في الوصول «إلى وثائق المؤسسات والهيئات والمكاتب والوكالات التابعة للاتحاد، بغض النظر عن شكلها».

قد يتعارض هذا الحق مع الحق في حماية البيانات إذا كان الوصول إلى وثيقة ما سيكشف البيانات الشخصية للآخرين. وتنص المادة 86 من اللائحة العامة لحماية البيانات بوضوح على أنه يجوز الكشف عن البيانات الشخصية في الوثائق الرسمية التي تحتفظ بها السلطات والهيئات

[98] محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-203/15 وC-698/15، قناة «تيلي 2 السويد المحدودة» ضد هيئة البريد والاتصالات السويدية، ووزير الداخلية بالمملكة المتحدة ضد توم واتسون وآخرين [الغرفة الكبرى]، 21 ديسمبر 2016، الفقرة 101؛ محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-293/12 وC-594/12، منظمة «ديجيتال رايتس آيرلاند» المحدودة ضد وزير الاتصالات والموارد البحرية والطبيعية بأيرلندا وآخرين وحكومة ولاية كيرنتن وآخرين [الغرفة الكبرى]، 8 أبريل 2014، الفقرة 28.

[99] مجلس أوروبا، لجنة الوزراء (2002)، التوصية 19 (81) R والتوصية 2 (2002)Rec للدول الأعضاء بشأن الوصول إلى الوثائق الرسمية، 21 فبراير 2002؛ اتفاقية مجلس أوروبا بشأن الوصول إلى الوثائق الرسمية، مؤتمر مجلس أوروبا للأطراف رقم 205، 18 يونيو 2009. لم تدخل الاتفاقية حيز التنفيذ بعد.

[100] اللائحة (الجماعة الأوروبية) رقم 1049/2001 الصادرة عن البرلمان الأوروبي والمجلس الأوروبي في 30 مايو 2001 بشأن وصول الجمهور إلى وثائق البرلمان الأوروبي والمجلس والمفوضية الأوروبية، الجريدة الرسمية 145 L 2001 OJ.

العامة من قبل السلطة أو الهيئة المعنية وفقاً لقانون الاتحاد الأوروبي[101] أو الدولة العضو للتوفيق بين وصول الجمهور إلى الوثائق الرسمية والحق في حماية البيانات وفقاً للائحة.

وبالتالي، قد تحتاج طلبات الوصول إلى الوثائق أو المعلومات التي تحتفظ بها السلطات العامة إلى الموازنة مع الحق في حماية البيانات للأشخاص الواردة بياناتهم في الوثائق المطلوبة.

مثال: في قضية شركة «'فولكر وماركوس شيكه' و'هارتموت أيفرت' ضد 'لاند هيسن'»،[102] كان على محكمة العدل التابعة للاتحاد الأوروبي أن تقرر مدى تناسب النشر، الذي كان مطلوباً بموجب تشريعات الاتحاد الأوروبي، لأسماء المستفيدين من الإعانات الفلاحية في الاتحاد الأوروبي والمبالغ التي حصلوا عليها. وقد كان الهدف من المنشور هو تعزيز الشفافية والمساهمة في المراقبة العامة للاستخدام المناسب للأموال العامة من قبل الإدارة. إلا أن العديد من المستفيدين طعنوا في تناسبية هذا المنشور.

دفعت محكمة العدل التابعة للاتحاد الأوروبي، مشيرة إلى أن الحق في حماية البيانات ليس مطلقاً، بإن النشر على موقع إلكتروني للبيانات التي تُعرِّف المستفيدين من صندوقي المساعدات الفلاحية للاتحاد الأوروبي والمبالغ الدقيقة المستلمة يشكل تدخلاً في حياتهم الخاصة بشكل عام وفي حماية بياناتهم الشخصية على وجه الخصوص.

ووجدت محكمة العدل التابعة للاتحاد الأوروبي أن مثل هذا التدخل في المادتين 7 و8 من ميثاق الحقوق الأساسية للاتحاد الأوروبي منصوص عليه بموجب القانون ويحقق هدفاً متعلقاً بالمصلحة العامة معترفاً به من قبل الاتحاد الأوروبي - وهو تعزيز شفافية استخدام أموال الصناديق المجتمعية. إلا أن محكمة العدل التابعة للاتحاد الأوروبي رأت أن نشر أسماء الأشخاص الطبيعيين المستفيدين من المساعدة الفلاحية للاتحاد الأوروبي من هذين الصندوقين والمبالغ الدقيقة التي تلقوها يشكل تدبيراً غير متناسب ولم يكن له ما يبرره مع مراعاة المادة 52 (1) من ميثاق الحقوق الأساسية للاتحاد الأوروبي. وأقرت المحكمة بأهمية إبقاء دافعي الضرائب على علم بكيفية استخدام الأموال العامة في مجتمع ديمقراطي. ولكن بما أنه «لا يمكن منح أولوية تلقائية لهدف الشفافية على الحق في حماية البيانات الشخصية»[103]، فقد اضطرت مؤسسات الاتحاد الأوروبي إلى الموازنة بين مصلحة الاتحاد في الشفافية والقيود المفروضة على ممارسة حقوق الخصوصية وحماية البيانات التي عانى منها المستفيدون بسبب المعلومات المنشورة.

واعتبرت محكمة العدل التابعة للاتحاد الأوروبي أن مؤسسات الاتحاد الأوروبي لم تنفذ هذه الموازنة بشكل صحيح، حيث كان من الممكن توخي تدابير من شأنها أن تؤثر بشكل أقل سلباً على الحقوق الأساسية للأفراد، بينما تساهم أيضاً بشكل فعال في تحقيق هدف الشفافية الذي يسعى إليه المنشور. فعلى سبيل المثال، بدلاً من إصدار منشور عام يؤثر على جميع المستفيدين، مع ذكر أسمائهم والمبالغ الدقيقة التي حصل عليها كل منهم، كان من الممكن تمييز تلك المعلومات بناءً على المعايير ذات الصلة مثل الفترات التي تلقى خلالها هؤلاء الأشخاص المساعدة أو وتيرة تلقّيهم لها أو قدرها وطبيعتها.[104] وعليه، قضت محكمة العدل التابعة للاتحاد الأوروبي بأن تشريعات الاتحاد الأوروبي المتعلقة بنشر المعلومات الخاصة بالمستفيدين من الصناديق الفلاحية الأوروبية هي باطلة جزئياً.

مثال: في قضية «ديوان المحاسبة النمساوي ضد الإذاعة النمساوية وآخرين»،[105] راجعت محكمة العدل التابعة للاتحاد الأوروبي مدى توافق بعض التشريعات النمساوية مع قانون حماية البيانات في الاتحاد الأوروبي. إذ يتطلّب التشريع النمساوي أن تقوم هيئة تابعة للدولة بجمع ونقل البيانات المتعلقة بالدخل لأغراض نشر أسماء ومداخيل الموظفين من مختلف الهيئات العامة في تقرير سنوي متاح للجمهور العام. لكن بعض الأفراد رفضوا الإفصاح عن بياناتهم بذريعة حماية البيانات.

[101] المادة 42 من ميثاق الحقوق الأساسية للاتحاد الأوروبي، المادة 15 (3) من اتفاقية سير عمل الاتحاد الأوروبي واللائحة 1049/2009.

[102] محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-92/09 وC-93/09، فولكر وماركوس شيكه (شركة يحكمها القانون المدني الألماني) وهارتموت أيفرت ضد لاند هيسن [الغرفة الكبرى]، 9 نوفمبر 2010، الفقرات 47-52 و58 و66-67 و75 و86 و92.

[103] نفس المرجع السابق، الفقرة 85.

[104] نفس المرجع السابق، الفقرة 89.

[105] محكمة العدل التابعة للاتحاد الأوروبي، القضايا المضمومة C-465/00 و C-138/01 وC-139/09، «ديوان المحاسبة الألماني ضد الإذاعة النمساوية وآخرين» و«كريستا نوكوم وجوزيف لاورمان ضد الإذاعة النمساوية»، 20 مايو 2003.

في رأيها، اعتمدت محكمة العدل التابعة للاتحاد الأوروبي على حماية الحقوق الأساسية كمبدأ عام لقانون الاتحاد الأوروبي وعلى المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان، مشيرة إلى أن ميثاق الحقوق الأساسية للاتحاد الأوروبي لم يكن مُلزِماً في ذلك الوقت. ورأت أن جمع البيانات عن الدخل المهني للفرد، ولا سيما تسليمها لأطراف ثالثة، يندرج في نطاق الحق في احترام الحياة الخاصة ويشكل انتهاكاً له. ويمكن أن يكون التدخل مبرراً إذا كان قد تم وفقاً للقانون وسعى لتحقيق هدف مشروع وكان ضرورياً في مجتمع ديمقراطي لتحقيق هذا الهدف. وأشارت محكمة العدل التابعة للاتحاد الأوروبي إلى أن التشريع النمساوي سعى إلى تحقيق هدف مشروع، حيث كان هدفه إبقاء رواتب موظفي القطاع العام ضمن حدود معقولة، وهو اعتبار يرتبط أيضاً بالرفاهية الاقتصادية للبلاد. غير أن مصلحة النمسا المتمثلة في ضمان أفضل استخدام للأموال العامة يجب أن تكون متوازنة مع خطورة التدخل في حق أصحاب البيانات في احترام حياتهم الخاصة.

وفي حين تركت محكمة العدل التابعة للاتحاد الأوروبي الأمر بيد المحكمة الوطنية للتأكد مما إذا كان نشر البيانات المتعلقة بدخل الأفراد ضرورياً ومتناسباً مع الهدف الذي يسعى إليه التشريع، دعت محكمة العدل التابعة للاتحاد الأوروبي المحكمة الوطنية إلى التحقق مما إذا كان هذا الهدف لا يمكن تحقيقه بنفس القدر من الفعالية بوسائل أقل تدخلاً. ومن بين الأمثلة على ذلك نقل البيانات الشخصية إلى هيئات المراقبة العامة فقط وليس إلى عامة الناس.

في القضايا اللاحقة، أصبح من الواضح أن الموازنة بين حماية البيانات والوصول إلى الوثائق تتطلب تحليلاً مفصلاً لكل حالة على حدة. ولا يمكن لأي من الحقين أن يطغى على الآخر تلقائياً. لقد تسنى لمحكمة العدل التابعة للاتحاد الأوروبي أن تفسر الحق في الوصول إلى الوثائق التي تحتوي على بيانات شخصية في قضيتين.

مثال: في قضية «المفوضية الأوروبية ضد شركة 'بافاريان لاجر'»،[106] حددت محكمة العدل التابعة للاتحاد الأوروبي نطاق حماية البيانات الشخصية في سياق الوصول إلى وثائق مؤسسات الاتحاد الأوروبي، والعلاقة بين اللائحة رقم 1049/2001 (لائحة الوصول إلى الوثائق) واللائحة رقم 45/2001 (لائحة حماية بيانات مؤسسات الاتحاد الأوروبي). لقد تأسست شركة «بافاريان لاجر» سنة 1992، وهي تستورد الجعة الألمانية المعبأة في زجاجات إلى المملكة المتحدة لتُستهلَك بشكل أساسي في البارات والحانات. إلا أنها واجهت صعوبات لأن التشريع البريطاني يعطي الأفضلية بحكم الواقع للمنتجين الوطنيين. ورداً على شكوى شركة «بافاريان لاجر»، أقامت المفوضية الأوروبية دعوى ضد المملكة المتحدة لإخفاقها في الوفاء بالتزاماتها، مما أدى بها إلى تعديل الأحكام المتنازع عليها ومواءمتها مع قانون الاتحاد الأوروبي. وبعد ذلك، طلبت شركة «بافاريان لاجر» من المفوضية عدة وثائق، من بينها نسخة من محضر الاجتماع الذي حضره ممثلو المفوضية الأوروبية والسلطات البريطانية و «اتحاد صناع الجعة في السوق المشتركة» (CBMC). وافقت المفوضية على الكشف عن وثائق معينة تتعلق بالاجتماع، لكنها طمست خمسة أسماء وردت في المحضر - إذ اعترض شخصان صراحة على الكشف عن هويتهما ولم تتمكن المفوضية من الاتصال بالثلاثة الآخرين. بموجب القرار الصادر في 18 مارس 2004، رفضت المفوضية طلباً جديداً من شركة «بافاريان لاجر» للحصول على محضر الاجتماع الكامل، مستشهدة على وجه الخصوص بحماية الحياة الخاصة لهؤلاء الأشخاص على النحو الذي تضمنه لائحة حماية البيانات الخاصة بمؤسسات الاتحاد الأوروبي.

ونظراً لعدم رضاها بهذا الموقف، رفعت شركة «بافاريان لاجر» دعوى أمام المحكمة الابتدائية. فألغت هذه الأخيرة قرار المفوضية الأوروبية بموجب حكم صادر في 8 نوفمبر 2007 (القضية T-194/04، «شركة 'بافاريان لاجر' المحدودة ضد لجنة الجماعات الأوروبية»)، ووجدت أن مجرد إدراج أسماء الأشخاص المعنيين في قائمة الأشخاص الذين حضروا اجتماعاً نيابة عن الهيئة التي يمثلونها لا يخل بالحياة الخاصة لهؤلاء الأشخاص ولا يعرضها لأي خطر.

[106] محكمة العدل التابعة للاتحاد الأوروبي، القضية C-28/08 P، المفوضية الأوروبية ضد «شركة بافاريان لاجر المحدودة» [الغرفة الكبرى]، 29 يونيو 2010.

وفي الاستئناف الذي تقدمت به المفوضية، ألغت محكمة العدل التابعة للاتحاد الأوروبي حكم المحكمة الابتدائية. حيث اعتبرت محكمة العدل التابعة للاتحاد الأوروبي أن لائحة الوصول إلى الوثائق تحدد «نظاماً خاصاً ومعززاً لحماية الشخص الذي يمكن، في بعض الحالات، نقل بياناته الشخصية إلى الجمهور». ووفقاً لمحكمة العدل التابعة للاتحاد الأوروبي، عندما يسعى طلب يستند إلى لائحة الوصول إلى الوثائق إلى الوصول إلى وثائق تتضمن بيانات شخصية، تصبح أحكام لائحة حماية البيانات الخاصة بمؤسسات الاتحاد الأوروبي قابلة للتطبيق في مجملها. وخلصت محكمة العدل التابعة للاتحاد الأوروبي بعد ذلك إلى أن المفوضية كانت على حق في رفض طلب الوصول إلى محضر الاجتماع الكامل المنعقد في أكتوبر 1996. وفي غياب موافقة المشاركين الخمسة في ذلك الاجتماع، امتثلت المفوضية بشكل كافٍ لواجبها في الانفتاح من خلال إصدار نسخة من الوثيقة المعنية مع طمس أسمائهم.

علاوة على ذلك، وفقاً لمحكمة العدل التابعة للاتحاد الأوروبي، «نظراً لأن شركة 'بافاريان لاجر' لم تقدم أي مبرر صريح ومشروع أو أي حجة مقنعة لإثبات ضرورة نقل تلك البيانات الشخصية إليها، لم تتمكن المفوضية من تقييم المصالح المختلفة للأطراف المعنية. كما أنها لم تكن قادرة على التحقق مما إذا كان هناك أي سبب لافتراض أن المصالح المشروعة لأصحاب البيانات قد تتضرر»، كما هو مطلوب بموجب لائحة حماية البيانات الخاصة بمؤسسات الاتحاد الأوروبي.

مثال: في قضية «'كلاينت أورث' وشبكة عمل مبيدات الآفات في أوروبا ضد الهيئة الأوروبية للسلامة الغذائية»،[107] تحققت محكمة العدل التابعة للاتحاد الأوروبي مما إذا كان قرار الهيئة الأوروبية للسلامة الغذائية (EFSA) برفض منح المدعيين الوصول الكامل إلى الوثائق ضرورياً لحماية حقوق الخصوصية و حماية بيانات الأشخاص الذين تشير إليهم الوثائق المعنية. وكانت هذه الوثائق عبارة عن مسودة تقرير إرشادي أعدته مجموعة عمل تابعة للهيئة الأوروبية للسلامة الغذائية بالتعاون مع خبراء خارجيين، بشأن وضع منتجات واقية للنباتات في السوق. في البداية، منحت الهيئة العامة للسلامة الغذائية الوصول الجزئي للمدعيين، مما منع وصولهما إلى بعض نسخ العمل لمشروع مسودة وثيقة التقرير الإرشادي. وبعد ذلك، منحتهما الهيئة حق الوصول إلى النسخة المسودة التي تضمنت التعليقات الفردية للخبراء الخارجيين. إلا أنها طمست أسماء الخبراء، مستشهدة بالمادة 8 (ب) من اللائحة 45/2001 بشأن معالجة البيانات الشخصية من قبل مؤسسات وهيئات الاتحاد الأوروبي والحاجة إلى حماية خصوصية الخبراء الخارجيين. وقد أيدت المحكمة العامة للاتحاد الأوروبي قرار الهيئة العامة للسلامة الغذائية في الحكم الابتدائي.

ولكن في الاستئناف الذي تقدم به المدعيين، ألغت محكمة العدل التابعة للاتحاد الأوروبي الحكم الابتدائي. وخلصت إلى أن نقل البيانات الشخصية في هذه الحالة كان ضرورياً للتأكد من حيادية كل من الخبراء الخارجيين في أداء مهامهم كعلماء ولضمان الحفاظ على شفافية عملية صنع القرار داخل الهيئة العامة للسلامة الغذائية. ووفقاً لمحكمة العدل التابعة للاتحاد الأوروبي، فإن الهيئة الأوروبية للسلامة الغذائية لم تحدد كيف أن الكشف عن أسماء الخبراء الخارجيين الذين أبدوا تعليقات محددة على مسودة وثيقة التقرير الإرشادي من شأنه أن يضر بمصالحهم المشروعة. إذ لا تُعد الحجةّ العامة، بأن الكشف عن المعلومات من المحتمل أن يخل بالخصوصية، كافيةً إذا لم تكن مدعومة بأدلة محددة وخاصة بكل حالة.

وفقاً لهذه الأحكام، يتطلب التدخل في الحق في حماية البيانات في سياق الوصول إلى الوثائق سبباً معيناً ومبرراً. ولا يمكن للحق في الوصول إلى الوثائق أن يطغى تلقائياً على الحق في حماية البيانات.[108]

تتشابه هذه المقاربة مع مقاربة المحكمة الأوروبية لحقوق الإنسان فيما يتعلق بالخصوصية والوصول الوثائق، كما يبين الحكم التالي. في الحكم الصادر في حق ماغيار هيلسينكي، ذكرت المحكمة الأوروبية لحقوق الإنسان أن المادة 10 لا تخول للفرد حق الوصول إلى المعلومات التي تملكها سلطة عامة ولا تجبر الحكومة على إطلاع الفرد على تلك المعلومات. إلا أن ذلك الحق أو الالتزام قد ينشأ - أولاً، عندما يكون الكشف عن المعلومات مفروضاً بموجب أمر قضائي اكتسب مفعولاً قانونياً؛ وثانياً، عندما يكون الوصول إلى المعلومات ضرورياً لكي يمارس

[107] محكمة العدل التابعة للاتحاد الأوروبي، القضية C-615/13P، «كلاينت أورث» و«شبكة عمل مبيدات الآفات في أوروبا» ضد الهيئة الأوروبية للسلامة الغذائية والمفوضية الأوروبية، 16 يوليو 2015.

[108] إطلع، مع ذلك، على المداولات المفصلة ضمن إصدار المشرف الأوروبي على حماية البيانات (2011): «وصول الجمهور إلى الوثائق التي تتضمن بيانات شخصية بعد الحكم الصادر في حق شركة 'بافاريان لاجر'»، بروكسيل، 24 مارس 2011.

الفرد حقه في حرية التعبير - لا سيما حرية تلقي المعلومات ونشرها - وعندما يشكل الحرمان منها تدخلاً في ذلك الحق.[109] ويجب تقييم ما إذا كان الحرمان من الوصول إلى المعلومات، ومدى تأثيره على حرية المدعي في التعبير في كل قضية على حدة وفي ضوء ظروفها الخاصة، بما في ذلك: (1) الغرض من طلب المعلومات؛ و(2) طبيعة المعلومات المطلوبة؛ و(3) ودور المدعي؛ و(4) ما إذا كانت المعلومات جاهزة ومتاحة.

مثال: في قضية «'ماغيار هيلسينكي بيزوتساغ' ضد المجر»،[110] طلب المدعي، وهو منظمة غير حكومية تُعنى بحقوق الإنسان، معلومات من الشرطة تتعلق بعمل محامي الدفاع بحكم المنصب، لإنجاز دراسة بشأن أداء نظام الدفاع العام في المجر. ولكن رفضت الشرطة منحه تلك المعلومات، معللة أنها تشكل بيانات شخصية لا يجوز الكشف عنها. بتطبيق المعايير السالفة الذكر، قضت المحكمة الأوروبية لحقوق الإنسان بحدوث تدخل في حق محمي بموجب المادة 10. وبشكل أدق، رغب المدعي في ممارسة الحق في نشر معلومات عن مسألة تخص المصلحة العامة، وسعى إلى الوصول إلى المعلومات لذلك الغرض، وكانت المعلومات ضرورية للمدعي حتى يمارس حقه في حرية التعبير. وكانت المعلومات المتعلقة بتعيين محاميي الدفاع العام ذات أهمية للمصلحة العامة. ولم يكن ثمة أي سبب يدعو إلى الشك في أن الاستطلاع المعني يتضمن معلومات تعهد المدعي بإطلاع الجمهور عليها والتي يحق لعامة الناس تلقيها. ولذلك كانت المحكمة مقتنعة بأن الوصول إلى المعلومات المطلوبة كان ضرورياً للمدعي لكي يقوم بالمهمة. وأخيراً، كانت المعلومات جاهزة ومتاحة.

خلصت المحكمة الأوروبية لحقوق الإنسان إلى أن الحرمان من الوصول إلى المعلومات في تلك الحالة قد أخل بجوهر حرية تلقي المعلومات. وعندما توصلت المحكمة إلى هذا الاستنتاج، دققت خصوصاً في الغرض من المعلومات المطلوبة ومساهمتها في نقاش عام مهم، وطبيعة المعلومات المطلوبة وما إذا كانت ذات أهمية للمصلحة العامة، والدور الذي يقوم به المدعي في المجتمع في هذه الحالة.

أشارت المحكمة في تعليلها إلى أن الدراسة التي اضطلعت بها المنظمة غير الحكومية همت سير العدالة والحق في محاكمة عادلة، وهو حق ذو أهمية قصوى بموجب الاتفاقية الأوروبية لحقوق الإنسان. ونظراً إلى أن المعلومات المطلوبة لا تتعلق ببيانات خارج نطاق المجال العام، فإن حقوق الخصوصية لأصحاب البيانات (محاميي الدفاع بحكم المنصب) لم تكن لتتضرر لو سمحت الشرطة للمدعي بالوصول إلى المعلومات. وكانت المعلومات التي طلبها المدعي ذات طبيعة إحصائية، وتتعلق بعدد المرات التي تم فيها تعيين المحامي بحكم المنصب لتمثيل المدعى عليهم في الدعاوى الجنائية العامة.

بالنسبة للمحكمة، وبالنظر إلى أن الدراسة كانت تهدف إلى المساهمة في نقاش مهم بشأن مسألة تهم المصلحة العامة، فإن أي قيود مفروضة على النشر الذي اقترحته المنظمة غير الحكومية كان ينبغي أن تخضع لأكبر قدر من التدقيق. وكانت المعلومات المعنية ذات أهمية للمصلحة العامة، لأن المصلحة العامة تشمل «الشؤون التي بإمكانها أن تثير جدلاً كبيراً، أو تهم مسألة اجتماعية مهمة، أو تتعلق بمشكلة يكون للجمهور مصلحة في إبلاغه بها».[111] ولذلك، فإنها تشمل لا محالة نقاشاً بشأن سير العدالة والمحاكمات العادلة، وهو ما شكل موضوع الدراسة التي أنجزها المدعي. بالموازنة بين مختلف الحقوق المعنية وبتطبيق مبدأ التناسب، قضت المحكمة الأوروبية لحقوق الإنسان بحدوث انتهاك غير مبرر لحقوق المدعي بموجب المادة 10 من الاتفاقية الأوروبية لحقوق الإنسان.

## 2.3.1. السرية المهنية

بموجب القانون الوطني، قد تخضع بعض الاتصالات المعينة للالتزام بالسرية المهنية. ويُفهم من السرية المهنية أنها واجب أخلاقي خاص ينشأ عنه التزام قانوني متأصل في مهن ووظائف معينة، ويستند إلى الأمانة والثقة. ويُجبر الأشخاص والمؤسسات التي تقوم بهذه الوظائف على كتمان المعلومات السرية التي تلقوها أثناء أداء مهامهم. وتنطبق السرية المهنية بصورة أوضح على مهنة الطب وخصوصية العلاقة

[109] المحكمة الأوروبية لحقوق الإنسان، القضية رقم 18030/11، ماغيار هيلسينكي بيزوتساغ ضد المجر [الغرفة الكبرى]، 8 نوفمبر 2016، الفقرة
[110] نفس المرجع السابق، الفقرة 181، والفقرات 187-200.
[111] نفس المرجع السابق، الفقرة 156.

بين المحامي وموكله، بالإضافة إلى إقرار الكثير من النظم القضائية بفرض التزام بالسرية المهنية على القطاع المالي. ولا تُعد السرية المهنية حقاً أساسياً، لكنها محمية من باب الحق في احترام الحياة الخاصة. على سبيل المثال، قضت محكمة العدل التابعة للاتحاد الأوروبي أنه في قضايا معينة، «قد يكون من الضروري حظر الكشف عن معلومات معينة مصنفة على أنها سرية، لحماية الحق الأساسي للجهة المعنية باحترام حياتها الخاصة المكرس في المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان والمادة 7 من ميثاق الحقوق الأساسية للاتحاد الأوروبي.[112] وطُلب أيضاً من المحكمة الأوروبية لحقوق الإنسان أن تحكم بشأن ما إذا كانت القيود المفروضة على السرية المهنية تشكل خرقاً للمادة 8 من الاتفاقية الأوروبية لحقوق الإنسان، كما هو موضح في الأمثلة المبرزة.

مثال: في قضية «'بروتيانو 'ضد رومانيا»،[113] تصرف المدعي بصفته محام لشركة تجارية كانت قد مُنعت من القيام بالمعاملات المصرفية عقب ادعاءات بالاحتيال. خلال التحقيق في القضية، أجازت المحاكم الرومانية لسلطات الادعاء اعتراض وتسجيل المكالمات الهاتفية لأحد شركاء الشركة خلال مدة معينة. وشملت التسجيلات والاعتراضات اتصالاته بمحاميه.

ادعى السيد بروتيانو أن ذلك شكل تدخلاً في حقه في احترام الحياة الخاصة ومراسلاته. وأبرزت المحكمة الأوروبية لحقوق الإنسان، في حكمها، مكانة علاقة المحامي بموكله وأهميتها. إن اعتراض مكالمات المحامي مع موكله شكل لا محالة اعتداءً على السرية المهنية التي كانت أساس العلاقة بين هذين الشخصين. في هذه الحالة، يستطيع المحامي أيضاً أن يشتكي من التدخل في حقه في احترام حياته الخاصة ومراسلاته. وقضت محكمة العدل التابعة للاتحاد الأوروبي بانتهاك المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان.

مثال: في قضية «'بريتو فيرينيو بيكسيفا فيلا-نوفا' ضد البرتغال»،[114] رفضت المدعية، وهي محامية، الكشف عن بياناتها المصرفية الشخصية للسلطات الضريبية على أساس السرية المهنية والسرية المصرفية. فتح مكتب المدعي العام تحقيقاً بشأن احتيال ضريبي، وطلب الإذن لتعليق السرية المهنية. فأمرت المحاكم الوطنية بتعليق قواعد السرية المهنية والسرية المصرفية، ورأت أن المصلحة العامة ينبغي لها أن تطغى على المصالح الخاصة للمدعية.

عندما وصلت القضية إلى المحكمة الأوروبية لحقوق الإنسان، قضت المحكمة بأن الاطلاع على البيانات المصرفية للمدعية يشكل تدخلاً في حقها في احترام السرية المهنية التي تقع ضمن نطاق الحياة الخاصة. وقد كان للتدخل أساس قانوني، لأنه استند إلى قانون الإجراءات الجنائية، وسعى إلى هدف مشروع. إلا أنه بعد التحقيق في ضرورة التدخل وتناسبه، أشارت المحكمة الأوروبية لحقوق الإنسان إلى أن الإجراءات المتعلقة برفع السرية تم القيام بها دون مشاركة المدعية وعلمها. ولذلك كانت المدعية غير قادرة على تقديم حججها. علاوة على ذلك، رغم أن القانون الوطني نص على وجوب استشارة رابطة المحامين في مثل هذه الإجراءات، فإن الرابطة لم تُستشر. وأخيراً، لم تكن المدعية تملك خيارا فعالاً للطعن في رفع السرية ، ولا أي سبيل من سبل الانتصاف يمكنها من الطعن في الإجراء. ونظراً إلى انعدام الضمانات الإجرائية والرقابة القضائية الفعالة على الإجراء الذي يعلق واجب السرية، خلصت المحكمة الأوروبية لحقوق الإنسان إلى أنه تم انتهاك المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان.

غالباً ما يكون التفاعل بين السرية المهنية وحماية البيانات متضارباً. فمن ناحية، تساعد قواعد حماية البيانات والضمانات التي يكرسها التشريع على ضمان السرية المهنية، على سبيل المثال، تسعى القواعد التي تشترط على المراقبين والمعالجين تنفيذ تدابير صارمة للحفاظ على أمن البيانات، من بين أمور أخرى، إلى الحيلولة دون فقدان سرية البيانات الشخصية المحمية بموجب السرية المهنية. بالإضافة إلى ذلك، تسمح اللائحة العامة لحماية البيانات للاتحاد الأوروبي بمعالجة بيانات الصحة التي تشكل فئات خاصة من البيانات الشخصية تستحق حماية أقوى، لكنها تشترط وجود تدابير مناسبة ومعينة لصون حقوق أصحاب البيانات، لا سيما الحق في السرية المهنية.[115]

[112] محكمة العدل التابعة للاتحاد الأوروبي، القضية T-462/12 R، «مجموعة بيلكينطون (شركة محدودة)» ضد المفوضية الأوروبية، الأمر الصادر عن رئيس المحكمة العامة، 11 مارس 2013، الفقرة 44.

[113] المحكمة الأوروبية لحقوق الإنسان، القضية 30181/05، بروتيانو ضد رومانيا، 3 فبراير 2015.

[114] المحكمة الأوروبية لحقوق الإنسان، القضية 96436/10، بريتو بفيرينيو بيكسيفا فيلا-نوفا ضد البرتغال، 1 ديسمبر 2015.

[115] اللائحة العامة لحماية البيانات، المادتان 9 (2) (ج) و 9 (3).

ومن ناحية أخرى، قد تقيد الالتزامات بالسرية المهنية المفروضة على المراقبين والمعالجين فيما يتعلق ببيانات شخصية معينة حقوق أصحاب البيانات، ولا سيما الحق في تلقي المعلومات. وعلى الرغم من أن اللائحة العامة لحماية البيانات تتضمن قائمة موسعة بالمعلومات التي تحتاج، مبدئياً، إلى تقديمها إلى صاحب البيانات عندما لا تكون البيانات الشخصية قد تم الحصول عليها منه، فإن شرط الكشف هذا لا ينطبق على الحالات التي يجب فيها أن تظل البيانات الشخصية سرية نظراً إلى الالتزام بالسرية المهنية الذي يقتضيه القانون الوطني أو قانون الاتحاد الأوروبي.[116]

تنص اللائحة العامة لحماية البيانات على إمكانية اعتماد الدول الأعضاء، بحكم القانون، قواعد خاصة لصون الالتزامات بالسرية المهنية أو غيرها من الالتزامات بالسرية المماثلة والتوفيق بين الحق في حماية البيانات الشخصية والالتزام بالسرية المهنية.[117]

تنص اللائحة العامة لحماية البيانات على أنه يجوز للدول الأعضاء اعتماد قواعد خاصة بشأن صلاحيات الهيئات الإشرافية فيما يتعلق بالمراقبين والمعالجين الذي يخضعون للالتزام بالسرية المهنية. وتتعلق هذه القواعد الخاصة بصلاحية الوصول إلى مرافق المراقب أو المعالج، ومعداته المستخدمة في معالجة البيانات والبيانات الشخصية التي يُحتفظ بها، عندما تكون تلك البيانات الشخصية قد تم تلقيها في سياق نشاط يشمله الالتزام بالسرية. ولذلك، يجب على الهيئات الإشرافية المكلفة بحماية البيانات احترام الالتزامات بالسرية المهنية التي تلزم المراقبين والمعالجين. علاوة على ذلك، يخضع أيضاً أعضاء الهيئات الإشرافية أنفسهم لواجب السرية المهنية خلال مدة شغل المنصب وبعدها، إذ يمكنهم الاطلاع على معلومات سرية خلال أداء مهامهم. وتنص المادة 54 (2) صراحة على التزامهم بالسرية المهنية فيما يخص تلك المعلومات السرية.

تقتضي اللائحة العامة لحماية البيانات من الدول الأعضاء أن تُشعر المفوضية بالقواعد التي تعتمدها للتوفيق بين حماية البيانات والمبادئ التي تكرسها اللائحة من جهة والتزام السرية المهنية من جهة أخرى.

### 3.3.1. حرية الدين والمعتقد

تحمي المادة 9 من الاتفاقية الأوروبية لحقوق الإنسان (حرية الفكر والوجدان والدين) والمادة 10 من ميثاق الاتحاد الأوروبي للحقوق الأساسية حرية الدين والمعتقد. وتُعد البيانات الشخصية التي تكشف عن المعتقدات الدينية أو الفلسفية بيانات حساسة بموجب كل من قانون الاتحاد الأوروبي وقانون مجلس أوروبا، وتشترط معالجتها واستخدامها حماية معززة.

مثال: كان المدعي في قضية «'سيناك إيسيك' ضد تركيا»[118] عضواً في الطائفة الدينية العلوية التي تتأثر عقيدتها بالصوفية وغيرها من المعتقدات التي كانت سائدة قبل الإسلام والتي يعتبرها بعض العلماء ديناً مختلفاً و يعتبرها البعض الآخر جزءاً من الإسلام. واشتكى المدعي من أن بطاقة الهوية الخاصة به احتوت، رغما عنه، على إطار يدل على أن دينه هو «الإسلام» لا «العلوية». ورفضت المحاكم الوطنية طلبه استبدال «الإسلام» بـ«العلوية» في بطاقة الهوية الخاصة به بحجة أن تلك الكلمة تعني طائفة فرعية من الإسلام وليس ديناً مختلفاً، ثم اشتكى المدعي أمام المحكمة الأوروبية لحقوق الإنسان من إجباره على الكشف عن عقيدته، دون موافقته، لأنه كان ضرورياً أن يُشار إلى دين الشخص في بطاقة الهوية وأن ذلك انتهاك لحقه في حرية الدين والوجدان، لا سيما بالنظر إلى أن تسمية «الإسلام» في بطاقة الهوية الخاصة به لم تكن صحيحة.

[116] نفس المرجع السابق، المادة 14 (5) (د).
[117] نفس المرجع السابق، الحيثية 164 والمادة 90.
[118] قضية المحكمة الأوروبية لحقوق الإنسان رقم 21924/05 المتعلقة بسيناك إيسيك ضد تركيا والمؤرخة في 02 فبراير 2010.

مثال: كان المدعي في قضية «'سيناك إيسيك' ضد تركيا»[118] عضواً في الطائفة الدينية العلوية التي تتأثر عقيدتها بالصوفية وغيرها من المعتقدات التي كانت سائدة قبل الإسلام والتي يعتبرها بعض العلماء ديناً مختلفاً و يعتبرها البعض الآخر جزءاً من الإسلام. واشتكى المدعي من أن بطاقة الهوية الخاصة به احتوت، رغما عنه، على إطار يدل على أن دينه هو «الإسلام» لا «العلوية». ورفضت المحاكم الوطنية طلبه استبدال «الإسلام» بـ«العلوية» في بطاقة الهوية الخاصة به بحجة أن تلك الكلمة تعني طائفة فرعية من الإسلام وليس ديناً مختلفاً، ثم اشتكى المدعي أمام المحكمة الأوروبية لحقوق الإنسان من إجباره على الكشف عن عقيدته، دون موافقته، لأنه كان ضرورياً أن يُشار إلى دين الشخص في بطاقة الهوية وأن ذلك انتهاك لحقه في حرية الدين والوجدان، لا سيما بالنظر إلى أن تسمية «الإسلام» في بطاقة الهوية الخاصة به لم تكن صحيحة.

ذكرت المحكمة الأوروبية لحقوق الإنسان مجدداً أن حرية الدين تستلزم حرية الشخص في إظهار دينه في المجتمع الذي يتشاركه مع الآخرين، وفي العلن، وضمن محيط الأشخاص الذين يشاركونه نفس العقيدة، وحتى عندما يكون بمفرده وفي حياته الخاصة. وكانت التشريعات الوطنية سارية المفعول آنذاك تلزم الأفراد بحمل بطاقة هوية، وهي وثيقة كان يجب إظهارها بناءً على طلب أي سلطة عامة أو مقاولة خاصة، تدل على دينهم. وقد فشل ذلك الإلزام في الإقرار بأن حق المرء في إظهار دينه كان يخول العكس أيضاً، أي حق المرء في عدم الاضطرار إلى الكشف عن معتقداته. وعلى الرغم من أن الحكومة احتجت بأنه قد تم تعديل التشريعات الوطنية بما يمكن الأفراد من طلب الإبقاء على الإطار الخاص بالدين في بطاقة الهوية الخاصة بهم فارغاً، فإنه في نظر المحكمة يمكن أن يشكل مجرد الاضطرار إلى تقديم طلب لحذف الدين كشفاً عن معلومات بشأن مواقفهم من الدين. وفضلاً عن ذلك، عندما تحتوي بطاقات الهوية على إطار خاص بديانة صاحبها، فإن تركه فارغاً تكون له دلالة خاصة، لأن حاملي بطائق الهوية التي لا تحتوي على معلومات عن الدين يتميزون عن أولئك الذين يحملون بطائق هوية تحتوي على إشارة إلى معتقداتهم. وخلصت المحكمة الأوروبية لحقوق الإنسان إلى أن التشريعات الوطنية تنتهك المادة 9 من الاتفاقية الأوروبية لحقوق الإنسان.

إلا أنه قد يتطلب تسيير الكنائس والجمعيات والمجتمعات المحلية الدينية معالجة المعلومات الشخصية لأعضائها لتمكين التواصل وتنظيم الأنشطة داخل الطائفة. لذلك، غالباً ما تنفذ الكنائس والجمعيات الدينية قواعد متعلقة بمعالجة البيانات الشخصية. وفقاً للمادة 91 من اللائحة العامة لحماية البيانات، عندما تكون تلك القواعد شاملة، يمكن أن تظل سارية المفعول، شريطة جعلها متوافقة مع أحكام اللائحة. ويجب أن تخضع الكنائس والجمعيات الدينية التي تتبع مثل هذه القواعد لرقابة هيئة إشرافية مستقلة، والتي يمكن أن تكون خاصة بها، شريطة أن تفي بمقتضيات اللائحة العامة لحماية البيانات الخاصة بتلك السلطات.[119]

قد تضطلع المنظمات الدينية بمعالجة البيانات الشخصية لعدة أسباب - على سبيل المثال، للحفاظ على الاتصال بأعضائها أو لإبلاغ معلومات عن الأحداث والاحتفالات الدينية والخيرية طور التنظيم. في بعض الدول، تحتاج الكنائس إلى الاحتفاظ بسجلات لأعضائها لأسباب ضريبية، لأن الانخراط في المؤسسات الدينية بإمكانه أن يؤثر على الضرائب التي يدفعها الأفراد. وفي جميع الأحوال، وبموجب القانون الأوروبي، فإن البيانات التي تكشف عن المعتقدات الدينية تُعد بيانات حساسة، ويجب على الكنائس أن تتحمل مسؤولية التعامل معها ومعالجتها، لا سيما لأن المعلومات التي تعالجها المنظمات الدينية تتعلق في أغلب الأحيان بالأطفال أو المسنين أو غيرهم من أفراد الفئات الهشة في المجتمع.

## 4.3.1. حرية الفنون والعلوم

من الحقوق الأخرى التي يجب التوفيق بينها وبين الحقين في احترام الحياة الخاصة وحماية البيانات حرية الفنون والعلوم، وهو حق محمي صراحة بموجب المادة 13 من ميثاق الاتحاد الأوروبي للحقوق الأساسية. يستند هذا الحق في المقام الأول إلى الحق في حرية الفكر والتعبير ويتعين ممارسته بمراعاة المادة 1 من ميثاق الحقوق الأساسية للاتحاد الأوروبي (الكرامة الإنسانية). وترى المحكمة الأوروبية لحقوق الإنسان أن حرية الفنون محمية بموجب المادة 10 من الاتفاقية الأوروبية لحقوق الإنسان،[120] كما يمكن أن يخضع الحق المحمي

[118] قضية المحكمة الأوروبية لحقوق الإنسان رقم 21924/05 المتعلقة بسيناك إيسيك ضد تركيا والمؤرخة في 02 فبراير 2010.
[119] اللائحة العامة لحماية البيانات، المادة 91 (2).
[120] قضية المحكمة الأوروبية لحقوق الإنسان رقم 10737/84 المتعلقة بمولر وآخرين ضد سويسرا والمؤرخة في 24 مايو 1988

بموجب المادة 13 من ميثاق الحقوق الأساسية للاتحاد الأوروبي أيضاً للقيود الواردة في المادة 52 (1) من ميثاق الحقوق الأساسية للاتحاد الأوروبي، والتي يمكن أن تُفسَّر أيضاً من منظور المادة 10 (2) من الاتفاقية الأوروبية لحقوق الإنسان.[121]

مثال: في قضية «رابطة الفنانين التشكيليين ضد النمسا»،[122] حظرت المحاكم النمساوية على الجمعية المدعية الاستمرار في عرض لوحة فنية تحتوي على صور فوتوغرافية لرؤوس مختلف الشخصيات العمومية في أوضاع جنسية. ورفع نائب نمساوي، كانت صورته الفوتوغرافية قد استُخدمت في هذه اللوحة الفنية، دعوى قضائية في حق الجمعية المدعية، ملتمساً أمراً احترازياً يحظر عليها عرض اللوحة الفنية. وبالفعل، أصدرت المحكمة الوطنية الأمر الاحترازي. من جهتها ذكرت المحكمة الأوروبية لحقوق الإنسان مجدداً أن المادة 10 من الاتفاقية الأوروبية لحقوق الإنسان تشمل نشر الأفكار التي تهين أو تصدم أو تضايق الدولة أو أي فئة من السكان. إن اللذين يبدعون أعمالاً فنية، أو ينجزونها أو يوزعونها أو يعرضونها يساهمون في تبادل الأفكار والآراء، وتلتزم الدولة بعدم الاعتداء، دون مبرر، على حريتهم في الفكر. ونظراً إلى أن اللوحة الفنية كانت عبارة عن خليط من الملصقات (أي «كولاج») ولم تستخدم سوى صوراً فوتوغرافية لرؤوس الأشخاص، وأن أجسادهم رُسمت بطريقة غير واقعية ومبالغ فيها، ما لا يهدف بوضوح إلى إبراز الواقع أو حتى الدلالة عليه، ذكرت المحكمة الأوروبية لحقوق الإنسان أيضاً أن «اللوحة الفنية من المستبعد أن تُفهم على أنها تتطرق إلى تفاصيل عن الحياة الخاصة [للشخص الذي يظهر عليها]، بل تتعلق بمكانته العامة بصفته سياسياً» وأنه «بهذه الصفة كان على الشخص [الذي يظهر عليها] أن يبدي تسامحاً أكبر تجاه الانتقاد». وبترجيحها لمختلف المصالح المعنية، استنتجت المحكمة الأوروبية لحقوق الإنسان أن الحظر اللامحدود على الاستمرار في عرض للوحة الفنية لم يكن متناسباً وخلصت إلى أنه تم انتهاك المادة 10 من الاتفاقية الأوروبية لحقوق الإنسان.

يقر القانون الأوروبي لحماية البيانات أيضاً بالقيمة الخاصة للعلم في المجتمع. وتسمح اللائحة العامة لحماية البيانات والاتفاقية 108 المحدثة بالاحتفاظ بالبيانات لمدد أطول ما دامت ستتم معالجتها لأغراض البحث العلمي أو التاريخي لا غير. إضافة إلى ذلك، وبغض النظر عن الغرض الأصلي لمعالجة معينة، فإن الاستخدام اللاحق للبيانات الشخصية لأغراض البحث العلمي لا يمكن أن يُعتبر غرضاً غير متوافق.[123] وفي نفس الوقت، يتعين تفعيل الضمانات المناسبة لتلك المعالجة لحماية حقوق وحريات أصحاب البيانات. وقد يتيح قانون الاتحاد الأوروبي أو الدولة العضو استثناءات لحقوق أصحاب البيانات، مثل الحق في الوصول والتصحيح وتقييده المعالجة والاعتراض عليها عندما يتعلق الأمر بمعالجة بياناتهم الشخصية لأغراض البحث العلمي أو التاريخي أو لأغراض إحصائية (انظر أيضاً الجزء 1.6 و الجزء 4.9).

## 5.3.1. حماية الملكية الفكرية

تكرس المادة 1 من البروتوكول الأول الملحق بالاتفاقية الأوروبية لحقوق الإنسان والمادة 17 (1) من ميثاق الاتحاد الأوروبي للحقوق الأساسية الحق في حماية الملكية. ومن بين الجوانب المهمة للحق في الملكية، والذي له صلة خاصة بحماية البيانات، حماية الملكية الفكرية، المشار إليها صراحة في المادة 17 (2) من ميثاق الحقوق الأساسية للاتحاد الأوروبي. كما تهدف عدة أوامر توجيهية في النظام القانوني للاتحاد الأوروبي إلى حماية الملكية الفكرية حماية فعالة، ولا سيما حق التأليف والنشر. ولا تشمل الملكية الفكرية الملكية الأدبية والفنية فحسب، وإنما أيضاً براءة الاختراع والعلامة التجارية والحقوق المرتبطة بها.

وكما أوضحت السوابق القضائية لمحكمة العدل التابعة للاتحاد الأوروبي، يجب التوفيق بين حماية الحق الأساسي في الملكية وحماية الحقوق الأساسية الأخرى، ولا سيما الحق في حماية البيانات.[124] وكانت ثمة حالات طالبت فيها مؤسسات حماية حقوق النشر والتأليف من مقدمي خدمات الإنترنت الكشف عن هوية مستخدمي منصات مشاركة الملفات على الإنترنت، والتي غالباً ما تمكن مستخدمي الإنترنت من تحميل المقاطع الموسيقية مجاناً رغم أنها محمية بموجب حقوق النشر والتأليف.

[121] توضيحات متعلقة بميثاق الحقوق الأساسية، الجريدة الرسمية لسنة 2007 القضية رقم 303..

[122] قضية المحكمة الأوروبية لحقوق الإنسان رقم 68354/01 المتعلقة برابطة الفنانين التشكيليين ضد النمسا والمؤرخة في 25 يناير 2007، الفقرتين 26 و34.

[123] اللائحة العامة لحماية البيانات، المادة 5 (1) (ب) والاتفاقية المحدثة 108، المادة 5 (4) (ب).

[124] قضية محكمة العدل التابعة للاتحاد الأوروبي رقم 275/06 المتعلقة بمنتجي الموسيقى إسبانيا (بروموسيكاي) ضد تيليفونيكا إسبانيا (شركة ذات مساهم واحد) [الغرفة الكبرى] والمؤرخة في 29 يناير 2008، الفقرات من 62 إلى 68.

مثال: تتعلق قضية «'بروموسيكاي' ضد 'تيليفونيكا إسبانيا'»[125] برفض مقدم خدمات الإنترنت الإسباني «تيليفونيكا» الكشف لـ«بروموسيكاي»، وهي منظمة غير ربحية لمنتجي الموسيقى وناشري التسجيلات الموسيقية والسمعية البصرية، عن البيانات الشخصية لبعض الأشخاص الذين زودتهم بخدمات الوصول إلى الإنترنت. وسعت «بروموسيكاي» إلى الكشف عن المعلومات حتى تشرع في إقامة دعوى مدنية في حق أولئك الأشخاص الذين زعمت أنهم كانوا يستخدمون برنامجاً لتبادل الملفات يتيح الوصول إلى تسجيلات صوتية كان أعضاء «بروموسيكاي» يملكون حقوق استغلالها.

أحالت المحكمة الإسبانية القضية إلى محكمة العدل التابعة للاتحاد الأوروبي، سائلة عما إذا كان يجب تقديم تلك البيانات الشخصية، بموجب قانون الاتحاد الأوروبي، في سياق الدعاوى المدنية لضمان الحماية الفعلية لحقوق النشر والتأليف. وأشارت إلى الأوامر التوجيهية 2000/31 و2001/29 و2004/48، التي قُرأت أيضاً في ضوء المادتين 17 و47 من ميثاق الحقوق الأساسية للاتحاد الأوروبي. وخلصت محكمة العدل التابعة للاتحاد الأوروبي إلى أن هذه الأوامر التوجيهية الثلاثة، بالإضافة إلى الأمر التوجيهي المتعلق بالخصوصية الإلكترونية (الأمر التوجيهي 2002/58)، لا تمنع الدول الأعضاء من أن تنص على التزام بكشف البيانات الشخصية في سياق الدعاوى المدنية لضمان حماية فعلية لحقوق النشر والتأليف.

كما أشارت محكمة العدل التابعة للاتحاد الأوروبي إلى أن القضية أثارت بذلك مسألة الحاجة إلى التوفيق بين مقتضيات حماية مختلف الحقوق الأساسية - أي بين الحق في احترام الحياة الخاصة والحقين في حماية الملكية وفي الانتصاف الفعال.

وخلصت إلى أن «الدول الأعضاء يجب عليها، عند إدماج الأوامر التوجيهية المذكورة سلفاً، أن تحرص على الاعتماد على تفسير تلك الأوامر بما يسمح بإيجاد توازن بين مختلف الحقوق الأساسية المحمية بموجب النظام القانوني للاتحاد الأوروبي. علاوة على ذلك، لا يجب على السلطات والدول الأعضاء، عند تنفيذ التدابير التي تدمج تلك الأوامر التوجيهية، الاعتماد على القانون الوطني بطريقة تنسجم مع تلك الأوامر فحسب، وإنما أيضاً التيقن من عدم الاعتماد على تفسيرها بما يخالف تلك الحقوق الأساسية أو غيرها من المبادئ العامة لقانون الاتحاد الأوروبي، مثل مبدأ التناسب.[126]

مثال: تتعلق قضية شركة «'بونيي أوديو' المحدودة وآخرين ضد شركة 'بيرفيكت كوميونيكايشن السويد»' المحدودة)[127] بالتوفيق بين حقوق الملكية الفكرية وحماية البيانات الشخصية، حيث أن المدعين - وهم خمس شركات للنشر تملك حقوق النشر والتأليف لـ27 كتاباً صوتياً - أقاموا دعوى قضائية أمام المحكمة السويدية، مدعين أن حقوق النشر والتأليف هذه قد انتُهكت بواسطة خادم بروتوكول نقل الملفات (بروتوكول نقل الملفات الذي يتيح مشاركة الملفات ونقل البيانات عبر الإنترنت). وطلب المدعون من مقدم خدمات الإنترنت الكشف عن اسم وعنوان الشخص صاحب عنوان بروتوكول الإنترنت الذي أُرسلت منه الملفات. اعترض مقدم خدمات الإنترنت، وهي شركة تُدعى «إيفون» (ePhone)، على الدعوى، زاعماً أنها تنتهك الأمر التوجيهي 2006/24 (الأمر التوجيهي المتعلق بالاحتفاظ بالبيانات - الذي أُلغي سنة 2014).

وأحالت المحكمة السويدية القضية إلى محكمة العدل التابعة للاتحاد الأوروبي، سائلة عما إذا كان الأمر التوجيهي 2006/24 يستبعد تطبيق مقتضى وطني مستند إلى المادة 8 من الأمر التوجيهي 2004/48 (الأمر التوجيهي المتعلق بتنفيذ حقوق الملكية الفكرية)، الذي يسمح بإصدار أمر احترازي يلزم مزودي خدمات الإنترنت بالكشف لمالكي حقوق النشر والتأليف عن معلومات متعلقة بالمشتركين أصحاب عناوين بروتوكول الإنترنت التي زُعم استخدامها في الانتهاكات. واستند السؤال إلى افتراض أن المدعي قدم أدلة واضحة على انتهاك حق معين من حقوق النشر والتأليف وأن هذا التدبير متناسب.

[125] نفس المرجع السابق، الفقرتين 54 و60.

[126] نفس المرجع السابق، الفقرتين 65 و68، إطلع أيضاً على قضية محكمة العدل التابعة للاتحاد الأوروبي رقم 360/10 المتعلقة بالشركة البلجيكية للمؤلفين والملحنين والموزعين الموسيقيين (SABAM) (CVBA) ضد نيتلوغ (شركة مغفلة) والمؤرخة في 16 فبراير 2012.

[127] قضية محكمة العدل التابعة للاتحاد الأوروبي رقم C-461/10 المتعلقة بالشركات المحدودة «بونيي أوديو» و«إيربوكس» و«نورستيدتس فورلاغسفروب» و«بيرات فورلاغيت» و«ستوريسايد» ضد الشركة المحدودة «بيرفيكت كوميونيكايشن السويد» والمؤرخة في 19 أبريل 2012.

أشارت محكمة العدل التابعة للاتحاد الأوروبي إلى أن الأمر التوجيهي 2006/24 تطرق حصراً إلى التعامل مع البيانات التي ينشئها مقدمو خدمات الاتصالات الإلكترونية والاحتفاظ بها لأغراض التحقيق والكشف عن الجرائم الخطيرة ومقاضاة مرتكبيها وتبليغها إلى السلطات الوطنية المختصة. ولذلك، فإن المقتضى الوطني الذي يدمج الأمر التوجيهي المتعلق بتنفيذ حقوق الملكية الفكرية يقع خارج نطاق الأمر التوجيهي 2006/24 ولذلك لا يستبعده ذلك الأمر التوجيهي.[128] فيما يتعلق بالإبلاغ عن الاسم والعنوان المعنيين، واللذين سعى المدعون إلى الحصول عليها، قضت محكمة العدل التابعة للاتحاد الأوروبي بأن ذلك الإجراء يشكل معالجة للبيانات الشخصية، وأنه يقع ضمن نطاق الأمر التوجيهي 2002/58 (الأمر التوجيهي المتعلق بالخصوصية الإلكترونية). وأشارت أيضاً إلى أن الإبلاغ عن تلك البيانات كان مطلوباً في الدعوى المدنية لصالح مالك حقوق النشر والتأليف لضمان حماية فعالة لحقوق النشر والتأليف وبذلك يقع أيضاً، من حيث موضوعه، ضمن نطاق الأمر التوجيهي 48/2004.[129]

استنتجت محكمة العدل التابعة للاتحاد الأوروبي وجوب تفسير الأمرين التوجيهيين 2002/58 و2004/48 بما لا يستبعد التشريعات الوطنية مثل التشريع المعني بالدعوى الرئيسية، طالما يمكن ذلك التشريع المحكمة التي عُرضت عليها دعوى لإصدار أمر للكشف عن البيانات الشخصية من أن توازن بين المصالح المتضاربة للأطراف المعنية، استناداً إلى وقائع كل قضية والمراعاة الواجبة لمقتضيات مبدأ التناسب.

## 6.3.1. حماية البيانات والمصالح الاقتصادية

في العصر الرقمي أو عصر البيانات الضخمة، تُوصف البيانات بـ«النفط الجديد» للاقتصاد لتشجيع الابتكار والإبداع.[130] وقد أنشأت العديد من الشركات نماذج تجارية متينة حول معالجة البيانات، وتتعلق تلك المعالجة في غالب الأحيان بالبيانات الشخصية. وقد تعتقد بعض الشركات أن قواعد معينة تتعلق بحماية البيانات الشخصية قد تنشأ عنها، من الناحية العملية، التزامات مرهقة للغاية قد تؤثر على مصالحها الاقتصادية. ولذلك، يُثار السؤال عما إذا كانت المصالح الاقتصادية للمراقبين والمعالجين، أو مصالح عامة الناس، باستطاعتها أن تبرر تقييد الحق في حماية البيانات.

مثال: في قضية «غوغل إسبانيا»،[131] قضت محكمة العدل التابعة للاتحاد الأوروبي بأن الأفراد يملكون، في ظروف معينة، الحق في الطلب من محركات البحث إزالة نتائج البحث من فهرس البحث الخاص بها. وأشارت محكمة العدل التابعة للاتحاد الأوروبي في تعليلها إلى أن استخدام محركات البحث ونتائج البحث المدرجة في قوائم بإمكانها أن تنشئ ملفاً شخصياً مفصلاً للفرد. وقد تخص هذه المعلومات جانباً كبيراً من الحياة الشخصية للفرد ولم تكن ليُعثر عليها أو يُربط بعضها بالبعض بسهولة لولا وجود محرك البحث. وبذلك يُحتمل أن تشكل تدخلاً فادحاً في الحقين الأساسيين في الخصوصية وحماية البيانات الشخصية لأصحاب البيانات.

ودققت محكمة العدل التابعة للاتحاد الأوروبي فيما إذا كان التدخل يمكن تبريره. وفيما يتعلق بالمصلحة الاقتصادية للشركة صاحبة محرك البحث في إجراء المعالجة، قالت محكمة العدل التابعة للاتحاد الأوروبي إنه «من الواضح أن [التدخل] لا يمكن تبريره بمجرد أن مشغل محرك البحث له مصلحة اقتصادية في تلك المعالجة»، وإنه «مبدئياً» يطغى الحقان الأساسيان بموجب المادتين 7 و8 من ميثاق الحقوق الأساسية للاتحاد الأوروبي على تلك المصلحة الاقتصادية ومصلحة عامة الناس في العثور على تلك المعلومات عند القيام ببحث يتعلق باسم صاحب البيانات.[132]

من بين الاعتبارات الأساسية للقانون الأوروبي لحماية البيانات أنه يتيح للأفراد سيطرة أكثر على بياناتهم الشخصية. ففي العصر الرقمي على وجه الخصوص، ثمة تباين بين قوة الكيانات التجارية التي تعالج وتصل إلى كميات ضخمة من البيانات الشخصية وبين قوة الأفراد الذين يملكون تلك البيانات للسيطرة على معلوماتهم. وتنهج محكمة العدل التابعة للاتحاد الأوروبي نهجاً خاصاً بكل قضية على حدة عند الموازنة

[128] نفس المرجع السابق، الفقرتين 40 و41.

[129] نفس المرجع السابق، الفقرتين 52 و54. إطلع ايضاً على قضية محكمة العدل التابعة للاتحاد الأوروبي رقم 275/06 المتعلقة بمنتجي الموسيقى إسبانيا (بروموسيكاي) ضد تيليفونيكا إسبانيا (شركة ذات مساهم واحد) [الغرفة الكبرى] والمؤرخة في 29 يناير 2008، الفقرة 58.

[130] إطلع، على سبيل المثال، على جريدة «فايننشل تايمز» (2016)، «البيانات هي النفط الجديد... من الذي سيملكها؟» الصادرة في 16 نوفمبر 2016.

[131] قضية محكمة العدل التابعة للاتحاد الأوروبي رقم 131/12 المتعلقة بغوغل إسبانيا (شركة محدودة) التابعة لشركة غوغل ضد الوكالة الإسبانية لحماية البيانات (APED) وماريو كوستيخا غونساليس [الغرفة الكبرى] والمؤرخة في 13 مايو 2014.

[132] نفس المرجع السابق، الفقرتين 81 و97.

بين حماية البيانات والمصالح الاقتصادية - مثل مصالح الأطراف الثالثة فيما يتعلق بشركات المساهمة والشركات ذات المسؤولية المحدودة، كما هو موضح في الحكم الصادر في قضية «ماني».

مثال: تتعلق قضية «ماني»[133] بإدراج البيانات الشخصية لأحد الأفراد في سجل تجاري عام. وكان السيد ماني قد طلب من الغرفة التجارية لمدينة ليتشي حذف بياناته الشخصية من ذلك السجل، بعدما اكتشف أن العملاء المحتملين سيلجؤون إلى السجل وسيطلعون على أنه قد كان مديراً لشركة أُعلن إفلاسها منذ أكثر من عقد. وقد أثرت هذه المعلومات على عملاءه المحتملين ويمكن أن يكون لها أثر سلبي على مصالحه التجارية.

طُلب من محكمة العدل التابعة للاتحاد الأوروبي أن تحدد ما إذا كان قانون الاتحاد الأوروبي يعترف بحق المرء في أن تُمحى بياناته في تلك القضية. وعندما توصلت المحكمة إلى استنتاجها، وازنت بين قواعد الاتحاد الأوروبي لحماية البيانات والمصلحة الاقتصادية للسيد ماني في حذف المعلومات المتعلقة بإفلاس شركته السابقة وبين مصلحة عامة الناس في الوصول إلى المعلومات. وأحاطت علماً على النحو الواجب أن الكشف عن السجل العام للشركات منصوص عليه بموجب القانون، لا سيما الأمر التوجيهي للاتحاد الأوروبي الرامي إلى جعل وصول الأطراف الثالثة إلى معلومات الشركات أكثر يسراً. وكان الكشف مهماً لحماية مصالح الأطراف الثالثة التي قد ترغب في القيام بأعمال تجارية مع شركة معينة، لأن الضمانات الوحيدة التي تقدمها شركات المساهمة والشركات ذات المسؤولية المحدودة للأطراف الثالثة هي أصولها. ولذلك «ينبغي الكشف عن الوثائق الأساسية للشركة المعنية حتى تتمكن الأطراف الثالثة من التحقق من محتوياتها وغيرها من المعلومات المتعلقة بالشركة، لا سيما بيانات الأشخاص المخول لهم إلزام الشركة».[134]

نظراً إلى أهمية الهدف المشروع الذي يُسعى إليه من خلال السجل، قضت محكمة العدل التابعة للاتحاد الأوروبي بأن السيد ماني لا يملك الحق في الحصول على محو بياناته الشخصية، لأن الحاجة إلى حماية مصالح الأطراف الثالثة فيما يتعلق بشركات المساهمة والشركات ذات المسؤولية المحدودة، وضمان اليقين القانوني، والتجارة العادلة، وبالتالي، الأداء السليم للسوق الداخلي، تطغى على حقوقه بموجب تشريعات حماية البيانات. ويصح ذلك خصوصاً بالنظر إلى أن الأفراد الذين يختارون المشاركة في التجارة من خلال شركات المساهمة والشركات ذات المسؤولية المحدودة يدركون أنهم مطالبون بالكشف عن المعلومات المتعلقة بهويتهم ووظائفهم.
وفي حين استنتجت محكمة العدل التابعة للاتحاد الأوروبي عدم وجود أسباب داعية إلى محو البيانات في هذه القضية، أقرت المحكمة فعلاً وجود الحق في الاعتراض على المعالجة، مشيرة إلى أنه «لا يمكن استبعاد إمكانية وجود حالات معينة تبرر فيها الأسباب الغالبة والمشروعة المتعلقة بقضية معينة للشخص المعني استثنائياً أن الوصول إلى البيانات الشخصية التي تم إدخالها في السجل يقتصر، عند انقضاء مدة طويلة بما يكفي، على الأطراف الثالثة التي قد تبدي مصلحة معينة في الاطلاع عليها».[135]

ذكرت محكمة العدل التابعة للاتحاد الأوروبي أنه، في كل قضية، وفيما يتعلق بجميع الظروف ذات الصلة بالفرد، يُترك للمحاكم الوطنية تقدير وجود أو غياب الأسباب المشروعة والطاغية التي يمكن أن تبرر استثنائياً تقييد وصول الأطراف الثالثة إلى البيانات الشخصية الواردة في سجلات الشركات. غير أنها أوضحت بخصوص قضية السيد ماني أن مجرد الادعاء بأن الكشف عن بياناته الشخصية الموجودة في السجل له أثر على عملائه لا يمكن أن يُحتسب سبباً مشروعاً وطاغياً، فالعملاء المحتملون للسيد ماني لهم مصلحة مشروعة في الاطلاع على المعلومات المتعلقة بإفلاس شركته السابقة.

إن التدخل في الحقين الأساسيين في الحياة الخاصة وحماية البيانات الشخصية للسيد ماني وغيره من الأشخاص المتضمنين في السجل كما تم التنصيص عليهما في المادتين 7 و8 من ميثاق الحقوق الأساسية للاتحاد الأوروبي يخدم هدفاً للمصلحة العامة وكان ضرورياً ومتناسباً.

لذلك، قضت محكمة العدل التابعة للاتحاد الأوروبي، في قضية «ماني»، بأن الحقين في حماية البيانات والخصوصية لم يطغيا على مصلحة الأطراف الثالثة في الوصول إلى المعلومات الواردة في سجل الشركات فيما يتعلق بشركات المساهمة والشركات ذات المسؤولية المحدودة.

[133] قضية محكمة العدل التابعة للاتحاد الأوروبي رقم 398/15 المتعلقة بغرفة التجارة والصناعة والحرف التقليدية والفلاحة لمدينة ليتشي ضد سالفاتوري ماني والمؤرخة في 09 مارس 2017

[134] نفس المرجع السابق، الفقرة 49.

[135] نفس المرجع السابق، الفقرة 60.

# 2
# مصطلحـــات حمايـــة البيانـــات

| الاتحاد الأوروبي | المسائل المتناولة | مجلس أوروبا |
|---|---|---|
| **البيانات الشخصية** | | |
| اللائحة العامة لحماية البيانات، المادة 4 (1)<br>اللائحة العامة لحماية البيانات، المادتان 4 (5) و5 (1) (ه)<br>اللائحة العامة لحماية البيانات، المادة 9<br>محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C92/09 وC-93/09، فولكر وماركوس شيكه (شركة يحكمها القانون المدني الألماني) وهارتموت أيفرت ضد لاند هيسن [الغرفة الكبرى]، 2010<br>محكمة العدل التابعة للاتحاد الأوروبي، القضية C-275/06، «منتجو الموسيقى إسبانيا (‚بروموسيكاي') ضد ‚تيليفونيكا إسبانيا'» (شركة ذات مساهم واحد) [الغرفة الكبرى]، 2008<br>محكمة العدل التابعة للاتحاد الأوروبي، القضية C-70/10 المتعلقة «‚بسكارليت إكستنديد' (شركة مساهمة) ضد الشركة البلجيكية للمؤلفين والملحنين والموزعين الموسيقيين (شركة تعاونية ذات مسؤولية محدودة) (SABAM)»، 2011<br>محكمة العدل التابعة للاتحاد الأوروبي، القضية C-582/14، «‚باتريك برايز' ضد جمهورية ألمانيا الاتحادية»، 2016<br>محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-372/12 و141/12 C، إ. س. ضد وزارة الهجرة والاندماج واللجوء ووزارة الهجرة والاندماج واللجوء ضد م. و س.، 2014 | التعريف القانوني لحماية البيانات | الاتفاقية 108 المحدثة، المادة 2 (أ)<br>المحكمة الأوروبية لحقوق الإنسان، القضية 24117/08، «‚بيرن لارسن هولدينغ' (شركة محدودة) وآخرون ضد النرويج»، 2013<br>المحكمة الأوروبية لحقوق الإنسان، القضية 35623/05، «‚أوتسون' ضد ألمانيا»، 2010<br>المحكمة الأوروبية لحقوق الإنسان، القضية 27798/95، «‚آمان' ضد سويسرا» [الغرفة الكبرى]، 2000 |

| | | |
|---|---|---|
| محكمة العدل التابعة للاتحاد الأوروبي، القضية C-101/01، دعوى جنائية ضد «بوديل ليندغفيست»، 2003 | الفئات الخاصة من البيانات الشخصية (البيانات الحساسة) | الاتفاقية 108 المحدثة، المادة 6 (1) |
| محكمة العدل التابعة للاتحاد الأوروبي، القضية C-434/16، «بيتر نوفاك' ضد مفوض حماية البيانات»، 2017 | البيانات الشخصية مخفاة المصدر والتي تستعمل اسماً مستعاراً | الاتفاقية 108 المحدثة، المادة 5 (4) (ه)<br>التقرير التفسيري الملحق بالاتفاقية 108 المحدثة، الفقرة 50 |
| **معالجة البيانات** | | |
| اللائحة العامة لحماية البيانات، المادة 4 (2)<br>محكمة العدل التابعة للاتحاد الأوروبي، القضية C-212/13، «'فرانتيسيك راينيس' ضد مكتب حماية البيانات الشخصية»، 2014<br>محكمة العدل التابعة للاتحاد الأوروبي، القضية C-398/15، «غرفة التجارة والصناعة والحرف التقليدية والفلاحة في ليتشي ضد 'سالفاتوري ماني'»، 2017<br>محكمة العدل التابعة للاتحاد الأوروبي، القضية C-101/01، دعوى جنائية ضد «بوديل ليندغفيست»، 2003<br>محكمة العدل التابعة للاتحاد الأوروبي، القضية C-131/12، «'غوغل إسبانيا' (شركة محدودة) التابعة لشركة 'غوغل' ضد الوكالة الإسبانية لحماية البيانات (APED) و'ماريو كوستيخا غونساليس'» [الغرفة الكبرى]، 2014 | تعاريف | الاتفاقية 108 المحدثة، المادة 2 (ب) و(ج) |
| **مستخدمو البيانات** | | |
| اللائحة العامة لحماية البيانات، المادة 4 (7)<br>محكمة العدل التابعة للاتحاد الأوروبي، القضية C-212/13، «'فرانتيسيك راينيسس' ضد مكتب حماية البيانات الشخصية»، 2014<br>محكمة العدل التابعة للاتحاد الأوروبي، القضية C-131/12، «'غوغل إسبانيا' (شركة محدودة) التابعة لشركة 'غوغل' ضد الوكالة الإسبانية لحماية البيانات (APED) و'ماريو كوستيخا غونساليس'» [الغرفة الكبرى]، 2014 | مراقب البيانات | الاتفاقية 108 المحدثة، المادة 2 (ج)<br>التوصية المتعلقة بالتنميط، المادة 1 (ز)* |
| اللائحة العامة لحماية البيانات، المادة 4 (8) | معالج البيانات | الاتفاقية 108 المحدثة، المادة 2 (د)<br>التوصية المتعلقة بالتنميط، المادة 1 (ز)* |
| اللائحة العامة لحماية البيانات، المادة 4 (9) | مستلم البيانات | الاتفاقية 108 المحدثة، المادة 2 (و) |
| اللائحة العامة لحماية البيانات، المادة 4 (10) | الطرف الثالث | |

| الموافقة | | |
|---|---|---|
| اللائحة العامة لحماية البيانات، المادة 4 (11) و 7<br>محكمة العدل التابعة للاتحاد الأوروبي، القضية C-543/09،<br>«'دويتشه تيليكوم' (شركة عامة محدودة) ضد جمهورية ألمانيا الاتحادية»، 2011<br>محكمة العدل التابعة للاتحاد الأوروبي، القضية C-536/15،<br>«'تيلي 2 هولندا› (شركة محدودة) وآخرون ضد هيئة المستهلكين والأسواق (AMC)»، 2017 | تعريف الموافقة الصحيحة وشروطها | الاتفاقية 108 المحدثة، المادة 5 (2)<br>التوصية المتعلقة بالبيانات الطبية، المادة 6، ومختلف التوصيات اللاحقة<br>المحكمة الأوروبية لحقوق الإنسان، القضية 61243/08، «'إلبيرت' ضد لاتفيا»، 2015 |

ملاحظة: * مجلس أوروبا، لجنة الوزراء (2010)، التوصيةCM/Rec(2010)13 الصادرة عن لجنة الوزراء والموجهة إلى الدول الأعضاء بشأن حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية في سياق التنميط (التوصية المتعلقة بالتنميط)، 23 نوفمبر 2010.

## 1.2. البيانات الشخصية

### النقاط الرئيسية

- تُعد البيانات بيانات شخصية إذا كانت تتعلق بشخص محدد الهوية أو يمكن التعرف على هويته، ويُدعى هذا الأخير بـ'صاحب البيانات'.
- لتحديد ما إذا كان الشخص الطبيعي يمكن التعرف على هويته، ينبغي على مراقب البيانات أو شخص آخر على حد سواء مراعاة جميع الوسائل المعقولة التي من المحتمل استخدامها - مثل الانتقاء - للتعرف على هوية الشخص الطبيعي بطريقة مباشرة أو غير مباشرة.
- يُقصد بالتحقق من الهوية إثبات أن شخصاً طبيعياً معيناً يمتلك هوية معينة و/أو مخول له القيام بأنشطة معينة.
- توجد فئات خاصة من البيانات، تُدعى بالبيانات الحساسة، مدرجة في الاتفاقية 108 المحدثة وقانون الاتحاد الأوروبي لحماية البيانات، وهي تتطلب حماية معززة، و لذلك فإنها تخضع لنظام قانوني خاص.
- تُعد البيانات بيانات مخفاة المصدر (anonymised data) إذا كانت لم تعد تتعلق بفرد محدد الهوية أو يمكن التعرف على هويته.
- يُقصد باستعمال اسم مستعار للبيانات (pseudonymisation) إجراءً لا يمكن من خلاله أن تُنسب البيانات الشخصية إلى صاحبها دون معلومات إضافية يُحتفظ بها منفصلة. ويجب أن يظل 'المفتاح' الذي يمكن من إعادة التعرف على هوية أصحاب البيانات منفصلاً وآمناً. وتظل البيانات التي خضعت لعملية إعتماد أسماء مستعارة بيانات شخصية. ولا يوجد مفهوم 'البيانات ذات الأسماء المستعارة « في قانون الاتحاد الأوروبي.
- لا تنطبق مبادئ وقواعد حماية البيانات على المعلومات مخفاة المصدر، إلا أنها تنطبق على البيانات ذات الأسماء المستعارة.

### 1.1.2. الجوانب الأساسية لمفهوم حماية البيانات

**وفق قانون الاتحاد الأوروبي** وكذلك **وفق قانون مجلس أوروبا**، تُعرَّف 'البيانات الشخصية' بالمعلومات المتعلقة بشخص طبيعي محدد الهوية أو يمكن التعرف على هويته.[136] وهي تتعلق بمعلومات عن شخص تكون هويته إما واضحة تماماً أو يمكن إثباتها بمعلومات إضافية. ولتحديد ما إذا كان شخص يمكن التعرف على هويته، يجب على مراقب البيانات أو شخص آخر مراعاة جميع الوسائل التي من المحتمل استخدامها بطريقة مباشرة أو غير مباشرة لتحديد هوية الفرد، مثل التمييز، ما يسمح بمعاملة شخص على نحو مختلف عن شخص آخر.[137]
إذا كانت بيانات ذلك الشخص قيد المعالجة، فإنه يُسمى بـ'صاحب البيانات'.

**صاحب البيانات**

**بموجب قانون الاتحاد الأوروبي**، يُعد الأشخاص الطبيعيون المستفيدين الوحيدين من قواعد حماية البيانات[138] والكائنات الحية الوحيدة التي يحميها القانون الأوروبي لحماية البيانات.[139] وتعرِّف اللائحة العامة لحماية البيانات البيانات الشخصية على أنها أية معلومات تتعلق بشخص طبيعي محدد الهوية أو يمكن التعرف على هويته.

يشير أيضاً **قانون مجلس أوروبا**، ولا سيما الاتفاقية 108 المحدثة، إلى حماية الأفراد فيما يتعلق بمعالجة بياناتهم الشخصية. وتعني البيانات الشخصية، بموجبه أيضاً، أي معلومة تتعلق بفرد محدد الهوية أو يمكن التعرف على هويته. ويُعرف ذلك الشخص أو الفرد في قانون حماية البيانات، كما هو مشار إليه في اللائحة العامة لحماية البيانات والاتفاقية 108 المحدثة على التوالي، بصاحب البيانات. يتمتع الأشخاص الاعتباريون أيضاً بنوع من الحماية. وتوجد سوابق قضائية للمحكمة الأوروبية لحقوق الإنسان تبت في دعاوى أقامها أشخاص قانونيون مدعين حدوث انتهاكات في حقهم في الحماية من استخدام بياناتهم بموجب المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان. وتشمل المادة 8 من

[136] اللائحة العامة لحماية البيانات، المادة 4 (1)؛ الاتفاقية المحدثة 108، المادة 2 (أ).
[137] اللائحة العامة لحماية البيانات، الحيثية 26.
[138] نفس المرجع السابق، المادة 1.
[139] نفس المرجع السابق، الحيثية 27. إطلع أيضاً على فريق عمل المادة 29 (2007)، الرأي رقم 4/2007 بخصوص مفهوم البيانات الشخصية، WP 136، المؤرخ في 20 يونيو 2007، الصفحة 22.

الاتفاقية الأوروبية لحقوق الإنسان كلاً من الحق في احترام الحياة الخاصة والعائلية، والحق في احترام حرمة المسكن والمراسلات. ولذلك يمكن للمحكمة أن تنظر في القضايا بموجب هذا الأخير ، وليس في إطار الحياة الخاصة.

مثال: تتعلق قضية «'بيرن لارسن هولدينغ (شركة محدودة) وآخرون ضد النرويج»[140] بشكوى قدمتها ثلاث شركات نرويجية بخصوص قرار صادر عن سلطة ضريبية يأمر الشركات المذكورة بتزويد مدققي الحسابات الضريبية بنسخة من جميع البيانات المخزنة في خادم حاسوب اشتركت الشركات في استخدامه.

استنتجت المحكمة الأوروبية لحقوق الإنسان أن ذلك الالتزام المفروض على الشركات المدعية شكّل تدخلاً في حقهم في احترام حرمة 'المسكن' و'المراسلات' بموجب المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان. واستنتجت المحكمة، من جهة أخرى، أن السلطات الضريبية قد وفرت ما يكفي من الضمانات الفعالة للوقاية من الاستعمال التعسفي: فقد أُشعرت الشركات المدعية في وقت مبكر وكانت حاضرة خلال مجريات العملية وقادرة على تقديم الملفات أثناء التدخل الميداني، علاوة على أن كافة المواد المتداولة كانت ستُدمَّر فور الانتهاء من المراجعة الضريبية. في تلك الظروف، تم تحقيق توازن عادل بين حق الشركات المدعية في احترام حرمة 'المسكن' و'المراسلات' ومصلحتها في حماية خصوصية الأشخاص العاملين لصالحها من ناحية، وبين المصلحة العامة في ضمان تفتيش فعال لأغراض التقييم الضريبي من ناحية أخرى. وعليه قضت المحكمة بعدم وقوع انتهاك للمادة 8.

**وفقاً للاتفاقية 108 المحدثة**، تتناول حماية البيانات، في المقام الأول، حماية الأشخاص الطبيعيين؛ إلا أن الأطراف المتعاقدة قد توسع نطاق حماية البيانات لتشمل الأشخاص الاعتباريين مثل المؤسسات التجارية والجمعيات في قوانينها الوطنية. ويذكر التقرير التفسيري الملحق بالاتفاقية المحدثة أن القانون الوطني قد يحمي المصالح المشروعة للأشخاص الاعتباريين بتوسيع نطاق الاتفاقية إلى تلك الجهات الفاعلة.[141] لا يشمل **القانون الأوروبي لحماية البيانات** معالجة البيانات التي تتعلق بالأشخاص الاعتباريين، ولا يتعلق على وجه الخصوص بالمقاولات المنشأة بصفة أشخاص اعتباريين، بما في ذلك اسم وشكل الشخص الاعتباري وبيانات الاتصال الخاصة به.[142] غير أن الأمر التوجيهي المتعلق بالخصوصية الإلكترونية يحمي سرية الاتصالات والمصالح المشروعة للأشخاص الاعتباريين فيما يتعلق بتزايد قدرة التخزين والمعالجة الآليين للبيانات التي تهم المشتركين والمستخدمين.[143] وبالمثل ، يوسع مشروع لائحة الخصوصية الإلكترونية الحماية للأشخاص الاعتباريين.

مثال: في قضية «'فولكر وماركوس شيكه' و'هارتموت أيفرت' ضد 'لاند هيسن'»،[144] قضت محكمة العدل التابعة للاتحاد الأوروبي، مشيرة إلى نشر بيانات شخصية متعلقة بمستفيدين من مساعدة فلاحية ، أن «الأشخاص الاعتباريين يمكنهم طلب الحماية التي تنص عليها المادتين 7 و8 من ميثاق الحقوق الأساسية للاتحاد الأوروبي فيما يتعلق بذلك التحديد للهوية فقط إذا كان الاسم الرسمي للشخص الاعتباري يحدد هوية شخص طبيعي واحد أو أكثر. ويتعلق الحق في احترام الحياة الخاصة فيما يخص معالجة البيانات الشخصية، الذي تقره المادتان 7 و8 من ميثاق الحقوق الأساسية للاتحاد الأوروبي، بأي معلومات تخص فرداً محدد الهوية أو يمكن التعرف على هويته» [145]

[136] اللائحة العامة لحماية البيانات، المادة 4 (1)؛ الاتفاقية المحدثة 108، المادة 2 (أ).
[137] اللائحة العامة لحماية البيانات، الحيثية 26.
[138] نفس المرجع السابق، المادة 1.
[139] نفس المرجع السابق، الحيثية 27. اطلع أيضاً على فريق عمل المادة 29 (2007)، الرأي رقم 4/2007 بخصوص مفهوم البيانات الشخصية، WP 136، المؤرخ في 20 يونيو 2007، الصفحة 22.
[140] قضية المحكمة الأوروبية لحقوق الإنسان رقم 24117/08 المتعلقة بيرن لارسن هولدينغ (شركة محدودة) والمؤرخة في 14 مارس 2013. إطلع أيضاً، مع ذلك، على قضية المحكمة الأوروبية لحقوق الإنسان رقم 58243/00 المتعلقة بليبيرتي وآخرين ضد المملكة المتحدة والمؤرخة في 01 يوليو 2008.
[141] التقرير التفسيري الملحق بالاتفاقية المحدثة 108، الفقرة 30.
[142] اللائحة العامة لحماية البيانات، الحيثية 14.
[143] الأمر التوجيهي المتعلق بالخصوصية الإلكترونية، الحيثية 7 والمادة 1 (2).
[144] قضيتا محكمة العدل التابعة للاتحاد الأوروبي المضمومتان رقم C-92/09 ورقم C-93/09 المتعلقتين بفولكر وماركوس شيكه (شركة يحكمها القانون المدني الألماني) وهارتموت أيفرت ضد لاند هيسن [الفرقة الكبرى] والمؤرختين في 09 نوفمبر 2010، الفقرة 53.
[145] نفس المرجع السابق، الفقرتين 52 و53.

بالتوفيق بين مصلحة الاتحاد الأوروبي في ضمان الشفافية بشأن تخصيص المساعدة من ناحية، والحقين الأساسيين في الخصوصية وحماية البيانات الخاصين بالأفراد الذين استفادوا من المساعدة من ناحية أخرى، رأت محكمة العدل التابعة للاتحاد الأوروبي أن التدخل في هذين الحقين الأساسيين كان غير متناسب. ورأت أن الهدف المراد من الشفافية كان من الممكن تحقيقه بتدابير أقل تدخلاً في حقوق الأفراد المعنيين. غير أنه عند التدقيق في تناسب نشر معلومات تخص الأشخاص الاعتباريين الذين تلقوا المساعدة، توصلت محكمة العدل التابعة للاتحاد الأوروبي إلى استنتاج مختلف، وقضت بأن ذلك النشر لم يتعدى حدود مبدأ التناسب. وذكرت أن «خطورة انتهاك الحق في حماية البيانات الشخصية يتجلى في طرق متنوعة فيما يخص الأشخاص الاعتباريين من ناحية، والأشخاص الطبيعيين من ناحية أخرى»،[146] وكان الأشخاص الاعتباريون يخضعون لالتزامات أكبر فيما يتعلق بنشر المعلومات الخاصة بهم. ورأت محكمة العدل التابعة للاتحاد الأوروبي أن مطالبة السلطات الوطنية بالتدقيق فيما إذا كانت بيانات كل شخص اعتباري مستفيد تحدد هوية أي أشخاص طبيعيين مرتبطين بها قبل نشرها، كان سيضع عبئاً إدارياً مبالغاً فيه على تلك السلطات. ولذلك، فقد وفَّقت التشريعات التي تشترط نشراً معمماً للبيانات المتعلقة بالأشخاص الاعتباريين توفيقاً عادلاً بين المصالح المتضاربة للمعنيين.

**طبيعة البيانات**

يمكن لأي نوع من البيانات أن يكون بيانات شخصية شريطة أن ترتبط بشخص محدد الهوية أو يمكن التعرف على هويته.

مثال: يكون تقييم مشرف لأداء موظف لعمله، المخزن في ملف شؤون الموظفين الخاص بذلك الموظف، بمثابة بيانات شخصية عن الموظف. ويصح ذلك رغم أنها قد تعكس، جزئياً أو كلياً، الرأي الشخصي للمشرف فحسب، مثل: «الموظف ليس متفانيا في عمله» - وليس حقائق ثابتة، مثل: «غاب الموظف عن العمل لمدة خمسة أسابيع خلال الأشهر الستة الماضية».

تشمل البيانات الشخصية المعلومات المتعلقة بالحياة الخاصة للشخص، و التي تشتمل أيضاً على الأنشطة المهنية، بالإضافة إلى معلومات عن حياته العامة.

في قضية «آمان»،[147] فسرت المحكمة الأوروبية لحقوق الإنسان مصطلح 'البيانات الشخصية' على أنه لا يقتصر على شؤون الحياة الخاصة للفرد. وينطبق هذا المعنى لمصطلح 'البيانات الشخصية' أيضاً على اللائحة العامة لحماية البيانات.

مثال: في قضية «'فولكر وماركوس شيكه' و'هارتموت أيفرت' ضد 'لاند هيسن'»،[148] ذكرت محكمة العدل التابعة للاتحاد الأوروبي أنه «لا يهم، في هذا الصدد، أن تكون البيانات المنشورة تتعلق بأنشطة ذات طبيعة مهنية. وقضت المحكمة الأوروبية لحقوق الإنسان، في هذا الصدد، بالإشارة إلى تفسير المادة 8 من الاتفاقية [الاتفاقية الأوروبية لحقوق الإنسان]، بأن مصطلح 'الحياة الخاصة' لا يجب تفسيره تفسيراً حصرياً وأنه لا يوجد سبب مبدئي يبرر استثناء الأنشطة ذات الطبيعة المهنية من مفهوم الحياة الخاصة».

مثال: في القضيتين المضمومتين «إ. س. ضد وزارة الهجرة والاندماج واللجوء» و«وزارة الهجرة والاندماج واللجوء ضد م. و س.»،[149] ذكرت محكمة العدل التابعة للاتحاد الأوروبي أن التحليل القانوني الوارد في مشروع قرار لإدارة الهجرة والتجنيس الذي يتناول طلبات الحصول على رخصة الإقامة لا يشكل في حد ذاته بيانات شخصية، رغم أنه قد يتضمن بعضاً من البيانات الشخصية.

تؤكد السوابق القضائية للمحكمة الأوروبية لحقوق الإنسان المتعلقة بالمادة 8 من الاتفاقية الأوروبية لحقوق الإنسان أنه قد يكون من الصعب الفصل التام بين شؤون الحياة المهنية والحياة الخاصة.[150]

[146] نفس المرجع السابق، الفقرة 87.

[147] إطلع على قضية المحكمة الأوروبية لحقوق الإنسان رقم 27798/95 المتعلقة بأمان ضد سويسرا والمؤرخة في 16 فبراير 2000، الفقرة 65.

[148] قضيتا محكمة العدل التابعة للاتحاد الأوروبي المضمومتان رقم C-92/09 ورقم C-93/09 المتعلقتين بفولكر وماركوس شيكه (شركة يحكمها القانون المدني الألماني) وهارتموت أيفرت ضد لاند هيسن [الغرفة الكبرى] والمؤرختين في 09 نوفمبر 2010، الفقرة 59.

[149] قضيتا محكمة العدل التابعة للاتحاد الأوروبي المضمومتان رقم C-141/12 ورقم C-372/12 المتعلقتين بـ إ. س. ضد وزارة الهجرة والاندماج واللجوء وبوزارة الهجرة والاندماج واللجوء ضد م. و س. المؤرختين في 17 يوليو 2014، الفقرة 39.

[150] إطلع، على سبيل المثال، على قضية المحكمة الأوروبية لحقوق الإنسان رقم 28341/95 المتعلقة بروتارو ضد رومانيا [الغرفة الكبرى] والمؤرخة في 04 مايو 2000، الفقرة 43؛ وقضية المحكمة الأوروبية لحقوق الإنسان رقم 13710/88 المتعلقة بنيميتز ضد ألمانيا والمؤرخة في 16 ديسمبر 1992، الفقرة 29.

مثال: في قضية «'باربوليسكو' ضد رومانيا»،[151] تم فصل المدعي لاستخدامه الإنترنت الخاص بصاحب العمل خلال ساعات العمل منتهكاً بذلك اللوائح الداخلية. وكان صاحب العمل قد راقب اتصالاته والسجلات، التي تظهر رسائل ذات طبيعة خاصة محضة، تم تقديمها خلال الدعوى المحلية. عند استنتاج المحكمة الأوروبية لحقوق الإنسان أن المادة 8 تنطبق، لم تحدد ما إذا كانت اللوائح التقييدية الخاصة بصاحب العمل قد تركت للمدعي توقعاً معقولاً للخصوصية، لكنها استنتجت، في جميع الأحوال، أن تعليمات صاحب العمل لا يمكن لها أن تحد تماماً من الحياة الاجتماعية الخاصة في مكان العمل. وفيما يتعلق بالموضوع، وجب منح الدول المتعاقدة هامشاً واسعاً للتقدير فيما يخص تقييم الحاجة إلى إنشاء إطار قانوني يحكم الظروف التي يمكن فيها لصاحب العمل أن ينظم الاتصالات غير المهنية - الإلكترونية أوغيرها على حد سواء - التي يقوم بها موظفوه في مقر العمل. ومع ذلك، توجب على السلطات الوطنية أن تكفل أن اعتماد صاحب العمل تدابير لمراقبة المراسلات وغيرها من الاتصالات، بغض النظر عن نطاق تلك التدابير أو مدتها، صاحبته ضمانات مناسبة وكافية للوقاية من الاستعمال التعسفي للسلطة. وكان مبدأ التناسب والضمانات الإجرائية للوقاية من التعسف ضرورية وحددت المحكمة الأوروبية لحقوق الإنسان عدداً من العوامل ذات الصلة بتلك الظروف. وشملت تلك العوامل، على سبيل المثال، مدى مراقبة صاحب العمل للموظفين ودرجة تدخله في خصوصية الموظف، وعواقب ذلك على الموظف وما إذا كان قد تم توفير الضمانات الكافية. وعلاوة على ذلك، توجب على السلطات الوطنية أن تضمن للموظف الذي تعرضت اتصالاته للمراقبة حصوله على سبل الانتصاف أمام هيئة قضائية من اختصاصها أن تحدد، على الأقل من حيث المضمون، كيف تم الالتزام بتلك المعايير المحددة وما إذا كانت التدابير المطعون فيها قانونية. في هذه القضية، استنتجت المحكمة الأوروبية لحقوق الإنسان أنه تم انتهاك المادة 8 لأن السلطات الوطنية لم توفر حماية كافية لحق المدعي في احترام حياته الخاصة ومراسلاته وفشلت في الموازنة العادلة بين مصالح المعنيين.

بموجب **قانون الاتحاد الأوروبي** وكذلك بموجب **قانون مجلس أوروبا**، تتضمن المعلومات بيانات عن شخص ما إذا:

- كان الفرد محدد الهوية أو يمكن التعرف على هويته بواسطة هذه المعلومات؛ أو
- كان الفرد يمكن تمييزه، على الرغم من كونه غير محدد الهوية، بطريقة تسمح باكتشاف هوية صاحب البيانات بإجراء المزيد من البحث

كلا النوعين من المعلومات محميان بنفس الطريقة بموجب القانون الأوروبي لحماية البيانات. وتتطلب قابلية تحديد الهوية المباشرة وغير المباشرة تقييماً مستمراً، «يراعي التكنولوجيا المتوفرة وقت المعالجة والتطورات التكنولوجية».[152] وذكرت المحكمة الأوروبية لحقوق الإنسان مراراً أن مفهوم 'البيانات الشخصية' بموجب الاتفاقية الأوروبية لحقوق الإنسان هو نفسه كما ورد في الاتفاقية 108، لا سيما فيما يتعلق بشرط الارتباط بأشخاص محددي الهوية أو يمكن التعرف على هويتهم.[153]

تنص اللائحة العامة لحماية على أن الشخص الطبيعي يمكن التعرف على هويته عندما «يكون محدد الهوية، بطريقة مباشرة أو غير مباشرة، خاصة بالرجوع إلى معرف مثل الاسم، أو رقم تحديد الهوية، أو بيانات الموقع الجغرافي، أو معرّف الهوية على الإنترنت، أو عامل واحد أو عدة عوامل تخص الهوية الجسدية أو الفيزيولوجية أو الجينية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية لذلك الشخص».[154] ولذلك يتطلب تحديد الهوية العناصر التي تصف الشخص بما يميزه عن جميع الأشخاص الآخرين وبما يسمح بالتعرف عليه بصفته فرداً. ويُعد اسم الشخص مثالاً رئيسياً عن تلك العناصر الوصفية، إذ يمكن له تحديد هوية الشخص مباشرة. في بعض الحالات، يمكن لصفات مميزة أخرى أن تفي بغرض الاسم، ما يجعل الشخص يمكن التعرف على هويته بطريقة غير مباشرة. إن رقم الهاتف، ورقم الضمان الاجتماعي، ورقم تسجيل السيارة كلها أمثلة عن المعلومات التي يمكن لها أن تجعل فرداً يمكن التعرف على هويته. ويمكن أيضاً استخدام صفات مميزة - مثل الملفات المحوسبة، أو ملفات تعريف الارتباط («كوكيز»)، أو أدوات مراقبة حركة مرور الإنترنت - لتمييز الأفراد بتحديد سلوكهم وعاداتهم. وكما هو موضح في رأي فريق عمل المادة 29، «حتى بدون الاستفسار عن اسم الفرد وعنوانه، يمكن تصنيفه استناداً إلى المعايير السوسيواقتصادية أو النفسية أو الفلسفية أو غيرها ونَسْب قرارات معينة إليه لأن نقطة الاتصال الخاصة بالفرد (الحاسوب) لم تعد تشترط الكشف عن هويته بالمعنى الضيق».[155] يُعد تعريف البيانات الشخصية بموجب كل من مجلس أوروبا والاتحاد الأوروبي واسعاً بما يكفي ليشمل جميع إمكانيات تحديد الهوية (و لذلك، جميع درجات قابلية تحديد الهوية).

[151] قضية المحكمة الأوروبية لحقوق الإنسان رقم 61496/08 المتعلقة بباربوليسكو ضد رومانيا [الغرفة الكبرى] والمؤرخة في 05 سبتمبر 2017، الفقرة 121.

[152] اللائحة العامة لحماية البيانات، الحيثية 26.

[153] إطلع على قضية المحكمة الأوروبية لحقوق الإنسان رقم 27798/95 المتعلقة بأمان ضد سويسرا [الغرفة الكبرى] والمؤرخة في 16 فبراير 2000، الفقرة 65.

[154] اللائحة العامة لحماية البيانات، المادة 4 (1).

[155] فريق عمل المادة 29 المتعلقة بحماية البيانات، الرأي 04/2007 بشأن مفهوم البيانات الشخصية، 136 WP، بتاريخ 20 يونيو 2007، ص. 15.

مثال: في قضية «'بروموسيكاي' ضد 'تيليفونيكا إسبانيا'»،[156] ذكرت محكمة العدل التابعة للاتحاد الأوروبي أنه «لا جدال في أن مسعى «بروموسيكاي» لكشف أسماء وعناوين بعض المستخدمين لـ[منصة معينة لمشاركة الملفات على الإنترنت] ينطوي على إتاحة البيانات الشخصية، أي المعلومات المتعلقة بأشخاص طبيعيين محددي الهوية أو يمكن التعرف على هويتهم، وفقاً للتعريف الوارد في المادة 2 (أ) من الأمر التوجيهي 95/46 [المادة 4 (1) من اللائحة العامة لحماية البيانات حالياً]. ويشكل ذلك الكشف عن معلومات مخزنة من قبل «تيليفونيكا»، حسب دفوع «بروموسيكاي» التي لم تفندها «تيليفونيكا»، معالجة للبيانات الشخصية».[157]

مثال: تتعلق قضية «'سكارليت إكستنديد' (شركة مغفلة) ضد الشركة البلجيكية للمؤلفين والملحنين والموزعين الموسيقيين (شركة تعاونية ذات مسؤولية محدودة) (SABAM)»[158] برفض مقدم خدمات الإنترنت، المسمى «سكارليت»، تثبيت نظام لترشيح الاتصالات الإلكترونية التي تستخدم برمجيات مشاركة الملفات لمنع عمليات مشاركة الملفات التي تنتهك حقوق التأليف والنشر المحمية من قبل الشركة البلجيكية للمؤلفين، وهي شركة إدارة تمثل المؤلفين والملحنين والموزعين الموسيقيين. قضت محكمة العدل التابعة للاتحاد الأوروبي بأن عناوين بروتوكول الإنترنت الخاصة بالمستخدمين «تُعد بيانات شخصية محمية لأنها تسمح بتعريف أولئك المستخدمين تعريفاً دقيقاً».

بما أن الكثير من الأسماء ليست فريدة من نوعها، فإن إثبات هوية الشخص قد يحتاج إلى صفات مميزة إضافية لضمان عدم الخلط بينه وبين شخص آخر. في بعض الأحيان، قد يتوجب الجمع بين الصفات المميزة المباشرة وغير المباشرة لتحديد هوية الفرد الذي ترتبط به المعلومات، فغالباً ما يُستخدم تاريخ الولادة ومكانها. إضافة إلى ذلك، تم اعتماد الأرقام الشخصية في بلدان معينة بغية تحسين التمييز بين المواطنين. وقد تُعد البيانات الضريبية المنقولة،[159] والبيانات المتعلقة بطالب رخصة الإقامة الواردة في وثيقة إدارية،[160] والوثائق المتعلقة بالمعاملات المصرفية والعلاقات الائتمانية[161] بيانات شخصية. ويتزايد استخدام البيانات البيومترية مثل بصمات الأصابع، والصور الفوتوغرافية الرقمية أو مسوح قزحية العين، وبيانات الموقع الجغرافي، والصفات المميزة الإلكترونية لتحديد هوية الأشخاص في عصر التكنولوجيا.

ومع ذلك، فإن انطباق القانون الأوروبي لحماية البيانات ليس بحاجة إلى التحديد الفعلي لهوية صاحب البيانات؛ فكون الشخص المعني يمكن التعرف على هويته يُعد كافياً. ويُعتبر الشخص على أنه يمكن التعرف على هويته إذا توفرت عناصر كافية يمكن من خلالها تحديد هويته بطريقة مباشرة أو غير مباشرة.[162] وفقاً للحيثية 26 من اللائحة العامة لحماية البيانات، فإن المعيار هو ما إذا كان من المحتمل أن تكون الوسائل المعقولة لتحديد الهوية متاحة وتتم إدارتها من قبل المستخدمين المتوقعين لتلك المعلومات؛ ويشمل ذلك المعلومات التي تمتلكها الأطراف الثالثة المستلمة للبيانات (اطلع على الجزء 2.3.2).

مثال: قررت سلطة محلية أن تجمع بيانات عن السيارات المسرعة على الشوارع المحلية. فبدأت تلتقط صوراً فوتوغرافية للسيارات، تسجل تلقائياً الوقت والموقع الجغرافي، حتى تنقل البيانات إلى السلطة المختصة لكي تتمكن من فرض غرامات على أولئك الذين تجاوزوا السرعة القصوى المسموح بها. فيقوم صاحب البيانات بتقديم شكوى، مدعياً أن السلطة المحلية لا تملك أساساً قانونياً بموجب قانون حماية البيانات لجمع تلك البيانات، وتؤكد السلطة المحلية أنها لا تجمع بيانات شخصية، وتقول إن لوحات السيارات تكون مجهولة المصدر، ولا تملك السلطة المحلية السلطة القانونية للوصول إلى سجل المربات العام لاكتشاف هوية مالك السيارة أو سائقها.

لا يتوافق هذا التعليل مع الحيثية 26 من اللائحة العامة لحماية البيانات، نظراً إلى أن جمع البيانات يكون غرضه بوضوح تحديد هوية أولئك الذين يتعدون السرعة القصوى وتغريمهم، فإنه من المتوقع أن يُسعى إلى تحديد هويتهم. على الرغم من أن السلطات المحلية لا تملك وسائل لتحديد الهوية متاحة لها مباشرة، فإنها ستنقل البيانات إلى السلطة المختصة، أي الشرطة، التي تملك حقاً تلك الوسائل. وتشتمل الحيثية 26 صراحة على سيناريو يُتوقع فيه أن يسعى المستلمون الآخرون للبيانات، غير المستخدم المباشر للبيانات، إلى تحديد هوية الفرد. في ضوء الحيثية 26، فإن إجراءات السلطة المحلية تكون بمثابة جمع البيانات عن أشخاص يمكن التعرف على هويتهم، ولذلك، تتطلب أساساً قانونياً بموجب قانون حماية البيانات.

---

[156] قضية محكمة العدل التابعة للاتحاد الأوروبي رقم 275/06 المتعلقة بمنتجي الموسيقى إسبانيا (بروموسيكاي) ضد تيليفونيكا إسبانيا (شركة ذات مساهم واحد) [الغرفة الكبرى] والمؤرخة في 29 يناير 2008، الفقرة 45.

[157] الأمر التوجيهي 95/46 سابقاً، المادة 2 (ب)، اللائحة العامة لحماية البيانات حالياً، المادة 4 (2).

[158] قضية محكمة العدل التابعة للاتحاد الأوروبي رقم C-70/10 المتعلقة بسكارليت إكستنديد (شركة مغفلة) ضد الشركة البلجيكية للمؤلفين والملحنين والموزعين الموسيقيين (شركة تعاونية ذات مسؤولية محدودة) (SABAM) والمؤرخة في 24 نوفمبر 2011، الفقرة 51.

[159] قضية محكمة العدل التابعة للاتحاد الأوروبي رقم 201/14 المتعلقة سمارانداً بارا وآخرين ضد الصندوق الوطني للتأمين الصحي وآخرين والمؤرخة في 01 أكتوبر 2015.

[160] قضيتا محكمة العدل التابعة للاتحاد الأوروبي المتعلقتين بـ «أ. س. ضد وزارة الهجرة والاندماج واللجوء» و«وزارة الهجرة والاندماج واللجوء ضد م. و س.» والمؤرخة في 17 يوليو 2014.

[161] قضية المحكمة الأوروبية لحقوق الإنسان رقم 28005/12 المتعلقة بم. ن. وآخرين ضد سان مارينو والمؤرخة في 07 يوليو 2015.

[162] اللائحة العامة لحماية البيانات، المادة 4 (1).

في سبيل «التثبت مما إذا كان من المرجح، في حدود المعقول، استخدام وسيلة معينة لغرض تحديد هوية الشخص الطبيعي، ينبغي أخذ جميع العوامل الموضوعية ذات الصلة في الاعتبار، مثل التكلفة ومقدار الوقت المطلوبين لتحديد الهوية، مع مراعاة التكنولوجيا المتاحة وقت المعالجة والتطورات التكنولوجية».[163]

مثال: في قضية «'برايز' ضد جمهورية ألمانيا الاتحادية»،[164] نظرت محكمة العدل التابعة للاتحاد الأوروبي في مفهوم قابلية التعرف غير المباشر على هوية أصحاب البيانات. وتطرقت القضية إلى عناوين بروتوكول الإنترنت الديناميةِ، و التي تتغير في كل مرة يتم فيها الاتصال مجدداً بالإنترنت. وقد سجلت المواقع الإلكترونية التي تديرها المؤسسات الألمانية الاتحادية عناوين بروتوكول الإنترنت الديناميةِ وخزنتها للحيلولة دون حدوث هجمات سيبرانية والشروع في الدعاوى الجنائية عند الاقتضاء. ويُعد مقدم خدمات الإنترنت الذي استخدمه السيد برايز الوحيد الذي كان يتوفر على المعلومات الإضافية الضرورية لتحديد هويته.

رأت محكمة العدل التابعة للاتحاد الأوروبي أن عنوان بروتوكول الإنترنت، الذي يسجله مزود خدمات وسائل الإعلام الإلكترونية عندما يصل الشخص إلى موقع إلكتروني يتيحه ذلك المزود لعامة الناس، يشكل بيانات شخصية حيث يكون الطرف الثالث - مقدم خدمات الإنترنت في هذه الحالة - وحده من يمتلك المعلومات الإضافية الضرورية لتحديد هوية الشخص. وقضت بأنه «ليس ضرورياً أن تكون جميع المعلومات التي تسمح بالتعرف على هوية صاحب البيانات في متناول شخص واحد» حتى تشكل بيانات شخصية. وقد يكون مستخدمو عنوان بروتوكول الإنترنت المسجل من قبل مقدم خدمات الإنترنت محددي الهوية في بعض الحالات، على سبيل المثال ضمن إطار الدعاوى الجنائية في حال حدوث هجمات سيبرانية، بمساعدة أشخاص آخرين.[166] ووفقاً لمحكمة العدل التابعة للاتحاد الأوروبي، عندما يكون مقدم الخدمات «يمتلك الوسائل القانونية التي تسمح له بالتعرف على هوية صاحب البيانات بالاعتماد على بيانات إضافية يملكها مقدم خدمات الإنترنت عن ذلك الشخص»، فإن ذلك يشكل «وسيلة من المحتمل أن يتم استخدامها للتعرف على هوية صاحب البيانات». ولذلك، تُعد تلك البيانات بيانات شخصية.

**بموجب قانون مجلس أوروبا**، تُفهم إمكانية التعرف على الهوية بنفس الطريقة. فالتقرير التفسيري للاتفاقية 108 المحدثة يشتمل على وصف مشابه: لا يحيل مفهوم 'شخص يمكن التعرف على هويته' إلى هوية الفرد المدنية أو القانونية فحسب، وإنما أيضاً إلى ما يسمح لشخص واحد بـ'تمييزه' أو عزله عن الآخرين، وبالتالي، احتمال معاملته معاملة مختلفة. ويمكن لذلك 'التمييز' أن يتم، على سبيل المثال، بالإحالة إلى ذلك الشخص على وجه الخصوص، أو إلى جهاز أو مجموعة من الأجهزة (الحاسوب أو الهاتف المحمول أو الكاميرا أو جهاز الألعاب وما إلى ذلك) المرتبطة برقم تحديد الهوية، أو اسم مستعار، أو بيانات بيومترية أو جينية، أو بيانات موقع جغرافي، أو عنوان بروتوكول الإنترنت، أو محدد هوية آخر.[167] ولا يُعد الفرد أنه 'يمكن' التعرف على هويته إذا كان ذلك يتطلب وقتاً أو مجهوداً أو موارد غير معقولة. و هذا هو الحال ، على سبيل المثال، عندما يتطلب تحديد هوية صاحب البيانات عمليات معقدة وطويلة المدة ومكلفة. ويجب تقييم معقولية الوقت أو المجهود أو الموارد على أساس كل قضية على حدة مع مراعاة عوامل مثل الغرض من المعالجة، وفوائد تحديد الهوية وتكلفتها، ونوع مراقب البيانات، والتكنولوجيا المستخدمة.[168]

وفيما يخص الشكل الذي تتخذه البيانات المخزنة أو المستخدمة، فإنه من المهم الإشارة إلى أنه لا يؤثر على انطباق قانون حماية البيانات من عدمه. وقد تحتوي الاتصالات المكتوبة والشفوية بيانات شخصية بالإضافة إلى الصور،[169] بما في ذلك مقطع فيديو[170] أو صوت تم تسجيله بكاميرا المراقبة[171] (CCTV)وقد تُعد أيضاً المعلومات المسجلة إلكترونياً والمعلومات المطبوعة على الأوراق بيانات شخصية. . حتى عينات خلايا من الأنسجة البشرية - التي

[163] نفس المرجع السابق، الحيثية 26.

[164] قضية محكمة العدل التابعة للاتحاد الأوروبي رقم C-582/14 المتعلقة بباتريك برايز ضد جمهورية ألمانيا الاتحادية والمؤرخة في 19 أكتوبر 2016، الفقرة 43.

[165] الأمر التوجيهي السابق، EC/95/46 الصادر عن البرلمان الأوروبي والمجلس والموقع في 24 أكتوبر 1995 بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وبشأن حرية حركة تلك البيانات، المادة 2 (أ).

[166] قضية محكمة العدل التابعة للاتحاد الأوروبي رقم C-70/10 المتعلقة بسكارليت إكستندد (شركة مغفلة) ضد الشركة البلجيكية للمؤلفين والملحنين والموزعين الموسيقيين (شركة تعاونية ذات مسؤولية محدودة) (SABAM) والمؤرخة في 24 نوفمبر 2011، الفقرتين 47 و48.

[167] التقرير التفسيري الملحق بالاتفاقية المحدثة 108، الفقرة 18.

[168] نفس المرجع السابق، الفقرة 17.

[169] قضية المحكمة الأوروبية لحقوق الإنسان رقم 59320/00 المتعلقة بفون هانوفر ضد ألمانيا المؤرخة في 24 يونيو 2004؛ قضية المحكمة الأوروبية لحقوق الإنسان رقم 50774/99 المتعلقة بشياكا ضد إيطاليا المؤرخة في 11 يناير 2005؛ قضية محكمة العدل التابعة للاتحاد الأوروبي رقم C-212/13 المتعلقة بفرانتيسيك رابينيس ضد مكتب حماية البيانات الشخصية المؤرخة في 11 ديسمبر 2014.

[170] قضية المحكمة الأوروبية لحقوق الإنسان رقم 44647/98 المتعلقة ببيك ضد المملكة المتحدة المؤرخة في 28 يناير 2003؛ قضية المحكمة الأوروبية لحقوق الإنسان رقم 420/07 المتعلقة بكوبكه ضد ألمانيا (قرار) المؤرخة في 05 أكتوبر 2010؛ المشرف الأوروبي على حماية البيانات (2010)، الأوامر التوجيهية المتعلقة بالمراقبة بالفيديو الصادرة عن المشرف الأوروبي على حماية البيانات والمؤرخة في 17 مارس 2010.

[171] قضية المحكمة الأوروبية لحقوق الإنسان رقم 44787/98 المتعلقة بـ ب.ج. وج.ه. ضد المملكة المتحدة والمؤرخة في 25 سبتمبر 2001، الفقرتين 59 و60؛ قضية المحكمة الأوروبية لحقوق الإنسان رقم 71611/01 المتعلقة بويس ضد فرنسا والمؤرخة في 20 ديسمبر 2005 (النسخة المكتوبة باللغة الفرنسية).

تحتوي على الحمض النووي للشخص - قد تكون مصادر يمكن استخلاص البيانات البيومترية منها،[172] ما دامت البيانات تتعلق بالخصائص الجينية المتوارثة أو المكتسبة، وتتيح معلومات فريدة عن صحة الشخص أو فيزيولوجيته، وتنشأ عن تحليل العينة البيولوجية المأخوذة من ذلك الشخص.[173]

**إخفاء مصدر البيانات**

وفقاً لمبدأ حصر مدة التخزين الوارد في كل من اللائحة العامة لحماية البيانات والاتفاقية 108 المحدثة (الذي نوقش بالتفصيل في الفصل 3)، يجب الاحتفاظ بالبيانات «في شكل يسمح بتحديد هوية صاحب البيانات لمدة لا تزيد عما هو ضروري للأغراض التي تُعالج من أجلها البيانات»،[174] وبالتالي يتعين محو البيانات أو إخفاء مصدرها إذا رغب مراقب البيانات في تخزينها بعد أن تنتفي الحاجة إليها ولم تعد تخدم الغرض الأولي منها.

يُقصد بعملية إخفاء مصدر البيانات حذف جميع العناصر المحددة للهوية من مجموعة من البيانات الشخصية بحيث لا يمكن التعرف على هويت صاحب البيانات بعد ذلك،[175] يحلل فريق عمل المادة 29، في رأيه الصادر في 05/2014، فعالية وأوجه قصور مختلف تقنيات إخفاء مصدر البيانات،[176] ويقر بالقيمة الممكنة لتلك التقنيات لكنه يبرز أن تقنيات بعينها لا تفي بغرضها في جميع الأحوال. ولإيجاد الحل الأفضل في حالة معينة، ينبغي البت في عملية إخفاء مصدر البيانات المناسبة على أساس كل قضية على حدة. وبغض النظر عن التقنية المستخدمة، يجب منع تحديد الهوية بطريقة لا رجعة فيها. وذلك يعني أنه لكي يتم إخفاء مصدر البيانات، لا يجب ترك أي عنصر في المعلومات التي من شأنها، من خلال بذل مجهود معقول، أن تخدم إعادة تحديد هوية الشخص المعني (أو الأشخاص المعنيين).[177] يمكن تقييم خطر إعادة تحديد الهوية بمراعاة «الوقت، و المجهود، و الموارد الضرورية في ضوء طبيعة البيانات، وسياق استخدامها، والتكنولوجيات المتاحة لإعادة تحديد الهوية والتكاليف المرتبطة بها»،[178]

حينما يتم إخفاء مصدر البيانات بنجاح، فإن البيانات تنتفي عنها صفة البيانات الشخصية بعد ذلك ولا تكون التشريعات الخاصة بحماية البيانات سارية المفعول بعد ذلك.

تنص اللائحة العامة لحماية البيانات على أنه لا يمكن إجبار الشخص أو المنظمة التي تتحكم في معالجة البيانات الشخصية على الاحتفاظ بمعلومات إضافية، أو الحصول عليها، أو معالجتها لتحديد هوية صاحب البيانات فقط لغرض للامتثال للائحة. إلا أن هذه القاعدة تتضمن استثناءً هاماً: عندما يتيح صاحب البيانات، لأغراض ممارسة الحقوق في الوصول إلى البيانات، وتصحيحها، ومحوها، وتقييد معالجتها، و نقلها، معلومات إضافية لمراقب البيانات تمكنه من تحديد هويته، حينها تصبح تلك البيانات، التي كانت فيما قبل مخفاة المصدر، بيانات شخصية مرة أخرى.[179]

**استعمال اسم مستعار للبيانات**

تحتوي المعلومات الشخصية على صفات مميِّزة، مثل الاسم أو تاريخ الولادة أو الجنس أو العنوان أو معلومات أخرى قد تفضي إلى التعرف عن هوية صاحبها. وتعني عملية استعمال اسم مستعار للبيانات الشخصية استبدال هذه الصفات المميِّزة باسم مستعار.

يعرف **قانون الاتحاد الأوروبي** استعمال اسم مستعار' بـ «معالجة البيانات الشخصية بشكل لا يسمح بنسبها إلى صاحب بيانات معين دون استخدام معلومات إضافية، شريطة أن يُحتفظ بتلك المعلومات الإضافية بطريقة منفصلة وأن تخضع لتدابير تقنية وتنظيمية لضمان عدم نسبة البيانات الشخصية إلى شخص طبيعي محدد الهوية أو يمكن التعرف على هويته»،[180] وخلافاً للبيانات مخفاة المصدر، تظل البيانات التي تستعمل اسماً مستعاراً بيانات شخصية، ولذلك، تخضع للتشريعات المتعلقة بحماية البيانات. على الرغم من أن استعمال اسم مستعار للبيانات قد يقلل من المخاطر الأمنية على أصحاب البيانات، فإن هذه البيانات لا تُستثنى من نطاق اللائحة العامة لحماية البيانات. تقر اللائحة العامة لحماية البيانات بالاستخدامات المتنوعة للبيانات

---

[172] إطلع على فريق عمل المادة 29 (2007)، الرأي 4/2007 المتعلق بمفهوم البيانات الشخصية، WP 136، المؤرخ في 20 يونيو 2007، ص. 9؛ مجلس أوروبا، التوصية رقم 4(2006) الصادرة عن لجنة الوزراء والموجهة إلى الدول الأعضاء بخصوص الأبحاث في المواد البيولوجية ذات الأصل الإنساني والمؤرخة في 15 مارس 2006.

[173] اللائحة العامة لحماية البيانات، المادة 4 (13).

[174] نفس المرجع السابق، المادة 5 (1) (e)؛ الاتفاقية المحدثة 108، المادة 5 (4) (e).

[175] اللائحة العامة لحماية البيانات، الحيثية 26.

[176] فريق عمل المادة 29 (2014)، القرار رقم 05/2014 المتعلق بتقنيات إخفاء مصدر البيانات، WP 216، المؤرخ في 10 أبريل 2014.

[177] اللائحة العامة لحماية البيانات، الحيثية 26.

[178] مجلس أوروبا، لجنة الاتفاقية 108 (2017)، الأوامر التوجيهية المتعلقة بحماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية في عالم البيانات الضخمة والمؤرخة في 23 يناير 2017، الفقرة 2.6.

[179] اللائحة العامة لحماية البيانات، المادة 11.

[180] نفس المرجع السابق، المادة 4 (5).

التي تستعمل اسماً مستعاراً بوصفها تدبيراً تقنياً مناسباً لتحسين حماية البيانات، ويُشار إلى هذا التدبير على وجه الخصوص لفرض تصميم وأمن عملية معالجة البيانات.[181] كما يُعد أيضاً ضمانة مناسبة قد تُستخدم لمعالجة البيانات الشخصية لأغراض غير تلك التي جُمعت البيانات من أجلها في الأصل.[18]
2

لم يُشِر صراحة إلى استعمال اسم مستعار للبيانات في التعريف القانوني الذي وضعته الاتفاقية 108 المحدثة **لمجلس أوروبا**. غير أن التقرير التفسيري الملحق بالاتفاقية 108 المحدثة يذكر بوضوح أن «استعمال اسم مستعار أو أي معرِّف هوية رقمي/هوية رقمية لا يفضي إلى إخفاء مصدرها لأن صاحب البيانات يظل يمكن التعرف على هويته أو تمييزه».[183] ويُعد تشفير البيانات من بين طرق استعمال اسم مستعار البيانات. وبمجرد استعمال اسم مستعار للبيانات، تصبح الصلة بالهوية في شكل اسم مستعار بالإضافة إلى مفتاح فك التشفير. وبدون ذلك المفتاح، يُعد من الصعب التعرف على هوية صاحب البيانات التي تستعمل اسماً مستعاراً. إلا أن إعادة تحديد الهوية يبقى سهلاً بالنسبة للأفراد الذين يحق لهم استخدام مفتاح فك التشفير. ويجب توخي الاحتياط خصوصاً من استخدام مفاتيح التشفير من قبل الأشخاص غير المرخصين. ولذلك، فإن «البيانات التي تستعمل اسماً مستعاراً يجب احتسابها بيانات شخصية» تشملها الاتفاقية 108 المحدثة.[184]

**التحقق من الهوية**

إن التحقق من الهوية إجراء يمكن الشخص من أن يثبت أنه يمتلك هوية معينة و/أو أنه مرخص له القيام بأشياء معينة، مثل الدخول إلى منطقة أمنية أو سحب النقود من الحساب البنكي. ويمكن القيام بالتحقق من الهوية من خلال مقارنة البيانات البيومترية، مثل الصورة وبصمات الأصابع الموجودة في جواز السفر، بيانات الشخص الذي يقدم نفسه، على سبيل المثال، في نقطة مراقبة الهجرة؛[185] أو بالاستفسار عن المعلومات التي ينبغي لها أن تكون معروفة فقط من قبل شخص ذي هوية أو ترخيص معين، مثل رقم تحديد الهوية الشخصية (PIN) أو كلمة المرور؛ أو بطلب تقديم رمز مميِّز ينبغي له أن يكون حصراً بحوزة شخص ذي هوية أو ترخيص معين، مثل بطاقة شريحة خاصة أو مفتاح خزينة البنك. باستثناء كلمات المرور وبطائق الشريحة، تُعد التوقيعات الإلكترونية - إلى جانب أرقام تحديد الهوية الشخصية أحياناً - أداة قادرة على نحو خاص على تحديد هوية الشخص والتحقق من هويته في الاتصالات الإلكترونية.

## 2.1.2. فئات خاصة من البيانات الشخصية

**بموجب قانون الاتحاد الأوروبي وقانون مجلس أوروبا**، هناك فئات خاصة من البيانات الشخصية التي بطبيعتها قد تشكل خطراً على أصحاب البيانات عند معالجتها وتتطلب حماية معززة. هذه البيانات تخضع لمبدأ الحظر، كما أن هناك عدد محدود من الشروط التي تكون وفقها هذه المعالجة قانونية.

وفي إطار الاتفاقية 108 المحدثة (المادة 6) واللائحة العامة لحماية البيانات (المادة 9)، تعتبر الفئات التالية بيانات حساسة:

- البيانات الشخصية التي تكشف عن الأصل العرقي أو الإثني؛
- البيانات الشخصية التي تكشف عن آراء سياسية أو دينية أو معتقدات أخرى، بما في ذلك المعتقدات الفلسفية؛
- البيانات الشخصية التي تكشف عن العضوية النقابية؛
- البيانات الجينية والبيانات البيومترية المعالجة لغرض تحديد هوية الشخص؛
- البيانات الشخصية المتعلقة بالصحة أو الحياة الجنسية أو التوجه الجنسي.

مثال: تتناول قضية «بوديل ليندغفيست»[186] مسألة الإشارة إلى مجموعة من الأشخاص بالاسم أو بطرق أخرى، مثل أرقام هواتفهم أو معلومات عن هواياتهم، على إحدى صفحات الإنترنت. وقد اعتبرت محكمة العدل التابعة للاتحاد الأوروبي أن «الإشارة إلى إصابة شخص في قدمه وأنه يعمل بدوام جزئي لأسباب طبية هي بمثابة بيانات شخصية تتعلق بالصحة».[187]

[181] نفس المرجع السابق، المادة 25 (1).
[182] نفس المرجع السابق، المادة 6 (4).
[183] التقرير التفسيري الملحق بالاتفاقية 108، الفقرة 18.
[184] نفس المرجع السابق.
[185] نفس المرجع السابق، الفقرتان 57-56.
[186] محكمة العدل التابعة للاتحاد الأوروبي، رقم C-101/01، «الدعوى الجنائية ضد بوديل ليندغفيست»، 6 نوفمبر 2003، الفقرة 51.
[187] الأمر التوجيهي السابق رقم EC/95/46، المادة 8 (1)، اللائحة العامة لحماية البيانات حالياً، المادة 9 (1).

**البيانات الشخصية المرتبطة بالجرائم والإدانات الجنائية**

تدرج الاتفاقية 108 المحدثة البيانات الشخصية المتعلقة بالجرائم والإجراءات والإدانات الجنائية والتدابير الأمنية ذات الصلة ضمن قائمة الفئات الخاصة للبيانات الشخصية.[188] أما في إطار اللائحة العامة لحماية البيانات، فلا يتم ذكر البيانات الشخصية المتعلقة بالجرائم والإدانات الجنائية أو التدابير الأمنية ذات الصلة ضمن قائمة الفئات الخاصة للبيانات، وإنما يتم التطرق إليها في مادة منفصلة. وتنص المادة 10 من اللائحة العامة لحماية البيانات على أنه لا تجوز معالجة هذه البيانات إلا «تحت إشراف هيئة رسمية أو عندما يُصرح بالمعالجة من قبل قانون الاتحاد أو الدول الأعضاء الذي ينص على ضمانات مناسبة تهم حقوق وحريات أصحاب البيانات». من ناحية أخرى، لا يمكن الاحتفاظ بسجلات شاملة تتضمن معلومات عن الإدانات الجنائية إلا تحت إشراف هيئات رسمية محددة.[189] هذا وتخضع معالجة البيانات الشخصية في سياق إنفاذ القانون داخل الاتحاد الأوروبي لصك قانوني محدد، وهو الأمر التوجيهي رقم EU/2016/680.[190] وينص هذا الأخير على قواعد محددة لحماية البيانات، وهي ملزمة للهيئات المختصة عند معالجة البيانات الشخصية تحديداً من أجل منع الجرائم الجنائية والتحقيق فيها والكشف عنها ومتابعة مرتكبيها (انظر الجزء 1.2.8).

## 2.2. معالجة البيانات

### النقاط الرئيسية

- يقصد بـ «معالجة البيانات» أي عملية تخضع لها البيانات الشخصية.
- يشمل مصطلح «المعالجة» المعالجة الآلية وغير الآلية.
- وفقاً لقانون الاتحاد الأوروبي، تشير «المعالجة» أيضاً إلى المعالجة اليدوية داخل أنظمة مُهيكلة لحفظ الملفات.
- وفقاً لقانون مجلس أوروبا، يمكن توسيع معنى «المعالجة» بموجب القانون المحلي ليشمل المعالجة اليدوية.

### 1.2.2. مفهوم معالجة البيانات

إن مفهوم معالجة البيانات الشخصية شامل **بموجب قانون الاتحاد الأوروبي ومجلس أوروبا**: «تعني 'معالجة البيانات الشخصية' [...] أي عملية [...] مثل جمع البيانات الشخصية وتسجيلها وتنظيمها وهيكلتها وتخزينها وتكييفها أو تعديلها واستخلاصها والاطلاع عليها واستخدامها وإفشائها عن طريق الإرسال أو نشرها أو إتاحتها بطريقة أخرى، أومواءمتها أو دمجها، أوتقييدها أو محوها أو إتلافها».[191] هذا وتضيف الاتفاقية 108 المحدثة حفظ البيانات الشخصية إلى التعريف.[192]

مثال: في قضية «فرانتيشيك رينيش»،[193] التقط السيد رينيش صورة لشخصين حطما النوافذ في منزله من خلال نظام كاميرات مراقبة منزلي كان قد ثبته لحماية ممتلكاته. وقد قررت محكمة العدل التابعة للاتحاد الأوروبي أن المراقبة بالفيديو التي تتضمن تسجيل وتخزين البيانات الشخصية هي بمثابة معالجة آلية للبيانات تقع ضمن نطاق قانون حماية البيانات في الاتحاد الأوروبي.

مثال: في قضية «غرفة التجارة والصناعة والحرف اليدوية والزراعة في ليتشي ضد سالفاتوري ماني»،[194] طلب السيد ماني إزالة بياناته الشخصية من سجل شركة تصنيف كان يربطه بتصفية شركة عقارية، وهو ما كان له تأثير سلبي على سمعته. وقد رأت محكمة العدل التابعة للاتحاد الأوروبي أنه «من خلال تدوين هذه المعلومات والاحتفاظ بها في السجل ونشرها، عند الاقتضاء، بناءً على طلب أطراف ثالثة، فإن الهيئة المسؤولة عن المحافظة على هذا السجل تقوم بتنفيذ 'معالجة البيانات الشخصية' باعتبارها 'المراقب'».

[188] الاتفاقية 108 المحدثة، المادة 6 (1).

[189] اللائحة العامة لحماية البيانات، المادة 10.

[190] الأمر التوجيهي (الاتحاد الأوروبي) رقم 2016/680 الصادر عن البرلمان الأوروبي والمجلس في 27 أبريل 2016 بشأن حماية الأشخاص الذاتيين فيما يتعلق بمعالجة البيانات الشخصية من قبل الهيئات المختصة لأغراض منع الجرائم الجنائية أو التحقيق فيها أو الكشف عنها أو متابعة مرتكبيها أو تنفيذ العقوبات الجنائية، وبشأن حرية حركة هذه البيانات، والذي يلغي القرار الإطار الصادر عن المجلس رقم JHA/2008/977، الجريدة الرسمية L 119 OJ، 2016.

[191] اللائحة العامة لحماية البيانات، المادة 4 (2). انظر أيضاً الاتفاقية 108 المحدثة، المادة 2 (ب).

[192] الاتفاقية 108 المحدثة، المادة 2 (ب).

[193] محكمة العدل التابعة للاتحاد الأوروبي، رقم C-212/13، قضية «فرانتيشيك رينيش ضد مكتب حماية البيانات الشخصية»، 11 ديسمبر 2014، الفقرة 25.

[194] محكمة العدل التابعة للاتحاد الأوروبي، رقم C-398/15، قضية «غرفة التجارة والصناعة والحرف اليدوية والزراعة في ليتشي ضد سالفاتوري ماني»، 9 مارس 2017، الفقرة 35.

مثال: يقوم أصحاب العمل بجمع ومعالجة البيانات الخاصة بموظفيهم، بما في ذلك المعلومات المتعلقة برواتبهم. وتقدم عقود العمل الأساس القانوني للقيام بذلك بشكل شرعي.
وسيتعين على أصحاب العمل إرسال البيانات المتعلقة برواتب موظفيهم إلى السلطات الضريبية. وسيكون نقل البيانات هذا أيضاً بمثابة «معالجة» بالمعنى المنصوص عليه في الاتفاقية 108 المحدثة وفي اللائحة العامة لحماية البيانات، غير أن عقود العمل ليست هي الأساس القانوني لهذا الإفصاح، إذ يجب أن يكون هناك أساس قانوني إضافي لعمليات المعالجة التي تنطوي إلى إرسال صاحب العمل البيانات المتعلقة بالرواتب إلى السلطات الضريبية. ويوجد هذا الأساس القانوني عادة في مقتضيات قوانين الضرائب الوطنية. وبدون هذه المقتضيات - وفي غياب أي أساس شرعي آخر للمعالجة - سيكون نقل البيانات الشخصية هذا بمثابة معالجة غير مشروعة.

## 2.2.2. المعالجة الآلية للبيانات

تنطبق حماية البيانات بموجب الاتفاقية 108 المحدثة واللائحة العامة لحماية البيانات بشكل كامل على المعالجة الآلية للبيانات.
وبموجب **قانون الاتحاد الأوروبي**، تشمل المعالجة الآلية للبيانات العمليات التي تخضع لها «البيانات الشخصية كلياً أو جزئياً بوسائل آلية».[195] وتتضمن الاتفاقية 108 المحدثة تعريفاً مشابهاً.[196] أما من الناحية العملية، فهذا يعني أن أي معالجة للبيانات الشخصية من خلال وسائل آلية بمساعدة جهاز كمبيوتر شخصي أو جهاز محمول أو موجه (راوتر)، على سبيل المثال، تخضع لقواعد حماية البيانات في الاتحاد الأوروبي ومجلس أوروبا.

مثال: تتناول قضية «بوديل ليندغفيست»[197] مسألة الإشارة إلى مجموعة من الأشخاص بالاسم أو بطرق أخرى، مثل أرقام هواتفهم أو معلومات عن هواياتهم، على إحدى صفحات الإنترنت. وقد ارتأت محكمة العدل التابعة للاتحاد الأوروبي أن «فعل الإشارة، على صفحة الإنترنت، إلى مجموعة من الأشخاص وتحديدهم بأسمائهم أو بطرق أخرى، كالكشف عن أرقام هواتفهم أو معلومات تتعلق بظروف عملهم أو هواياتهم، هو بمثابة 'معالجة كلية أو جزئية للبيانات بوسائل آلية'« بالمعنى المقصود في المادة 3 (1) من الأمر التوجيهي رقم 95/46.[198]
مثال: في قضية «غوغل إسبانيا» وشركة «غوغل» ضد الوكالة الإسبانية لحماية البيانات وماريو كوستيخا غونزاليس،[199] طلب السيد غونزاليس إزالة أو تغيير رابط بين اسمه في محرك «غوغل» للبحث وصفحتين في جريدة تعلنان عن مزاد عقاري لاسترداد ديون الضمان الاجتماعي. وقد صرحت محكمة العدل التابعة للاتحاد الأوروبي بأنه «من خلال استكشاف الإنترنت آلياً وبشكل مستمر ومنهجي بحثاً عن المعلومات التي يتم نشرها هناك، يقوم مشغل محرك البحث بـ'جمع' البيانات ومن ثم 'استخلاصها' و'تسجيلها' و'تنظيمها' في وقت لاحق ضمن إطار برامج الفهرسة الخاصة به، و'تخزينها' على خوادمه، وعند الاقتضاء، 'الكشف عنها' و 'إتاحتها' لمستخدميه على شكل قوائم لنتائج البحث».[200]
وخلصت المحكمة إلى أن مثل هذه الإجراءات هي بمثابة «معالجة»، وذلك «بغض النظر عن كون مشغل محرك البحث يقوم أيضاً بتنفيذ نفس العمليات فيما يتعلق بأنواع أخرى من المعلومات ولا يميز بين هذه الأخيرة والبيانات الشخصية».

## 3.2.2. المعالجة غير الآلية للبيانات

تتطلب المعالجة اليدوية للبيانات بدورها حماية هذه البيانات.
لا تقتصر حماية البيانات **بموجب قانون الاتحاد الأوروبي** بأي حال من الأحوال على المعالجة الآلية للبيانات. وفقاً لذلك، وبموجب قانون الاتحاد الأوروبي، تنطبق حماية البيانات على معالجة البيانات الشخصية في نظام ملفات يدوي، أي ملف ورقي مهيكل بشكل خاص.[201] ويقصد بنظام الملفات المهيكل النظام الذي يصنف مجموعة من البيانات الشخصية، مما يجعل الوصول إليها متاحاً وفقاً لمعايير معينة. وعلى

[195] اللائحة العامة لحماية البيانات، المادة 2 (1) و4 (2).
[196] الاتفاقية 108 المحدثة، المادة 2 (ب) و(ج)؛ التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 21.
[197] محكمة العدل التابعة للاتحاد الأوروبي، رقم C-101/01، «الدعوى الجنائية ضد بوديل ليندغفيست»، 6 نوفمبر 2003، الفقرة 27.
[198] اللائحة العامة لحماية البيانات، المادة 2 (1).
[199] محكمة العدل التابعة للاتحاد الأوروبي، رقم C-131/12، قضية «غوغل إسبانيا وشركة غوغل ضد الوكالة الإسبانية لحماية البيانات وماريو كوستيخا غونزاليس» [الغرفة الكبرى]، 13 مايو 2014.
[200] نفس المرجع السابق، الفقرة 28.
[201] اللائحة العامة لحماية البيانات، المادة 2 (1).

سبيل المثال، إذا احتفظ صاحب العمل بملف ورقي بعنوان «إجازات الموظفين» يتضمن جميع تفاصيل الإجازات التي حصل عليها الموظفون في السنة المنصرمة وتم فرزها حسب الترتيب الأبجدي، فسيكون الملف بمثابة نظام ملفات يدوي يخضع لقواعد حماية البيانات في الاتحاد الأوروبي. ويرجع تمديد نطاق حماية البيانات هذا إلى ما يلي:

1. يمكن هيكلة الملفات الورقية بطريقة تجعل العثور على المعلومات مسألة يسيرة ولا تستغرق وقتاً؛
2. تخزين البيانات الشخصية في ملفات ورقية مُهيكَلة يُسهِّل التملص من القيود التي ينص عليها القانون الخاص بالمعالجة الآلية للبيانات.[202]

و**بموجب قانون مجلس أوروبا**، يقر تعريف المعالجة الآلية بأن بعض مراحل الاستخدام اليدوي للبيانات الشخصية قد تكون مطلوبة بين العمليات الآلية.[203] وتنص المادة 2 (ج) من الاتفاقية 108 المحدثة على أنه «في حال عدم استخدام المعالجة الآلية، تعني معالجة البيانات أي عملية أو مجموعة عمليات تخضع لها البيانات الشخصية ضمن مجموعة مُهيكَلة من هذه البيانات يمكن الوصول إليها أو استخلاصها وفقًا لمعايير محددة».

## 3.2. مستخدمو البيانات الشخصية

### النقاط الرئيسية

- أي شخص يحدد وسائل وأغراض معالجة البيانات الشخصية للآخرين هو «مراقب البيانات» بموجب قانون حماية البيانات؛ وإذا اتخذ العديد من الأشخاص هذا القرار معاً، فقد يكونون بمثابة «مراقبين مشتركين».
- «المعالج» هو شخص ذاتي أو اعتباري يعالج البيانات الشخصية نيابة عن المراقب.
- يصبح المعالج مراقباً إذا قام بتحديد وسائل وأغراض معالجة البيانات بنفسه.
- أي شخص يتم الكشف له عن البيانات الشخصية هو بمثابة «متلقٍ».
- «الطرف الثالث» هو شخص ذاتي أو اعتباري بخلاف صاحب البيانات والمراقب والمعالج والأشخاص المصرح لهم بمعالجة البيانات الشخصية تحت الإشراف المباشر للمراقب أو المعالج.
- إن الموافقة كأساس قانوني لمعالجة البيانات الشخصية يجب أن تُمنح بحرية، وعن علم، وبشكل محدد، وأن تكون بمثابة إشارة واضحة لا لبس فيها إلى الرغبات من خلال إجراء تأكيدي واضح يدل على الموافقة على المعالجة.
- إن معالجة الفئات الخاصة من البيانات على أساس الموافقة تتطلب موافقة صريحة.

### 1.3.2. المراقبون والمعالجون

إن أهم ما يترتب عن الاضطلاع بدور المراقب أو المعالج هو المسؤولية القانونية المرتبطة بالامتثال للالتزامات ذات الصلة بموجب قانون حماية البيانات. في القطاع الخاص، يتقلد هذه المسؤولية عادةً شخص ذاتي أو اعتباري؛ أما في القطاع العام، عادة ما تقع هذه المسؤولية على عاتق إحدى الهيئات. وهناك فرق كبير بين مراقب البيانات ومعالجها: فالأول هو الشخص الذاتي أو الاعتباري الذي يحدد أغراض ووسائل المعالجة، أما الثاني فهو الشخص الذاتي أو الاعتباري الذي يعالج البيانات نيابة عن المراقب، وذلك وفقاً لتعليمات صارمة من قبل هذا الأخير. ومن حيث المبدأ، فإن مراقب البيانات هو من يجب أن يراقب المعالجة وهو من يتحمل مسؤولية ذلك، بما في ذلك المسؤولية القانونية. بيد أنه في ظل إصلاح قواعد حماية البيانات، أصبح المعالجون الآن ملزمون بالامتثال للعديد من المتطلبات التي تنطبق على المراقبين. فعلى سبيل المثال، بموجب اللائحة العامة لحماية البيانات، يجب على المعالجين الاحتفاظ بسجل لجميع فئات أنشطة المعالجة لإثبات امتثالهم للالتزاماتهم بموجب اللائحة.[204] هذا ويُشترط من المعالجين أيضاً تنفيذ التدابير التقنية والتنظيمية المناسبة لضمان أمن المعالجة،[205] وتعيين مسؤول عن حماية البيانات في حالات معينة،[206] وإخطار المراقب بأي خروقات تتعرض لها البيانات.[207]

[202] اللائحة العامة لحماية البيانات، الحيثية 15.
[203] الاتفاقية 108 المحدثة، المادة 2 (ب) و(ج).
[204] اللائحة العامة لحماية البيانات، المادة 30 (2).
[205] نفس المرجع السابق، المادة 32.
[206] نفس المرجع السابق، المادة 37.
[207] نفس المرجع السابق، المادة 33 (2).

وتبقى قدرة الشخص على تقرير وتحديد غرض ووسائل المعالجة رهينةً بالعناصر الوقائعية والظروف الخاصة بكل حالة على حدة. ووفقاً لتعريف مراقب البيانات الوارد في اللائحة العامة لحماية البيانات، يمكن أن يكون الشخص الذاتي أو الشخص الاعتباري أو أي هيئة أخرى مراقباً للبيانات. في المقابل، شدد فريق عمل المادة 29 على أنه لتزويد الأفراد بكيان أكثر استقراراً يُمكّنهم من ممارسة حقوقهم، «ينبغي من باب الأفضلية اعتبار الشركة أو الهيئة مراقباً، بدلاً من شخص معين داخل الشركة أو الهيئة».[208] وعلى سبيل المثال، فإن الشركة التي تبيع لوازم الرعاية الصحية للمهنيين هي المراقب فيما يتعلق بتجميع وحفظ قائمة التوزيع لجميع المهنيين في منطقة معينة، وليس مدير المبيعات الذي يستخدم القائمة ويحتفظ بها فعلياً.

مثال: عندما يخطط قسم التسويق في شركة «صانشاين» لمعالجة البيانات من أجل استقراء السوق، ستكون الشركة، وليس موظفي قسم التسويق، هي مراقب هذه المعالجة. ولا يمكن أن يكون قسم التسويق هو المراقب، لأن ليس له هوية منفصلة.

ويمكن للأشخاص الذاتيين أن يكونوا مراقبين للبيانات بموجب قانون الاتحاد الأوروبي وقانون مجلس أوروبا. لكن عند معالجة البيانات الخاصة بالآخرين فيما يتعلق بنشاط شخصي أو منزلي بحت، لا يخضع الأفراد لقواعد اللائحة العامة لحماية البيانات والاتفاقية 108 المحدثة، ولا يُعتبرون بمثابة مراقبين.[209] وقد يُعفى الفرد الذي يحتفظ بمراسلاته، وبمذكرات شخصية تصف الأحداث التي صادفته مع الأصدقاء والزملاء، والسجلات الصحية لأفراد الأسرة، من قواعد حماية البيانات، حيث يمكن أن تكون هذه الأنشطة شخصية بحتة أو مجرد أنشطة منزلية. وتحدد اللائحة العامة لحماية البيانات أيضاً أن الأنشطة الشخصية أو المنزلية يمكن أن تشمل كذلك النشاط على شبكات التواصل الاجتماعي وعبر الإنترنت عندما يكون في سياق هذه الأنشطة.[210] وعلى عكس ذلك، تنطبق قواعد حماية البيانات بالكامل على المراقبين والمعالجين الذين يوفرون وسائل معالجة البيانات الشخصية الخاصة بالأنشطة الشخصية أو المنزلية (على سبيل المثال، منصات التواصل الاجتماعي).[211]

إن وصول المواطنين إلى الإنترنت وإمكانية استخدام منصات التجارة الإلكترونية وشبكات التواصل الاجتماعي ومواقع التدوين لنشر معلومات شخصية عن أنفسهم وأشخاص آخرين يصعبان بشكل متزايد فصل المعالجة الشخصية عن غير الشخصية.[212] ويعتمد تحديد ما إذا كانت الأنشطة شخصية أو منزلية بحتة على الظروف الخاصة بكل حالة.[213] فالأنشطة التي لها جوانب مهنية أو تجارية لا يمكن أن تندرج ضمن إطار الإعفاء الخاص بالأنشطة المنزلية.[214] وبالتالي، عندما يشير حجم وتكرار معالجة البيانات إلى نشاط مهني أو بدوام كامل، يمكن اعتبار الفرد مراقباً. وعلاوة على الطابع المهني أو التجاري لنشاط المعالجة، هناك عامل آخر يجب أن يؤخذ بعين الاعتبار وهو ما إذا كانت البيانات الشخصية متاحة لعدد كبير من الأشخاص خارج المجال الخاص للفرد. وقد خلصت السوابق القضائية ضمن إطار الأمر التوجيهي الخاص بحماية البيانات إلى أن قانون حماية البيانات ينطبق عند نشر شخص خاص، أثناء استخدام الإنترنت، بيانات عن أشخاص آخرين على موقع إلكتروني عام. ولم تحكم محكمة العدل التابعة للاتحاد الأوروبي بعد في وقائع مماثلة ضمن إطار اللائحة العامة لحماية البيانات، والتي تقدم مزيداً من الإرشادات حول الموضوعات التي يمكن اعتبارها خارج نطاق تشريع حماية البيانات ضمن إطار «الإعفاء الخاص بالأنشطة المنزلية»، مثل استخدام وسائل التواصل الاجتماعي لأغراض شخصية.

مثال: تتناول قضية «بوديل ليندغفيست»[215] مسألة الإشارة إلى مجموعة من الأشخاص بالاسم أو بطرق أخرى، مثل أرقام هواتفهم أو معلومات عن هواياتهم، على إحدى صفحات الإنترنت. وقد اعتبرت محكمة العدل التابعة للاتحاد الأوروبي أن «فعل الإشارة، على صفحة الإنترنت، إلى مجموعة من الأشخاص وتحديدهم بأسمائهم أو بطرق أخرى [...] هو بمثابة 'معالجة كلية أو جزئية للبيانات بوسائل آلية'« بالمعنى المقصود في المادة 3 (1) من الأمر التوجيهي الخاص بحماية البيانات.[216]

لا تندرج معالجة البيانات الشخصية هذه ضمن الأنشطة الشخصية أو المنزلية البحتة، والتي تقع خارج نطاق قواعد حماية البيانات في الاتحاد الأوروبي، حيث إن هذا الاستثناء «يجب [...] تفسيره على أنه يتعلق فقط بالأنشطة التي يتم تنفيذها في سياق الحياة الخاصة أو الأسرية للأفراد، وهو ما لا ينطبق على معالجة البيانات الشخصية التي تتضمن النشر على الإنترنت بحيث تصبح هذه البيانات في متناول عدد غير محدد من الأشخاص».[217]

[208] فريق عمل المادة 29 (2010)، الرأي رقم 2010/1 بشأن مفهومي «المراقب» و«المعالج»، WP 169، بروكسيل، 16 فبراير 2010

[209] اللائحة العامة لحماية البيانات، الحيثية 18 والمادة 2 (2) (ج)؛ الاتفاقية 108 المحدثة، المادة 3 (2).

[210] اللائحة العامة لحماية البيانات، الحيثية 18.

[211] نفس المرجع السابق، الحيثية 18؛ التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 29.

[212] انظر بيان فريق عمل المادة 29 بشأن المناقشات المتعلقة بحزمة إصلاح حماية البيانات (2013)، الملحق 2: المقترحات والتعديلات المتعلقة بالإعفاء الخاص بالأنشطة الشخصية أو المنزلية، 27 فبراير 2013.

[213] التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 28.

[214] انظر اللائحة العامة لحماية البيانات، الحيثية 18 والتقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 27.

[215] محكمة العدل التابعة للاتحاد الأوروبي، رقم C-101/01، «الدعوى الجنائية ضد بوديل ليندغفيست»، 6 نوفمبر 2003.

[216] نفس المرجع السابق، الفقرة 27؛ الأمر التوجيهي السابق رقم EC/95/46، المادة 3 (1)، اللائحة العامة لحماية البيانات حالياً، المادة 2

[217] محكمة العدل التابعة للاتحاد الأوروبي، رقم C-101/01، «الدعوى الجنائية ضد بوديل ليندغفيست»، 6 نوفمبر 2003، الفقرة 47.

ووفقاً لمحكمة العدل التابعة للاتحاد الأوروبي، يمكن لتشريعات حماية البيانات في الاتحاد الأوروبي أن تشمل كذلك التسجيلات المرئية لكاميرات المراقبة المثبتة لأغراض شخصية في ظروف معينة.

مثال: في قضية «فرانتيشيك رينيش»،[218] التقط السيد رينيش صورة لشخصين حطما النوافذ في منزله من خلال نظام كاميرات مراقبة منزلي كان قد ثبته لحماية ممتلكاته. وقد تم تسليم التسجيل فيما بعد لرجال الشرطة وتم الاعتماد عليه في الإجراءات الجنائية.
ورأت محكمة العدل التابعة للاتحاد الأوروبي أنه «بما أن كاميرات المراقبة [...] تغطي، ولو جزئيا، فضاء عاماً، وهي موجهة بالتالي إلى خارج الفضاء الخاص للشخص الذي عالج البيانات بتلك الصورة، فإنه لا يمكن اعتبارها نشاطاً 'شخصياً أو منزلياً' بحتاً».[219]

**مراقب البيانات**

**في قانون الاتحاد الأوروبي**، يُعرَّف مراقب البيانات بأنه شخص «يحدد بمفرده أو بالاشتراك مع آخرين أغراض ووسائل معالجة البيانات الشخصية».[220] كما يحدد قرار المراقب سبب وكيفية معالجة البيانات.

وفي **قانون مجلس أوروبا**، تُعرّف الاتفاقية 108 المحدثة «مراقب البيانات» على أنه «الشخص الذاتي أو الاعتباري، أو الهيئة العامة، أو المصلحة، أو الوكالة أو أي هيئة أخرى تتمتع، بمفردها أو بالاشتراك مع آخرين، بصلاحية اتخاذ القرار فيما يتعلق بمعالجة البيانات».[221] وتهم صلاحية اتخاذ القرار هذه أغراض ووسائل المعالجة، بالإضافة إلى فئات البيانات التي يجب معالجتها، والوصول إلى البيانات.[222] هذا ويجب تحديد ما إذا كانت هذه الصلاحية مستمدة من تعيين قانوني أو من ظروف وقائعية بناءً على كل حالة على حدة.[223]

مثال: في قضية «غوغل إسبانيا»،[224] رفع مواطن إسباني دعوة سعياً منه إلى سحب تقرير إخباري في إحدى الجرائد يخص سجله المالي من غوغل. وقد سئلت محكمة العدل التابعة للاتحاد الأوروبي عما إذا كانت شركة «غوغل»، بصفتها مشغل محرك البحث، هي «مراقب البيانات» بالمعنى المقصود في المادة 2 (د) من الأمر التوجيهي الخاص بحماية البيانات.[225] ونظرت المحكمة في تعريف واسع لمفهوم «مراقب البيانات» لضمان «الحماية الفعالة والكاملة لأصحاب البيانات».[226] وقد خلصت إلى أن مشغل محرك البحث قد حدد أغراض ووسائل النشاط وأتاح البيانات التي تم تحميلها على صفحات الإنترنت من قبل ناشري المواقع الإلكترونية لأي مستخدم إنترنت يقوم بإجراء بحث بناءً على اسم صاحب البيانات.[227] لذلك، قررت المحكمة أنه يمكن اعتبار «غوغل» بمثابة «مراقب للبيانات».[228]

عندما يكون مقر مراقب البيانات أو المعالج خارج الاتحاد الأوروبي، يتعين على هذه الشركة تعيين ممثل داخل الاتحاد الأوروبي كتابياً.[229] وتشدد اللائحة العامة لحماية البيانات على وجوب تواجد الممثل «في إحدى الدول الأعضاء حيث يتواجد أصحاب البيانات الذين تتم معالجة بياناتهم الشخصية بغرض عرض السلع والخدمات لهم، أو الذين يتم تتبع سلوكهم».[230] وفي حال لم يتم تعيين ممثل، يمكن بدء الإجراءات القانونية ضد المراقب أو المعالج نفسه[231].

[218] محكمة العدل التابعة للاتحاد الأوروبي، رقم C-212/13، قضية «فرانتيشيك رينيش ضد مكتب حماية البيانات الشخصية»، 11 ديسمبر 2014، الفقرة 33.
[219] الأمر التوجيهي السابق رقم EC/95/46، المادة 3 (2) الشق الثاني، اللائحة العامة لحماية البيانات حالياً، المادة 2 (2) (ج).
[220] اللائحة العامة لحماية البيانات، المادة 4 (7).
[221] الاتفاقية 108 المحدثة، المادة 2 (د).
[222] التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 22.
[223] نفس المرجع السابق.
[224] محكمة العدل التابعة للاتحاد الأوروبي، رقم C-131/12، قضية «غوغل إسبانيا وشركة غوغل ضد الوكالة الإسبانية لحماية البيانات وماريو كوستيخا غونزاليس» [الغرفة الكبرى]، 13 مايو 2014.
[225] اللائحة العامة لحماية البيانات، المادة 4 (7)؛ محكمة العدل التابعة للاتحاد الأوروبي، رقم C-131/12، قضية «غوغل إسبانيا وشركة غوغل ضد الوكالة الإسبانية لحماية البيانات وماريو كوستيخا غونزاليس» [الغرفة الكبرى]، 13 مايو 2014، الفقرة 21.
[226] محكمة العدل التابعة للاتحاد الأوروبي، رقم C-131/12، قضية «غوغل إسبانيا وشركة غوغل ضد الوكالة الإسبانية لحماية البيانات وماريو كوستيخا غونزاليس» [الغرفة الكبرى]، 13 مايو 2014، الفقرة 34.
[227] نفس المرجع السابق، الفقرات 40-35.
[228] نفس المرجع السابق، الفقرة 41.
[229] اللائحة العامة لحماية البيانات، المادة 27 (1).
[230] نفس المرجع السابق، المادة 27 (3).
[231] نفس المرجع السابق، المادة 27 (5).

**المراقبة المشتركة للبيانات**

تنص اللائحة العامة لحماية البيانات على أنه عندما يقوم مراقبان أو أكثر على نحو مشترك بتحديد الغرض من المعالجة ووسائلها، فإنهم يعتبرون مراقبين مشتركين (أي مراقبين بالتشارك). هذا يعني أنهم قرروا سوية معالجة البيانات لغرض مشترك.[232] وينص التقرير التفسيري للاتفاقية 108 المحدثة على جواز وجود عدة مراقبين مشتركين - أو نظام مراقبة مشتركة للبيانات - ضمن **إطار مجلس أوروبا**.[233]

ويشير فريق عمل المادة 29 إلى أن المراقبة المشتركة للبيانات قد تتخذ أشكالاً مختلفة، وأن مشاركة المراقبين المختلفين في أنشطة مراقبة البيانات يجوز لها أن تكون غير متساوية.[234] وتمكن هذه المرونة من تلبية احتياجات معالجة البيانات التي تزداد تعقيداً يوماً بعد يوم.[235] لذلك يجب على المراقبين المشتركين تحديد مسؤوليات كل واحد منهم فيما يخص الامتثال للالتزامات المنصوص عليها في اللائحة وذلك في إطار اتفاق محدد.[236]

تترتب عن المراقبة المشتركة مسؤولية مشتركة تجاه أعمال المعالجة.[237] وفي إطار قانون الاتحاد الأوروبي، يعني هذا الأمر أنه يمكن تحميل كل مراقب أو معالج المسؤولية الكاملة عن الضرر الكامل الناجم عن المعالجة في إطار المراقبة المشتركة، وذلك لضمان تعويض صاحب البيانات بشكل فعال.[238]

مثال: إن قاعدة البيانات التي يتم تشغيلها بشكل مشترك من قبل العديد من مؤسسات الائتمان بشأن عملائها المتعثرين هي مثال شائع للمراقبة المشتركة للبيانات. وعندما يتقدم شخص ما بطلب للحصول على خط ائتمان من أحد البنوك الأعضاء في نظام المراقبة المشتركة، يستعين البنك بقاعدة البيانات المشتركة لاتخاذ قرار مستنير بشأن الجدارة الائتمانية لمقدم الطلب.

لا تنص المقتضيات القانونية صراحةً على ما إذا كانت المراقبة المشتركة للبيانات تتطلب أن يكون الغرض المشترك هو نفسه لكل واحد من المراقبين أو ما إذا كان يكفي أن تكون أغراضهم متداخلة جزئياً فقط. وحتى اللحظة، لا توجد سوابق قضائية ذات صلة على المستوى الأوروبي. وفي رأيه لعام 2010 بشأن المراقبين والمعالجين، ينصح فريق عمل المادة 29 على أنه يجوز للمراقبين المشتركين تشارك جميع أغراض ووسائل المعالجة كما يمكنهم تشارك بعض الأغراض أو الوسائل فقط أو جزء منها.[239] وفي حين أن الخيار الأول قد يعني ضمنياً وجود علاقة وثيقة جداً بين مختلف الفاعلين، فإن الخيار الثاني يشير إلى علاقة أقل تقييداً.

هذا ويدعو فريق عمل المادة 29 إلى تفسير أوسع لمفهوم المراقبة المشتركة بهدف السماح ببعض المرونة للاستجابة للتعقيد المتزايد لواقع معالجة البيانات الحالي.[240] وتوضح القضية المتعلقة بجمعية الاتصالات المالية العالمية بين البنوك (SWIFT) موقف فريق العمل.

مثال: في القضية التي عرفت بقضية «سويفت» (أي «جمعية الاتصالات المالية العالمية بين البنوك (SWIFT)»)، وظفت مؤسسات بنكية أوروبية هذه الأخيرة، في البداية بصفة معالج، لتشغيل نقل البيانات في سياق المعاملات البنكية. وقد أفشت الجمعية هذه البيانات، المخزنة في مركز خدمات الحوسبة في الولايات المتحدة، إلى وزارة الخزانة الأمريكية دون أن تصدّر لها أوامر صريحة للقيام بذلك من قبل المؤسسات البنكية الأوروبية التي وظفتها. وقد خلص فريق عمل المادة 29، عند تقييم مشروعية هذا الوضع، إلى أن المؤسسات البنكية الأوروبية التي وظفت الجمعية، وكذلك الجمعية نفسها، يجب أن يُنظر إليها على أنها بمثابة مراقبين مشتركين أمام العملاء الأوروبيين، وتتحمل جميعها مسؤولية إفشاء بياناتهم إلى السلطات الأمريكية.[241]

---

[232] نفس المرجع السابق، المادة 4 (7) والمادة 26.

[233] الاتفاقية 108 المحدثة، المادة 2 (د)؛ التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 22.

[234] فريق عمل المادة 29 (2010)، الرأي رقم 2010/1 بشأن مفهومي «المراقب» و«المعالج»، WP 169، بروكسيل، 16 فبراير 2010، ص. 19.

[235] نفس المرجع السابق.

[236] اللائحة العامة لحماية البيانات، الحيثية 79.

[237] نفس المرجع السابق، الفقرة 21.

[238] نفس المرجع السابق، المادة 82 (4).

[239] فريق عمل المادة 29 (2010)، الرأي رقم 2010/1 بشأن مفهومي «المراقب» و«المعالج»، WP 169، بروكسيل، 16 فبراير 2010، ص. 19.

[240] نفس المرجع السابق.

[241] فريق عمل المادة 29 (2010)، الرأي رقم 2006/1 بشأن معالجة البيانات الشخصية من قبل جمعية الاتصالات المالية العالمية بين البنوك (SWIFT)، WP 128، بروكسيل، 22 نوفمبر 2006.

**المعالج**

يُعرَّف المعالج في **قانون الاتحاد الأوروبي** بأنه الشخص الذي يعالج البيانات الشخصية نيابة عن المراقب.[242] وقد تقتصر الأنشطة الموكلة إلى المعالج على مهمة محددة أو سياق محدد للغاية أو قد تكون عامة وشاملة.

وفي **قانون مجلس أوروبا**، فإن معنى المعالج هو نفسه الوارد في قانون الاتحاد الأوروبي.[243]
إلى جانب معالجة البيانات نيابة عن الآخرين، سيكون المعالجون أيضاً بمثابة مراقبين للبيانات فيما يتعلق بالمعالجة التي يؤدونها لأغراضهم الخاصة، كإدارة شؤون موظفيهم ومبيعاتهم وحساباتهم على سبيل المثال.

مثال: تختص شركة «إيفريديي» بمعالجة البيانات لإدارة بيانات الموارد البشرية لشركات أخرى. وعند أدائها لهذه هذه الوظيفة، تعد الشركة بمثابة معالج. لكن عندما تعالج بيانات موظفيها، فهي تصبح المراقب في العمليات المنفذة لغرض الوفاء بالتزاماتها كصاحب عمل.

**العلاقة بين المراقب والمعالج**

وكما رأينا سابقاً، يُعرّف المراقب بأنه الشخص الذي يحدد أغراض ووسائل المعالجة. وتنص اللائحة العامة لحماية البيانات بوضوح على أنه لا يمكن للمعالج أن يعالج البيانات الشخصية إلا بناءً على تعليمات من المراقب، الا إذا طلب قانون الاتحاد الأوروبي أو قانون الدول الأعضاء من المعالج القيام بذلك.[244] ويعد العقد بين المراقب والمعالج عنصراً أساسياً في علاقتهما، وهو شرط قانوني.[245]

مثال: قرر مدير شركة «صانشاين» أن شركة «كلاودي» - المختصة في تخزين البيانات على مستوى السحابة - يجب أن تدير بيانات عملاء شركته. بناء على ذلك، تظل شركة «صانشاين» هي المراقب، بينما تبقى شركة «كلاودي» هي المعالج، لأن هذه الأخيرة، وفقاً للعقد، لا يجوز لها استخدام بيانات عملاء شركة «صانشاين» إلا للأغراض التي تحددها هذه الأخيرة.

وفي حال تفويض سلطة تحديد وسائل المعالجة إلى المعالج، يجب أن يكون المراقب مع ذلك قادراً على ممارسة درجة مناسبة من الإشراف على قرارات المعالج فيما يتعلق بوسائل المعالجة. وتظل المسؤولية العامة على عاتق المراقب، والذي يجب أن يشرف على المعالجين للتأكد من أن قراراتهم تتوافق مع قانون حماية البيانات وتعليماته الخاصة.

علاوة على ذلك، في حال عدم احترام المعالج لشروط معالجة البيانات على النحو المحدد من قبل المراقب، فسيصبح المعالج هو المراقب على الأقل في حدود تعليمات المراقب التي تم خرقها. وسيؤدي هذا الوضع على الأرجح إلى جعل المعالج مراقباً يعمل بشكل غير قانوني. وفي المقابل، سيتعين على المراقب الأولي أن يشرح كيف كان من ممكنا للمعالج أن ينتهك صلاحياته.[246] ويميل فريق عمل المادة 29 إلى افتراض المراقبة المشتركة في مثل هذه الحالات، لأن هذا يسمح بأفضل حماية لمصالح أصحاب البيانات.[247]

قد تكون هناك أيضاً إشكاليات متعلقة بتقسيم المسؤولية عندما يكون المراقب شركة صغيرة والمعالج شركة كبيرة لها القدرة على إملاء شروط خدماتها. ومع ذلك، في مثل هذه الظروف، يؤكد فريق عمل المادة 29 على أنه لا ينبغي خفض معيار المسؤولية على أساس عدم التوازن الاقتصادي وأنه يجب الحفاظ على مغزى مفهوم المراقب.[248]

---

[242] اللائحة العامة لحماية البيانات، المادة 4 (8).
[243] الاتفاقية 108 المحدثة، المادة 2 (و).
[244] اللائحة العامة لحماية البيانات، المادة 29.
[245] نفس المرجع السابق، المادة 28 (3).
[246] نفس المرجع السابق، المادة 82 (2).
[247] فريق عمل المادة 29 (2010)، الرأي 2010/1 بشأن مفهومي «المراقب» و«المعالج»، WP 169، بروكسيل، 16 فبراير 2010، ص. 25؛ فريق عمل المادة 29 (2006)، الرأي 10/2006 بشأن معالجة البيانات الشخصية من قبل جمعية الاتصالات المالية العالمية بين البنوك (SWIFT)، WP 128، بروكسيل، 22 نوفمبر 2006.
[248] فريق عمل المادة 29 (2010)، الرأي 2010/1 بشأن مفهومي «المراقب» و«المعالج»، WP 169، بروكسيل، 16 فبراير 2010، ص. 26؛

وحتى يتحقق الوضوح والشفافية، يجب تسجيل تفاصيل العلاقة بين المراقب والمعالج في عقد مكتوب.[249] ويجب أن يتضمن هذا الأخير على وجه الخصوص موضوع المعالجة وطبيعتها والغرض منها ومدتها ونوع البيانات الشخصية وفئات أصحاب البيانات. كما يجب أن ينص على التزامات وحقوق المراقب والمعالج، مثل المتطلبات المتعلقة بالسرية والأمن. ويعتبر عدم وجود مثل هذا العقد انتهاكاً لالتزام المراقب بتقديم وثائق مكتوبة تتضمن المسؤوليات المتبادلة، وقد يؤدي إلى فرض عقوبات. وعندما يحدث الضرر نتيجة للتصرف خارج إطار التعليمات القانونية للمراقب أو عدم الامتثال لها، لا يمكن تحميل المراقب المسؤولية وحده، وإنما يشاركه فيها المعالج.[250] ويجب أن يحتفظ المعالج بسجلات لجميع فئات أنشطة المعالجة التي يقوم بها نيابة عن المراقب.[251] هذا ويجب إتاحة هذه السجلات للهيئة الإشرافية عند طلبها إياها، حيث يجب أن يتعاون كل من المراقب والمعالج مع تلك الهيئة خلال أداء مهامها.[252] كما يمكن للمراقبين والمعالجين الالتزام بمدونة سلوك معتمدة أو بإحدى آليات إصدار شهادات التصديق لإثبات امتثالهم لمتطلبات اللائحة العامة لحماية البيانات.[253]

وقد يرغب المعالجون في تفويض مهام معينة إلى معالجين فرعيين إضافيين. هذا الأمر مسموح به قانوناً، شريطة أن يتم وضع البنود التعاقدية المناسبة بين المراقب والمعالج، بما في ذلك ما إذا كان ترخيص المراقب ضرورياً في كل حالة على حدة أو ما إذا كان الإخبار وحده كافياً. وتنص اللائحة العامة لحماية البيانات على أن المعالج الأولي يظل مسؤولاً بالكامل أمام المراقب في حال عدم وفاء المعالج الفرعي بالتزاماته الخاصة بحماية البيانات.[254]

وبموجب **قانون مجلس أوروبا**، فإن تفسير مفهومي المراقب والمعالج، كما هو موضح أعلاه، قابل للتطبيق بالكامل.[255]

## 2.3.2. المتلقون والأطراف الثالثة

يكمن الاختلاف بين هاتين الفئتين من الأشخاص أو الكيانات، واللتين تم تقديمهما في الأمر التوجيهي الخاص بحماية البيانات، بشكل أساسي في علاقتهما بالمراقب، وبالتالي، في الترخيص لهما بالوصول إلى البيانات الشخصية التي يحتفظ بها المراقب.

يقصد بـ «الطرف الثالث» شخص غير المراقب والمعالج. ووفقاً للمادة 4 (10) من اللائحة العامة لحماية البيانات، فإن الطرف الثالث هو «شخص ذاتي أو اعتباري، أو هيئة عامة، أو وكالة أو أي هيئة أخرى مرخص لها بمعالجة البيانات الشخصية غير صاحب البيانات والمراقب والمعالج والأشخاص الذين يخضعون لسلطة المراقب أو المعالج المباشرة». هذا يعني أن الأشخاص الذين يعملون في منظمة غير المنظمة التي تتولى مهمة المراقب - حتى لو كانت تنتمي إلى نفس المجموعة أو الشركة القابضة - سيكونون بمثابة «طرف ثالث» (أو ينتمون إليه). ومن ناحية أخرى، فإن فروع بنك تعالج حسابات العملاء تحت السلطة المباشرة لمقرهم الرئيسي لن تكون «أطرافاً ثالثة».[256]

إن «المتلقي» مصطلح أوسع من مصطلح «الطرف الثالث». فبالمعنى المقصود في المادة 4 (9) من اللائحة العامة لحماية البيانات، يقصد بالمتلقي «شخص ذاتي أو اعتباري، أو هيئة عامة، أو وكالة أو أي هيئة أخرى، يتم الكشف له عن البيانات، سواء أكان طرفًا ثالثًا أم لا». وقد يكون هذا المتلقي إما شخصاً غير المراقب أو المعالج - وسيكون بذلك طرفًا ثالثاً - أو شخصاً ضمن الهيئة التي تتولى مهمة المراقب أو المعالج، مثل موظف أو قسم آخر داخل نفس الشركة أو الهيئة.

وتكمن أهمية التمييز بين المتلقين والأطراف الثالثة فقط في شروط الكشف القانوني عن البيانات. فقد يكون موظفو المراقب أو المعالج عبارة عن متلقين للبيانات الشخصية دون الحاجة إلى مزيد من المتطلبات القانونية إذا كانوا يشاركون في عمليات المعالجة الخاصة بالمراقب أو المعالج. في المقابل، فإن الطرف الثالث، غير المراقب أو المعالج، غير مصرح له باستخدام البيانات الشخصية التي يعالجها المراقب، ما لم يكن ذلك لأسباب قانونية محددة في حالة بعينها.

---

[249] اللائحة العمة لحماية البيانات، المادة 28 (3) و(9).
[250] نفس المرجع السابق، المادة 82 (2).
[251] نفس المرجع السابق، المادة 30 (2).
[252] نفس المرجع السابق، المادة 30 (4) و31.
[253] نفس المرجع السابق، المادتين 28 (5) و42 (4).
[254] نفس المرجع السابق، المادة 28 (4).
[255] انظر، على سبيل المثال، الاتفاقية 108 المحدثة، المادة 2 (ب) و(و)؛ التوصيات الخاصة بالتنميط، المادة 1.
[256] فريق عمل المادة 29 (2010)، الرأي 2010/1 بشأن مفهومي «المراقب» و«المعالج»، WP 169، بروكسيل، 16 فبراير 2010، ص. 31؛

مثال: إن الموظف لدى المراقب، الذي يستخدم البيانات الشخصية في نطاق المهام التي أوكلها إليه صاحب العمل، هو متلق للبيانات، ولكنه ليس طرفاً ثالثاً، لأنه يستخدم البيانات نيابة عن المراقب وبناء على تعليماته. على سبيل المثال، إذا كشف صاحب العمل عن بيانات شخصية حول موظفيه لقسم الموارد البشرية في ضوء تقييمات الأداء القادمة، فسيكون فريق الموارد البشرية عبارة عن متلقين للبيانات الشخصية، حيث تم الكشف عن البيانات لهم أثناء معالجتها نيابة عن المراقب. لكن في حال قدمت المؤسسة بيانات عن موظفيها لشركة تدريب ستستخدمها لتصميم برنامج تدريب للموظفين، تصبح شركة التدريب عبارة عن طرف ثالث. والسبب هو أن شركة التدريب ليس لديها شرعية محددة أو ترخيصاً محدداً (والذي ينبع في حالة «الموارد البشرية» من علاقة العمل مع مراقب البيانات) لمعالجة هذه البيانات الشخصية. بمعنى آخر، لم تتلقى الشركة المعلومات أثناء عملها مع المراقب.

## 4.2. الموافقة

### النقاط الرئيسية

- إن الموافقة كأساس قانوني لمعالجة البيانات الشخصية يجب أن تُمنح بحرية، وعن علم، وبشكل محدد، وأن تكون بمثابة إشارة واضحة لا لبس فيها إلى الرغبات من خلال إجراء تأكيدي واضح يدل على الموافقة على المعالجة.
- إن معالجة الفئات الخاصة من البيانات تتطلب موافقة صريحة.

كما سنرى بشكل مفصل في الفصل 4، تعد الموافقة أحد الأسس المشروعة الستة لمعالجة البيانات الشخصية. وتعني الموافقة «أي إشارة لرغبات صاحب البيانات يتم إعطاؤها بحرية وبشكل محدد ومستنير ولا لبس فيه»،[257]

يحدد **قانون الاتحاد الأوروبي** العديد من العناصر لكي تكون الموافقة صحيحة. وتهدف هذه العناصر إلى ضمان أن أصحاب البيانات يقصدون حقاً الموافقة على استخدام معين لبياناتهم:[258]

- يجب منح الموافقة من خلال إجراء تأكيدي واضح يمثل إشارة مقدمة بحرية وبشكل محدد ومستنير ولا لبس فيه لموافقة صاحب البيانات على معالجة بياناته الشخصية. قد يكون هذا الإجراء فعلًا أو قولاً.
- يجب أن يكون لصاحب البيانات الحق في سحب الموافقة في أي وقت.
- في سياق إعلان كتابي يغطي أيضاً مسائل أخرى، مثل «شروط الخدمة»، يجب أن تكون طلبات الموافقة بلغة واضحة وبسيطة وبشكل يسهل فهمه واستيعابه، مما يميز بوضوح الموافقة عن الأمور الأخرى؛ إذا كان هناك جزء من هذا الإعلان ينتهك اللائحة العامة لحماية البيانات، فإنه لن يكون ملزماً.

لن تكون الموافقة صحيحة في سياق قانون حماية البيانات إلا إذا تم استيفاء جميع هذه المتطلبات. وتقع على عاتق المراقب مسؤولية إثبات أن صاحب البيانات وافق على معالجة بياناته.[259] وستتم مناقشة عناصر الموافقة الصحيحة بشكل أكثر تفصيلاً في الجزء 1.1.4 المتعلق بالأسس القانونية لمعالجة البيانات الشخصية.

لا تتضمن الاتفاقية 108 تعريفاً للموافقة؛ فذلك متروك للقانون المحلي. ومع ذلك، بموجب **قانون مجلس أوروبا**، تتوافق عناصر الموافقة الصحيحة مع العناصر الموضحة سابقاً.[260]

[257] اللائحة العامة لحماية البيانات، المادة 4 (11). انظر أيضاً الاتفاقية 108 المحدثة، المادة 5 (2).
[258] اللائحة العامة لحماية البيانات، المادة 7.
[259] نفس المرجع السابق، المادة 7 (1).
[260] الاتفاقية 108 المحدثة، المادة 5 (2)؛ التقرير التفسيري للاتفاقية 108 المحدثة، من الفقرة 42 إلى الفقرة 45.

إن المتطلبات الإضافية للموافقة الصحيحة بموجب القانون المدني، مثل الأهلية القانونية، تنطبق بشكل طبيعي أيضاً في سياق حماية البيانات، لأن هذه المتطلبات هي عبارة عن شروط مسبقة قانونية أساسية. وستؤدي الموافقة غير الصحيحة للأشخاص الذين لا يتمتعون بالأهلية القانونية إلى عدم وجود أساس قانوني لمعالجة البيانات المتعلقة بهؤلاء الأشخاص. وفيما يتعلق بالأهلية القانونية للقاصرين فيما يخص إبرام العقود، تنص اللائحة العامة لحماية البيانات على أن قواعدها بشأن الحد الأدنى لسن الحصول على موافقة صحيحة لا تؤثر على قانون العقود العام للدول الأعضاء.[261]

ويجب منح الموافقة بطريقة واضحة حتى لا تترك أي شك حول نية صاحب البيانات.[262] كما يجب أن تكون الموافقة صريحة عندما يتعلق الأمر بمعالجة البيانات الحساسة، ويمكن أن تكون شفهية أو كتابية.[263] ويمكن أن تكون هذه الأخيرة بوسائل إلكترونية.[264] وفي إطار كل من **قانون الاتحاد الأوروبي وقانون مجلس أوروبا**، يجب منح الموافقة على معالجة البيانات الشخصية للفرد قولاً أو من خلال إجراء تأكيدي واضح.[265] وبالتالي، لا يمكن استنتاج الموافقة من الصمت أو الخانات أو النماذج المملوءة مسبقًا أو من غياب الفعل.[266]

[261] اللائحة العامة لحماية البيانات، المادة 8 (3).
[262] نفس المرجع السابق، المادتان 6 (1) (أ) و9 (2) (أ).
[263] نفس المرجع السابق، الحيثية 32.
[264] نفس المرجع السابق.
[265] نفس المرجع السابق، المادة 4 (11)؛ التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 42.
[266] اللائحة العامة لحماية البيانات، الحيثية 32؛ التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 42

# 3
# المبـــادئ الرئيسيـــة لقانـــون حمايـــة البيانـــات الأوروبـــي

| الاتحاد الأوروبي | المسائل المتناولة | مجلس أوروبا |
|---|---|---|
| اللائحة العامة لحماية البيانات، المادة 5 (1) (أ) | مبدأ المشروعية | الاتفاقية 108 المحدثة، المادة 5 (3) |
| اللائحة العامة لحماية البيانات، المادة 5 (1) (أ) | مبدأ الإنصاف | الاتفاقية 108 المحدثة، المادة 5 (4) (أ)<br>المحكمة الأوروبية لحقوق الإنسان، قضية «ك. ه. وآخرون ضد سلوفاكيا»، رقم 04/32881، 2009 |
| اللائحة العامة لحماية البيانات، المادة 5 (1) (أ)<br>محكمة العدل التابعة للاتحاد الأوروبي، قضية C-201/14، «سمارانداً بارا وآخرون ضد الصندوق الوطني للتأمين الصحي وآخرين»، 2015 | مبدأ الشفافية | الاتفاقية 108 المحدثة، المادة 5 (4) (أ) والمادة 8<br>المحكمة الأوروبية لحقوق الإنسان، قضية «هارالامبي ضد رومانيا»، رقم 03/21737، 2009 |
| اللائحة العامة لحماية البيانات، المادة 5 (1) (ب) | مبدأ حصر الغرض | الاتفاقية 108 المحدثة، المادة 5 (4) (ب) |
| اللائحة العامة لحماية البيانات، المادة 5 (1) (ج)<br>محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-293/12 و C-594/12، «ديجيتال رايتس آيرلند وحكومة كيرنتن وآخرون» [الغرفة الكبرى]، 2014. | مبدأ تقليل البيانات | الاتفاقية 108 المحدثة، المادة 5 (4) (ج) |
| اللائحة العامة لحماية البيانات، المادة 5 (1) (د)<br>محكمة العدل التابعة للاتحاد الأوروبي، رقم C-553/07، قضية «مجلس العمدة وضباط القانون في روتردام ضد م. إ. إ. رايكيبور»، 2009 | مبدأ صحة البيانات | الاتفاقية 108 المحدثة، المادة 5 (4) (د) |

| | | |
|---|---|---|
| اللائحة العامة لحماية البيانات، المادة 5 (1) (ه) محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-293/12 وC-594/12، «ديجيتال رايتس آيرلند وحكومة كيرنتن وآخرون» [الغرفة الكبرى]، 2014. | مبدأ حصر مدة التخزين | الاتفاقية 108 المحدثة، المادة 5 (4) (ه) المحكمة الأوروبية لحقوق الإنسان، قضية «س. و مارير ضد المملكة المتحدة» [الغرفة الكبرى]، رقم 04/30562 ورقم 04/30566، 2008 |
| اللائحة العامة لحماية البيانات، المادتان 5 (1) (و) و32 | مبدأ أمن (سلامة وسرية) البيانات | الاتفاقية 108 المحدثة، المادة 7 |
| اللائحة العامة لحماية البيانات، المادة 5 (2) | مبدأ المساءلة | الاتفاقية 108 المحدثة، المادة 10 |

تحدد المادة 5 من اللائحة العامة لحماية البيانات المبادئ التي تؤطر معالجة البيانات الشخصية. وتشمل هذه المبادئ ما يلي:

- المشروعية والإنصاف والشفافية؛
- حصر الغرض؛
- تقليل البيانات ؛
- صحة البيانات؛
- حصر مدة التخزين؛
- السلامة والسرية.

تشكل المبادئ نقطة انطلاق لأحكام أكثر تفصيلاً في المواد التي تليها ضمن اللائحة. وتظهر أيضاً في المواد 5 و7 و8 و10 من الاتفاقية 108 المحدثة. ويجب أن تمتثل جميع تشريعات حماية البيانات اللاحقة على مستوى مجلس أوروبا أو الاتحاد الأوروبي لهذه المبادئ، ويتعين أخذ هذه الأخيرة بعين الاعتبار عند تفسير مثل هذه التشريعات. وبموجب قانون الاتحاد الأوروبي، لا يُسمح بفرض قيود على مبادئ المعالجة إلا بالقدر الذي تتوافق فيه مع الحقوق والالتزامات المنصوص عليها في المواد من 12 إلى 22، كما يجب أن تحترم جوهر الحقوق والحريات الأساسية. ويجوز أن يكون منصوصاً على استثناءات وقيود تخص هذه المبادئ الأساسية على مستوى الاتحاد الأوروبي أو على المستوى الوطني؛ حيث يجب أن ينص عليها القانون، وأن تسعى لتحقيق هدف مشروع، وأن تكون عبارة عن تدابير ضرورية ومتناسبة في مجتمع ديمقراطي. جميع هذه الشروط الثلاثة يجب استيفاؤها.

[267] الاتفاقية 108 المحدثة، المادة 11 (1)؛ اللائحة العامة لحماية البيانات، المادة 23 (1).

[268] اللائحة العامة لحماية البيانات، المادة 23 (1).

## 1.3. مبادئ مشروعية معالجة البيانات وإنصافها وشفافيتها

### النقاط الرئيسية

- تنطبق مبادئ المشروعية والإنصاف والشفافية على جميع عمليات معالجة البيانات الشخصية.
- بموجب اللائحة العامة لحماية البيانات، تتطلب المشروعية أحد هذه الشروط:
  - موافقة صاحب البيانات؛
  - الضرورة لإبرام عقد؛
  - التزام قانوني؛
  - الضرورة لحماية المصالح الحيوية لصاحب البيانات أو شخص آخر؛
  - الضرورة لأداء مهمة لخدمة المصلحة العامة؛
  - الضرورة لخدمة المصالح المشروعة للمراقب أو لطرف ثالث، إذا لم تطغى عليها مصالح وحقوق صاحب البيانات.

- يجب أن تتم معالجة البيانات الشخصية بطريقة منصفة.
- يتعين إبلاغ صاحب البيانات بالمخاطر للتأكد من أنه ليست للمعالجة آثار سلبية غير متوقعة.

- يجب أن تتم معالجة البيانات الشخصية بطريقة شفافة.
- يتعين على المراقبين إبلاغ أصحاب البيانات قبل معالجة بياناتهم بشأن الغرض من المعالجة وهوية المراقب وعنوانه، من ضمن تفاصيل أخرى.
- يجب تقديم المعلومات المتعلقة بعمليات المعالجة بلغة واضحة وبسيطة للسماح لأصحاب البيانات باستيعاب القواعد والمخاطر والضمانات والحقوق المعنية بسهولة.
- يحق لأصحاب البيانات الوصول إلى بياناتهم أينما تمت معالجتها.

### 1.1.3. مشروعية المعالجة

تتطلب **قوانين حماية البيانات في الاتحاد الأوروبي ومجلس أوروبا** معالجة البيانات الشخصية بشكل قانوني.[269] وتتطلب المعالجة القانونية موافقة صاحب البيانات أو أساسا شرعياً آخر ينص عليه التشريع الخاص بحماية البيانات.[270] وتتضمن المادة 6 (1) من اللائحة العامة لحماية البيانات خمسة أسس قانونية للمعالجة، إلى جانب الموافقة، وهي عندما تكون معالجة البيانات الشخصية ضرورية لتنفيذ عقد، أو لأداء مهمة يتم تنفيذها في إطار ممارسة السلطة العامة، أو للامتثال لالتزام قانوني، أو لغرض المصالح المشروعة للمراقب أو الأطراف الثالثة، أو إذا كانت ضرورية لحماية المصالح الحيوية لصاحب البيانات. وسيتم مناقشة هذا الأمر بشكل أكثر تفصيلاً في الجزء 1.4.

### 2.1.3. الإنصاف في المعالجة

بالإضافة إلى مشروعية المعالجة، تتطلب قوانين حماية البيانات في الاتحاد الأوروبي ومجلس أوروبا أن تتم معالجة البيانات الشخصية بشكل منصف.[271] ويؤطر مبدأ المعالجة المنصفة في المقام الأول العلاقة بين المراقب وصاحب البيانات.

ينبغي على المراقبين إخطار أصحاب البيانات وعامة الناس بأنهم سيعالجون البيانات بطريقة قانونية وشفافة ويجب أن يكونوا قادرين على إثبات امتثال عمليات المعالجة للائحة العامة لحماية البيانات. ويجب ألا تجري عمليات المعالجة في السر، كما يجب أن يكون أصحاب البيانات على دراية بالمخاطر المحتملة. علاوة على ذلك، يجب على المراقبين التصرف، قدر الإمكان، بطريقة تمتثل فوراً لرغبات صاحب البيانات، لا سيما عندما تشكل موافقته الأساس القانوني لمعالجة البيانات.

---

[269] الاتفاقية 108 المحدثة، المادة 5 (3)؛ اللائحة العامة لحماية البيانات، المادة 5 (1) (أ).

[270] ميثاق الحقوق الأساسية للاتحاد الأوروبي، المادة 8 (2)؛ اللائحة العامة لحماية البيانات، الحيثية 40 والمواد من 6 إلى 9؛ الاتفاقية 108 المحدثة، المادة 5 (2)؛ التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 41.

[271] اللائحة العامة لحماية البيانات، المادة 5 (1) (أ)؛ الاتفاقية 108 المحدثة، المادة 5 (4) (أ).

مثال: في قضية «ك. ه. وآخرون ضد سلوفاكيا»،[272] تم علاج المدعيات - وهن نساء تنحدرن من الروما - في مستشفيين في شرق سلوفاكيا خلال الحمل والولادة. لكن فيما بعد، لم تتمكن أي منهن من الإنجاب مرة أخرى على الرغم من عدة محاولات. وقد أمرت المحاكم الوطنية المستشفيين بالسماح للمدعيات وممثليهن بالاطلاع على السجلات الطبية واقتباس أجزاء منها بخط اليد، لكنها رفضت طلبهن المتعلق بنسخ الوثائق، زاعمة أن السبب وراء ذلك هو منع إساءة استغلالها. غير أن الالتزامات الإيجابية للدول بموجب المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان قد تضمنت بالضرورة التزاماً بإتاحة نسخ من ملفات البيانات الخاصة بصاحب البيانات لهذا الأخير. وكان من واجب الدولة أن تحدد الترتيبات الخاصة بنسخ ملفات البيانات الشخصية، أو عند الاقتضاء، تقديم أسباب مقنعة لرفض القيام بذلك. وفي هذه القضية بالذات، بررت المحاكم المحلية منع المدعيات من نسخ سجلاتهن الطبية أساساً بالحاجة إلى حماية المعلومات ذات الصلة من سوء الاستغلال. لكن المحكمة الأوروبية لحقوق الإنسان لم تفهم كيف يمكن للمدعيات، اللاتي تم منحهن،في كل الاحوال، حق الوصول إلى ملفاتهن الطبية كاملة، إساءة استخدام المعلومات المتعلقة بهن. علاوة على ذلك، كان من الممكن منع خطر حدوث سوء الاستغلال هذا بوسائل أخرى غير رفض نسخ المدعيات لملفاتهن، مثل الحد من عدد الأشخاص الذين يحق لهم الوصول إلى الملفات. هذا ولم تتمكن الدولة من إثبات وجود أسباب مقنعة بما يكفي لحرمان المدعيات من الوصول الفعلي إلى المعلومات المتعلقة بصحتهن. وبالتالي، خلصت المحكمة إلى أنه تم انتهاك المادة 8.

وفيما يتعلق بخدمات الإنترنت، يجب أن تمكن خصائص أنظمة معالجة البيانات أصحاب البيانات من فهم ما الذي يحدث فعلا لبياناتهم، وعلى أي حال، يتجاوز مبدأ الإنصاف التزامات الشفافية ويمكن أيضاً ربطه بمعالجة البيانات الشخصية بطريقة أخلاقية.

مثال: أجرى قسم الأبحاث بإحدى الجامعات تجربة لتحليل تغيرات الحالة المزاجية لدى 50 شخصاً. وقد طُلب من هؤلاء تسجيل أفكارهم في ملف إلكتروني كل ساعة في وقت معين. وقد أعطى الأشخاص الخمسون موافقتهم على هذا المشروع بالذات، وهذا الاستخدام المحدد للبيانات من قبل الجامعة. لكن سرعان ما اكتشف قسم الأبحاث أن تسجيل الأفكار إلكترونياً سيكون مفيداً جداً لمشروع آخر يركز على الصحة العقلية، ينسقه فريق آخر. وعلى الرغم من أنه كان بإمكان الجامعة، بصفتها المراقب، أن تستخدم نفس البيانات في عمل فريق آخر دون خطوات إضافية لضمان مشروعية معالجة تلك البيانات، بالنظر إلى أن الغرضين متوافقين، أبلغت الجامعة أصحاب البيانات وطلبت موافقة جديدة، متبعة بذلك مدونة أخلاقيات البحث ومبدأ المعالجة المنصفة.

## 3.1.3. شفافية المعالجة

تقتضي **قوانين حماية البيانات في الاتحاد الأوروبي ومجلس أوروبا** أن تتم معالجة البيانات الشخصية «بطريقة شفافة فيما يتعلق بصاحب البيانات»،[273] ينص هذا المبدأ على التزام المراقب باتخاذ أي إجراء مناسب من أجل إبقاء أصحاب البيانات - الذين قد يكونون مستخدمين أو زبناء أو عملاء - على علم بكيفية استخدام بياناتهم،[274] وقد تشير الشفافية إلى المعلومات المقدمة للفرد قبل بدء المعالجة،[275] وإلى المعلومات التي يجب أن تكون متاحة بسهولة لأصحاب البيانات خلال المعالجة،[276] وكذلك إلى المعلومات المقدمة لأصحاب البيانات بعد طلب الوصول إلى بياناتهم الخاصة.[277]

مثال: في قضية «هارالامبي ضد رومانيا»،[278] لم يُسمح للمدعي بالوصول إلى المعلومات المتعلقة به التي تحتفظ بها أجهزة المخابرات السرية إلا بعد خمس سنوات من طلبه. وقد عاودت المحكمة الأوروبية لحقوق الإنسان التأكيد على أن لدى الأفراد الذين كانوا موضوع ملفات شخصية بحوزة السلطات العامة مصلحة حيوية في التمكن من الوصول إليها. وكان واجباً على السلطات توفير إجراء فعال لتسهيل الوصول إلى هذه المعلومات. واعتبرت المحكمة الأوروبية لحقوق الإنسان أنه لا كمية الملفات المنقولة ولا أوجه القصور في نظام الأرشيف تبرر تأخيراً لمدة خمس سنوات في الموافقة على طلب المدعي الوصول إلى ملفاته. هذا ولم تقدم السلطات للمدعي أي إجراء فعال ومتاح لتمكينه من الوصول إلى ملفاته الشخصية في غضون فترة زمنية معقولة. وخلصت المحكمة إلى أنه كان هناك انتهاك للمادة 8 من الاتفاقية الأوروبية لحقوق الإنسان.

[272] المحكمة الأوروبية لحقوق الإنسان، قضية «ك. ه. وآخرون ضد سلوفاكيا»، رقم 04/32881، 28 أبريل 2009.
[273] اللائحة العامة لحماية البيانات، المادة 5 (1) (أ)؛ الاتفاقية 108 المحدثة، المادتان 5 (4) (أ) و8.
[274] اللائحة العامة لحماية البيانات، المادة 12.
[275] نفس المرجع السابق، المادتان 13 و14.
[276] فريق عمل المادة 29، الرأي 2017/2 بشأن معالجة البيانات في مقر العمل، ص. 23.
[277] اللائحة العامة لحماية البيانات، المادة 15.
[278] المحكمة الأوروبية لحقوق الإنسان، قضية «هارالامبي ضد رومانيا»، رقم 03/21737، 27 أكتوبر 2009.

هذا ويجب شرح عمليات المعالجة لأصحاب البيانات بطريقة يسهل استيعابها مما يضمن فهمهم لما سيحدث لبياناتهم. هذا يعني أن الغرض المحدد لمعالجة البيانات الشخصية يجب أن يكون معروفاً من قبل صاحب البيانات عند جمع البيانات الشخصية.[279] وتقتضي شفافية المعالجة استخدام لغة واضحة وبسيطة،[280] ويجب أن تكون المخاطر والقواعد والضمانات والحقوق المتعلقة بمعالجة البيانات الشخصية واضحة بالنسبة للأشخاص المعنيين.[281]

ويحدد **قانون مجلس أوروبا** كذلك أن بعض المعلومات الأساسية يجب تقديمها إلزاماً بصورة استباقية من قبل المراقب إلى أصحاب البيانات. ويمكن تقديم معلومات عن اسم وعنوان المراقب (أو المراقبين المشتركين)، والأساس القانوني لمعالجة البيانات وأغراضها، وفئات البيانات المعالجة والمتلقين، إلى جانب وسائل ممارسة الحقوق، بأي صيغة مناسبة (إما من خلال موقع إلكتروني، أو أدوات تكنولوجية على الأجهزة الشخصية، أو غيرها) طالما يتم تقديمها بشكل منصف وفعال لصاحب البيانات. ويجب أن تكون المعلومات المقدمة متاحة بسهولة وسهلة القراءة ومفهومة ومكيفة مع أصحاب البيانات (بلغة مراعية للأطفال عند الضرورة على سبيل المثال). كما يجب إتاحة أي معلومات إضافية ضرورية لضمان معالجة منصفة للبيانات أو مفيدة لهذا الغرض، مثل فترة الحفظ أو معرفة المنطق وراء معالجة البيانات أو المعلومات المتعلقة بنقل البيانات إلى متلق في دولة طرف أخرى أو في دولة غير طرف (بما يشمل ما إذا كانت هذه الأخيرة توفر مستوى مناسباً من الحماية أو التدابير المتخذة من قبل المراقب لضمان مثل هذا المستوى المناسب من حماية البيانات).[282]

ووفقاً للحق في الوصول إلى البيانات،[283] يحق لصاحب البيانات بناءً على طلبه، أن يتم إخباره من قبل المراقب إذا كانت بياناته قيد المعالجة، وإذا كان الأمر كذلك، أن يتم إخباره أي بيانات تخضع لهذه المعالجة.[284] إضافة إلى ذلك، وفقاً للحق في الإخبار،[285] يجب إبلاغ الأشخاص الذين تتم معالجة بياناتهم بشأن أغراض المعالجة مدتها ووسائلها، من ضمن تفاصيل أخرى، بشكل استباقي من قبل المراقبين أو المعالجين، مبدئياً قبل بدء نشاط المعالجة.

مثال: تتعلق قضية «سمارانديا بارا وآخرون ضد رئيس الصندوق الوطني للتأمين الصحي والوكالة الوطنية لإدارة الضرائب»[286] بنقل البيانات الضريبية المتعلقة بدخل الأشخاص العاملين لحسابهم الخاص من الوكالة الوطنية لإدارة الضرائب إلى الصندوق الوطني للتأمين الصحي في رومانيا، والذي على أساسه كان مطلوباً دفع متأخرات رسوم التأمين الصحي. وقد طُلب من محكمة العدل التابعة للاتحاد الأوروبي تحديد ما إذا كان ينبغي تقديم معلومات مسبقة إلى صاحب البيانات فيما يتعلق بهوية مراقب البيانات والغرض من نقل هذه البيانات قبل معالجتها من طرف الصندوق الوطني للتأمين الصحي. واعتبرت المحكمة أنه عندما تقوم هيئة إدارية عامة لدولة عضو بنقل البيانات الشخصية إلى هيئة إدارية عامة أخرى تقوم بدورها بمعالجة هذه البيانات، يجب إبلاغ أصحاب البيانات بهذا النقل أو هذه المعالجة.

تسمح بعض الحالات على نحو الاستثناء بعدم التقيد بالالتزام المتعلق بإشعار أصحاب البيانات بخصوص معالجة البيانات، وسيتم تناولها باستفاضة في الجزء 1.6 الخاص بحقوق صاحب البيانات.

[279] اللائحة العامة لحماية البيانات، الحيثية 39.
[280] نفس المرجع السابق.
[281] نفس المرجع السابق.
[282] التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 68.
[283] اللائحة العامة لحماية البيانات، المادة 15.
[284] الاتفاقية 108 المحدثة، المادتان 8 و9 (1) (ب).
[285] اللائحة العامة لحماية البيانات، المادتان 13 و14.
[286] محكمة العدل التابعة للاتحاد الأوروبي، رقم C-201/14، قضية «سمارانديا بارا وآخرون ضد الصندوق الوطني للتأمين الصحي وآخرين»، 1 أكتوبر 2015، الفقرات من 28 إلى 46.

## 2.3. مبدأ حصر الغرض

### النقاط الرئيسية

- يجب حصر الغرض من المعالجة قبل الشروع فيها.
- لا يمكن إجراء مزيد من عمليات المعالجة للبيانات على نحو لا يتوافق مع الغرض الأصلي، بالرغم من إشارة اللائحة العامة لحماية البيانات إلى استثناءات متعلقة بهذه القاعدة لأغراض الأرشفة من أجل المصلحة العامة أو لأغراض البحث العلمي والتاريخي ولأغراض إحصائية.
- من حيث الجوهر، يقصد بمبدأ حصر الغرض أن أي معالجة للبيانات الشخصية يجب أن تتم لغرض محدد ومعين وفقط لأغراض إضافية ومحددة تتوافق مع الغرض الأصلي.

إن مبدأ حصر الغرض يعد من المبادئ الأساسية لقانون حماية البيانات الأوروبي، وهو مرتبط ارتباطاً وثيقاً بالشفافية والتوقعية وتحكم المستخدم: إذا كان الغرض من المعالجة محدداً وواضحاً بشكل كافٍ، فإن الأفراد يدركون ما سيتوقعونه، وبذلك يتم تعزيز الشفافية واليقين القانوني. وفي نفس الوقت، يعد التحديد الواضح للغرض مهماً لتمكين أصحاب البيانات من ممارسة حقوقهم بفعالية، كالحق في الاعتراض على المعالجة.[287]

ويقتضي المبدأ أن أي عملية معالجة للبيانات الشخصية يجب أن تجرى لغرض محدد ومعين وفقط لأغراض إضافية ومحددة تتوافق مع الغرض الأصلي.[288] وبالتالي، تعد معالجة البيانات الشخصية ذات الغرض غير المحدد و/أو غير المقيد غير قانونية. وينطبق الأمر عينه على معالجة البيانات الشخصية التي لا يكون لها غرض معين أو التي تكون مبنية فقط على كونها قد تكون مفيدة في المستقبل. وستتوقف مشروعية معالجة البيانات الشخصية على الغرض منها والذي يجب أن يكون صريحاً ومحدداً ومشروعاً.

يجب أن يكون لكل غرض جديد لمعالجة البيانات لا يتوافق مع الغرض الأصلي أساسه القانوني الخاص ولا يمكن أن يرتكز على كون أن البيانات قد تم الحصول عليها أو معالجتها لغرض مشروع آخر. ومن ناحية أخرى، تكون المعالجة المشروعة محدودة في الغرض المحدد في البداية وسيتطلب أي غرض جديد للمعالجة أساساً قانونياً جديداً منفصلاً. وعلى سبيل المثال، يجب النظر بعناية في مسألة كشف البيانات الشخصية لأطراف أخرى لغرض جديد، لأن هذا الكشف سيتطلب أساساً قانونياً إضافياً مغايراً عن ذلك الذي جمعت البيانات من أجله.

مثال: تجمع شركة طيران البيانات من ركابها للقيام بالحجوزات لتدبير رحلة الطيران بشكل ملائم. وستحتاج شركة الطيران إلى بيانات حول: أرقام مقاعد الركاب والإعاقات الجسدية الخاصة، كالحاجة للكراسي المتحركة؛ والمتطلبات الغذائية الخاصة، كطعام «الكوشر» والأكل الحلال. وإذا طلب من شركات الطيران إرسال هذه البيانات، الموجودة في سجل اسم الركاب، إلى سلطات الهجرة في مطار الوصول، فإن هذه البيانات قد استعملت لأغراض المراقبة الخاصة بالهجرة، والتي تختلف عن الغرض الأولي لجمع البيانات.
إن إرسال هذه البيانات إلى السلطة المكلفة بالهجرة سيتطلب أساساً قانونياً جديداً ومنفصلاً.

عند النظر في نطاق غرض معين وحدوده، ترتكز الاتفاقية 108 المحدثة واللائحة العامة لحماية البيانات على مبدأ التوافق: يُسمح باستخدام البيانات لأغراض متوافقة بناء على الأساس القانوني الأولي. لذلك، فإن معالجة البيانات الإضافية لا يمكن أن تتم بطريقة غير متوقعة وغير مناسبة أو غير مقبولة بالنسبة لصاحب البيانات.[289] ولتقييم ما إذا كانت المعالجة الإضافية تعتبر متوافقة، يتعين على المراقب أن يأخذ بعين الاعتبار ( ضمن جملة من الأمور) ما يلي:

[287] فريق عمل المادة 29 (2013)، الرأي رقم 2013/3 بشأن حصر الغرض، 2 ،WP 203 أبريل 2013.
[288] اللائحة العامة لحماية البيانات، المادة 5 (1) (ب).
[289] التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 49.

- «أي صلة بين هذه الأغراض والأغراض الخاصة بالمعالجة الإضافية المراد القيام بها؛
- السياق الذي تم فيه جمع البيانات الشخصية، خاصة فيما يتعلق بالتوقعات المعقولة لأصحاب البيانات فيما يخص استخدامها الإضافي بناء على علاقتهم بالمراقب؛
- طبيعة البيانات الشخصية؛
- الآثار المترتبة عن المعالجة الإضافية المراد القيام بها بالنسبة لأصحاب البيانات؛
- وجود ضمانات في كل من عمليات المعالجة الأصلية والمعالجة المزمع القيام بها لاحقاً.»[290] على سبيل المثال، يمكن القيام بهذا الأمر من خلال التشفير أو استخدام أسماء مستعارة.

مثال: تحصل شركة «صانشاين» على بيانات العملاء في إطار إدارة العلاقات مع العملاء. ثم ترسل هذه البيانات إلى شركة تسويق مباشر، وهي شركة «مونلايت» التي تريد استخدام البيانات لدعم حملات تسويقية لشركات أخرى. يشكل إرسال شركة «صانشاين» للبيانات لاستعمالها من أجل التسويق من قبل شركات أخرى استعمالاً إضافيا للبيانات لغرض جديد، وهو ما لا يتوافق مع إدارة العلاقات مع العملاء، والغرض الأولي لشركة «صانشاين» من تجميع بيانات العملاء. وعليه، فإن إرسال البيانات إلى شركة «مونلايت» يتطلب أساساً قانونياً خاصاً به.
في المقابل، يعد استعمال شركة «صانشاين» لبيانات إدارة العلاقات مع العملاء لأغراض تسويقية خاصة بها، أي إرسال رسائل تسويقية خاصة بمنتجاتها لعملائها، مقبولاً على العموم كغرض متوافق.

تصرح اللائحة العامة لحماية البيانات والاتفاقية 108 المحدثة أن «المعالجة الإضافية لأغراض الأرشفة التي تصب في المصلحة العامة ولأغراض البحث العلمي والتاريخي أو لأغراض إحصائية» تعتبر على الأرجح متوافقة مع الغرض الأولي.[291] إلا أنه يجب وضع ضمانات مناسبة أثناء معالجة البيانات الشخصية لاحقا من قبيل إخفاء مصدر البيانات أو تشفيرها أو استعمال أسماء مستعارة، وتقييد الوصول إلى البيانات.[292] وتضيف اللائحة العامة لحماية البيانات أنه «في حال أعطى صاحب البيانات موافقته أو كانت المعالجة مبنية على قانون الاتحاد أو الدولة العضو وتشكل ضرورة وتكون تدبيراً متناسباً في مجتمع ديمقراطي لصون أهداف مصلحة عامة مهمة على وجه الخصوص، يتعين السماح للمراقب إجراء معالجة إضافية على البيانات الشخصية بغض النظر عن توافق الأغراض.»[293] أثناء القيام بمعالجة إضافية، ينبغي إشعار صاحب البيانات بأغراضها،و كذلك بحقوقه بما فيها حق الاعتراض.[294]

## 3.3. مبدأ تقليل البيانات

### النقاط الرئيسية

- يجب أن تكون معالجة البيانات محدودة فيما هو ضروري لتحقيق غرض مشروع.
- يتعين إجراء معالجة البيانات الشخصية فقط إذا كان من غير الممكن تحقيق الغرض منها بشكل معقول بأي طريقة أخرى.
- لا يمكن أن تتداخل معالجة البيانات بشكل غير متناسب مع المصالح والحقوق والحريات الموجودة على المحك.

تتم معالجة هذه البيانات فقط على أنها «ملائمة وذات صلة وغير مبالغ فيها بالنظر إلى الغرض التي جمعت من أجله و/أو تمت معالجتها بصورة إضافية من أجله.»[295] يجب أن تكون فئات البيانات المختارة من أجل المعالجة ضرورية قصد تحقيق الهدف العام المصرح به لعمليات المعالجة، ويتعين على المراقب تحديد جمع البيانات بصرامة في المعلومات ذات صلة مباشرة بالغرض المحدد الذي تسعى إليه المعالجة.

[290] اللائحة العامة لحماية البيانات، الحيثية 50 والمادة 6 (4)؛ القرار التفسيري للاتفاقية 108 المحدثة، الفقرة 49.
[291] اللائحة العامة لحماية البيانات، المادة 5 (1) (ب)؛ الاتفاقية 108 المحدثة، المادة 5 (4) (ب). ومن بين هذه المقتضيات الوطنية نجد قانون حماية البيانات النمساوي (Datenschutzgesetz)، الجريدة الرسمية للقانون الاتحادي ا، رقم 165/1999، الفقرة 46.
[292] اللائحة العامة لحماية البيانات المادة 6 (4)؛ الاتفاقية 108 المحدثة، المادة 5 (4) (ب)؛ التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 50.
[293] اللائحة العامة لحماية البيانات، الحيثية 50.
[294] نفس المرجع السابق.
[295] الاتفاقية 108 المحدثة، المادة 5 (4) (ج)؛ اللائحة العامة لحماية البيانات، المادة 5 (1) (ج).

مثال: في قضية شركة» ديجيتال رايتس آيرلاند»،[296] ترى محكمة العدل التابعة للاتحاد الأوروبي أن صلاحية الأمر التوجيهي بشأن الاحتفاظ بالبيانات، الذي هدف إلى مواءمة المقتضيات الوطنية الخاصة بالاحتفاظ بالبيانات الشخصية المولدة أو المعالجة من قبل خدمات الاتصالات أو الشبكات الإلكترونية المتاحة للعموم من أجل إرسالها المحتمل للسلطات المختصة لمحاربة الجرائم الخطيرة، كالجريمة المنظمة والإرهاب. وبغض النظر عن أن هذا الأمر قد اعتبر غرضاً يستجيب حقاً لمصلحة عامة، إلا أن الصيغة العامة التي جاء بها الأمر التوجيهي في هذا الصدد: «جميع الأفراد وجميع وسائل الاتصال الإلكتروني وكذلك جميع بيانات الحركة دون أي تمييز أو قيود أو استثناءات في ضوء هدف مكافحة الجرائم الخطيرة»، قد اعتبرت إشكالية.[297]

علاوة على ذلك، من خلال استخدام تكنولوجيا تعزيز الخصوصية، من الممكن في بعض الأحيان تجنب استخدام البيانات الشخصية كليا، أو استخدام تدابير لتقليل القدرة على إسناد البيانات إلى صاحبها (على سبيل المثال، من خلال استخدام اسم مستعار)، وهو ما يترتب عنه حل يراعي الخصوصية. ويعد هذا الأمر مناسباً بشكل خاص في أنظمة المعالجة الواسعة النطاق.

مثال: يقدم مجلس المدينة بطاقة رقاقة للمستخدمين المنتظمين لنظام النقل العام في المدينة مقابل رسوم معينة. ويكتب اسم المستخدم على واجهة البطاقة وأيضاً على الرقاقة في صيغة إلكترونية. عند استخدام الحافلة أو الترام، يجب تمرير بطاقة الرقاقة أمام أجهزة القراءة المثبتة، على سبيل المثال، في الحافلات والترام. ويتم التثبت من البيانات التي يقرأها الجهاز إلكترونياً من خلال قاعدة بيانات تحتوي على أسماء الأشخاص الذين اشتروا بطاقة التنقل.

إن هذا النظام لا يلتزم بمبدأ تقليل البيانات بالطريقة المثلى: يمكن التحقق مما إذا كان مسموحاً للفرد باستخدام مرافق النقل دون مقارنة البيانات الشخصية الموجودة على البطاقة الذكية بقاعدة بيانات، على سبيل المثال، يكفي وجود صورة إلكترونية خاصة، مثل الرمز الشريطي، في شريحة البطاقة التي تمرر أمام جهاز القراءة، لتؤكد ما إذا كانت البطاقة صالحة أم لا. لن يقوم مثل هذا النظام بتسجيل من استخدم مرفق النقل وفي أي وقت. سيكون هذا هو الحل الأمثل بالمعنى المقصود في مبدأ التقليل، حيث ينتج عن هذا المبدأ الالتزام بتقليل جمع البيانات.

تنص المادة 5 (1) من الاتفاقية 108 المحدثة على شرط التناسبية لمعالجة البيانات الشخصية فيما يتعلق بالغرض المشروع المنشود. ويجب أن يكون هناك توازن عادل بين جميع المصالح المعنية في جميع مراحل المعالجة. وهذا يعني أنه «يجب اعتبار البيانات الشخصية الملائمة وذات الصلة والتي قد تؤدي إلى تدخل غير متناسب في الحقوق والحريات الأساسية مبالغاً فيها.» [298]

## 4.3. مبدأ دقة البيانات

### النقاط الرئيسية

- يجب تنفيذ مبدأ دقة البيانات من قبل المراقب في جميع عمليات المعالجة.
- يجب محو البيانات غير الدقيقة أو تصحيحها دون تأخير.
- قد يتوجب فحص البيانات بانتظام وتحديثها لضمان الدقة.

لا يجوز للمراقب الذي يحتفظ بالمعلومات الشخصية استخدام هذه المعلومات دون اتخاذ خطوات للتأكد بدرجة معقولة من اليقين من أن البيانات دقيقة ومحدثة.

يجب النظر إلى الالتزام بضمان دقة البيانات في سياق الغرض من معالجة البيانات.[299]

[296] محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-293/12 وC-594/12، قضية «شركة ديجيتال رايتس آيرلاند» المحدودة ضد وزير الاتصالات والموارد البحرية والطبيعية وآخرين» وحكومة كيرنتن وآخرين [الغرفة الكبرى]، 8 أبريل 2014.

[297] نفس المرجع السابق، الفقرتان 44 و57.

[298] التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 52؛ اللائحة العامة لحماية البيانات، المادة 5 (1) (ج).

[299] اللائحة العامة لحماية البيانات، المادة 5 (1) (د)؛ الاتفاقية 108 المحدثة، المادة 5 (4) (د).

مثال: في قضية «ريكبوور»،[300] نظرت محكمة العدل التابعة لاتحاد الأوروبي في طلب مواطن هولندي لتلقي معلومات من الإدارة المحلية لمدينة أمستردام حول هوية الأشخاص الذين تم إبلاغهم بالسجلات الخاصة به التي كانت توجد في حوزة السلطة المحلية في العامين السابقين، وكذلك على محتوى البيانات التي تم الكشف عنها. ذكرت محكمة العدل أن «الحق في الخصوصية يعني إمكانية تأكد صاحب البيانات من معالجة بياناته الشخصية بطريقة صحيحة وقانونية، أي على وجه الخصوص، أن البيانات الأساسية المتعلقة به دقيقة وأنه تم الكشف عنها للجهات المتلقية المصرح لها». ثم أشارت المحكمة إلى مقدمة الأمر التوجيهي بشأن حماية البيانات، والتي تنص على أن أصحاب البيانات يجب أن يتمتعوا بالحق في الوصول إلى بياناتهم الشخصية حتى يتمكنوا من التحقق من صحتها.[301]

قد تكون هناك أيضا حالات يكون فيها تحديث البيانات المخزنة محظوراً قانوناً، لأن الغرض من تخزين البيانات هو بشكل أساسي يتمثل في توثيق الأحداث باعتبارها «لمحة» (بمعنى نبذة أو لقطة) تاريخية.

مثال: لا يجب تغيير السجل الطبي لعملية ما، بمعنى آخر «تحديثه»، حتى وإن تبين لاحقاً أن النتائج المذكورة في السجل كانت خاطئة. وفي مثل هذه الظروف، لا يجوز سوى الإدلاء بإضافات على الملاحظات الواردة في السجل، طالما تم تمييزها بوضوح على أنها مساهمات مقدمة في مرحلة لاحقة.

من ناحية أخرى، هناك حالات يكون فيها من الضروري للغاية تحديث البيانات والتحقق بانتظام من دقتها، بسبب الضرر المحتمل الذي قد يلحق بصاحب البيانات إذا ظلت البيانات غير دقيقة.

مثال: إذا أراد شخص ما إبرام عقد ائتماني مع مؤسسة بنكية، يتحقق البنك عادة من الجدارة الائتمانية للعميل المحتمل. لهذا الغرض، توجد قواعد بيانات خاصة تتضمن معلومات عن التاريخ الائتماني للأفراد بصفتهم الشخصية. إذا كانت قاعدة البيانات هذه توفر بيانات غير صحيحة أو قديمة عن شخص ما، فقد يعاني هذا الشخص من آثار سلبية. لذلك يتعين على مراقبي قواعد البيانات مثل هذه بذل جهود خاصة لاتباع مبدأ الدقة.

## 5.3. مبدأ حصر مدة التخزين

### النقاط الرئيسية

- يرمي مبدأ حصر مدة التخزين إلى ضرورة حذف البيانات الشخصية أو جعلها مجهولة المصدر بمجرد انتفاء الحاجة إليها لتحقيق الأغراض التي جُمعت من أجلها.

تنص المادة 5 (1) (هـ) من اللائحة العامة لحماية البيانات، وكذلك المادة 5 (4) (هـ) من الاتفاقية 108 المحدثة على «الاحتفاظ بالبيانات الشخصية في شكل يسمح بتحديد أصحاب البيانات لمدة لا تزيد عن الوقت اللازم لتحقيق أغراض معالجة البيانات. لذلك يجب محو البيانات أو إخفاء هوية صاحبها عندما يتم تحقيق هذه الأغراض. ولهذه الغاية، «يجب وضع حدود زمنية من قبل المراقب لمحو البيانات أو القيام بمراجعة دورية» للتأكد من الاحتفاظ بالبيانات لمدة لا تزيد عن اللازم.[302]

في قضية» س. ومارير»، خلصت المحكمة الأوروبية لحقوق الإنسان إلى أن المبادئ الأساسية للصكوك ذات الصلة الخاصة بمجلس أوروبا، وقانون وممارسة الأطراف المتعاقدة الأخرى، تنص على الاحتفاظ بالبيانات بشكل يتناسب مع الغرض من جمعها ويكون محدوداً في الوقت، ولا سيما في قطاع الشرطة.[303]

[300] محكمة العدل التابعة للاتحاد الأوروبي، رقم C-553/07، «مجلس العمدة وأعضاء مجلس بلدية روتردام ضد إم إي إي ريكبوور»، 7 مايو 2009.

[301] الحيثية السابقة 41 ، ديباجة الأمر التوجيهي رقم EC/95/46.

[302] اللائحة العامة لحماية البيانات، الحيثية 39.

[303] المحكمة الأوروبية لحقوق الإنسان، قضية س. مارير ضد المملكة المتحدة [الغرفة الكبرى]، الرقمان 30562/04 و30566/04، 4 ديسمبر 2008؛ انظر أيضاً، على سبيل المثال، المحكمة الأوروبية لحقوق الإنسان، قضية م. م. ضد المملكة المتحدة، رقم 24029/07، 13 نوفمبر 2012.

مثال: في قضية «س. ومارير»،[304] قضت المحكمة الأوروبية لحقوق الإنسان بأن الاحتفاظ إلى أجل غير مسمى ببصمات الأصابع وعينات الخلايا وملفات الحمض النووي للمدعيين غير متناسب وغير ضروري في مجتمع ديمقراطي، اخذة بعين الاعتبار أن الإجراءات الجنائية ضد كلا المدعيين قد تم إنهاؤها بموجب حكم بالبراءة ووقف المتابعة على التوالي.

تنطبق المهلة الزمنية لتخزين البيانات الشخصية فقط على البيانات المحفوظة في شكل يسمح بتحديد أصحابها. وبالتالي، يمكن أن يتم التخزين القانوني للبيانات التي لم تعد هناك حاجة إليها عن طريق إخفاء هوية صاحب البيانات.

قد يتم تخزين البيانات المؤرشفة لغرض المصلحة العامة أو لأغراض علمية أو تاريخية، أو للاستخدام الإحصائي، لفترات أطول بشرط استخدامها فقط للأغراض المذكورة أعلاه.[305] ويجب تنفيذ التدابير التقنية والتنظيمية المناسبة للتخزين المستمر واستخدام البيانات الشخصية لصون حقوق وحريات صاحب البيانات.

كما تفتح الاتفاقية 108 المحدثة المجال لاستثناءات خاصة بمبدأ حصر مدة التخزين، بشرط أن ينص عليها القانون، وتحترم جوهر الحقوق والحريات الأساسية، وتكون ضرورية ومتناسبة لتحقيق عدد محدود من الأهداف المشروعة.[306] وتشمل، ضمن جملة من الأمور الأخرى، حماية الأمن الوطني، والتحقيق في الجرائم الجنائية ومقاضاة مرتكبيها، وتنفيذ العقوبات الجنائية، وحماية أصحاب البيانات وحماية حقوق الأشخاص الآخرين وحرياتهم الأساسية.

مثال: في قضية شركة «ديجيتال رايتس آيرلاند»،[307] نظرت محكمة العدل التابعة للاتحاد الأوروبي في صلاحية الأمر التوجيهي بشأن بالاحتفاظ بالبيانات، والذي كان يهدف إلى مواءمة الأحكام الوطنية المتعلقة بالاحتفاظ بالبيانات الشخصية التي يتم توليدها أو معالجتها بواسطة خدمات أو شبكات الاتصالات الإلكترونية المتاحة للجمهور لمكافحة الجرائم الخطيرة، مثل الجريمة المنظمة والإرهاب. وقد فرض الأمر التوجيهي بشأن الاحتفاظ بالبيانات فترة للاحتفاظ بالبيانات وحددها في «ستة أشهر على الأقل، دون أي تمييز بين فئات البيانات المنصوص عليها في المادة 5 من ذلك الأمر التوجيهي على أساس فائدتها المحتملة بالنسبة لأغراض الهدف المنشود أو وفقاً للأشخاص المعنيين».[308] ولقد أثارت محكمة العدل أيضا مسألة عدم وجود معايير موضوعية في الأمر التوجيهي بشأن الاحتفاظ بالبيانات، والذي على أساسها يجب تحديد الفترة المحددة للاحتفاظ بالبيانات - والتي يمكن أن تتراوح من ستة أشهر كحد أدنى إلى 24 شهراً كحد أقصى - من أجل ضمان اقتصار هذه الفترة على ما هو ضروري للغاية.[309]

## 6.3. مبدأ أمن البيانات

### النقاط الرئيسية

- إن أمن وسرية البيانات الشخصية عاملان مهمان لمنع الآثار السلبية على صاحب البيانات.
- يمكن أن تكون التدابير الأمنية ذات طابع تقني و/أو تنظيمي.
- إن استخدام أسماء مستعارة عملية يمكن أن تحمي البيانات الشخصية.
- يجب تحديد ملاءمة التدابير الأمنية على أساس كل حالة على حدة ويجب أن تتم مراجعتها بانتظام.

[304] المحكمة الأوروبية لحقوق الإنسان، قضية س. مارير ضد المملكة المتحدة [الغرفة الكبرى]، الرقمان 30562/04 و30566/04، 4 ديسمبر 2008.
[305] اللائحة العامة لحماية البيانات، المادة 5 (1) (ه)؛ الاتفاقية 108 المحدثة، المادتان 5 (4) (ب) و11 (2).
[306] الاتفاقية 108 المحدثة، المادة 1.11؛ التقرير التفسيري للاتفاقية 108 المحدثة، الفقرات من91 إلى 98.
[307] محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-293/12 و C-594/1، شركة «ديجيتال رايتس آيرلاند» ضد وزير الاتصالات والموارد البحرية والطبيعية وآخرين وحكومة كيرنتن وآخرين [الغرفة الكبرى]، 8 أبريل 2014.
[308] نفس المرجع السابق، الفقرة 63.
[309] نفس المرجع السابق، الفقرة 64.

يستدعي مبدأ أمن البيانات تفعيل التدابير التقنية أو التنظيمية المناسبة أثناء معالجة البيانات الشخصية لحمايتها من الوصول إليها أو استخدامها أو تعديلها أو الإفصاح عنها أو فقدانها أو إلحاق الضرر بها أو إتلافها بشكل عرضي أو غير مصرح به أو غير القانوني.[310] وتشير اللائحة العامة لحماية البيانات إلى أن المراقب والمعالج يجب أن يأخذا بعين الاعتبار «آخر المستجدات وتكاليف التنفيذ وطبيعة المعالجة ونطاقها وسياقها والغرض منها، فضلاً عن خطر تفاوت الاحتمالية والخطورة فيما يتعلق بحقوق الأشخاص الطبيعيين وحرياتهم»، أثناء تفعيل هذه التدابير.[311] وحسب الظروف الخاصة بكل حالة، قد تشمل التدابير التقنية والتنظيمية على سبيل المثال استخدام أسماء مستعارة، أو تشفير البيانات الشخصية و/أو الاختبار والتقييم المنتظمين للتدابير لضمان أمن معالجة البيانات.[312]

وكما تم شرحه في الجزء 1.1.2، يقصد باستعمال الأسماء المستعارة تبديل الأوصاف في البيانات الشخصية - التي تسمح بتحديد صاحب البيانات - باسم مستعار والإبقاء على هذه الأوصاف منفصلة، بمقتضى التدابير التقنية أو التنظيمية. ويجب عدم الخلط بين عملية استخدام الأسماء المستعارة وعملية إخفاء مصدر البيانات، حيث يتم قطع جميع الروابط التي تؤدي إلى تحديد هوية الشخص.

مثال: يمكن استخدام أسماء مستعارة في جملة «شارلز سبنسر، مواليد 3 أبريل 1967، رب أسرة من أربعة أطفال، صبيان وبنتان» على النحو التالي:
«ش. س. 1967 رب أسرة من أربعة أطفال، صبيان وبنتان»، أو
«324 رب أسرة من أربعة أطفال، صبيان وبنتان»، أو
«YESz320l رب أسرة من أربعة أطفال، صبيان وبنتان».

عادةً لن يكون باستطاعة المستخدمين الذين يصلون إلى البيانات ذات الأسماء المستعارة القدرة على تحديد هوية « شارلز سبنسر، مواليد 3 أبريل 1967» من خلال «324» أو «YESz3201» لذلك، من المرجح أن تكون هذه البيانات في مأمن من سوء الاستخدام.
غير أن المثال الأول يعد أقل أمناً. إذا كانت الجملة «ش. س. 1967 رب أسرة تتكون من أربعة أطفال، صبيان وبنتان»، تستخدم داخل القرية الصغيرة التي يعيش فيها تشارلز سبنسر، قد يكون من السهل التعرف عليه. ويمكن أن تؤثر طريقة استخدام الاسم المستعار على فعالية حماية البيانات.

تُستخدم البيانات الشخصية ذات الأوصاف المشفرة أو المحفوظة بشكل منفصل في العديد من السياقات كوسيلة للحفاظ على سرية الهويات الشخصية. ويعد هذا الأمر مفيداً بشكل خاص حين يكون مراقبو البيانات في حاجة إلى التأكد من أنهم يتعاملون مع نفس أصحاب البيانات ولكنه ليس من الضروري أو لا ينبغي أن يحصلوا على الهويات الحقيقية لأصحاب البيانات. هذا هو الحال، على سبيل المثال، عندما يدرس الباحث تطور المرض لدى المرضى، الذين لا تكون هويتهم معروفة إلا للمستشفى الذي يعالجون فيه والذي يحصل الباحث منه على سجلات الحالات بأسماء مستعار. وبالتالي، فإن استخدام الأسماء المستعارة هو حلقة وصل قوية في ترسانة تكنولوجيا تعزيز الخصوصية. ويمكن أن يعمل كعنصر مهم أثناء تفعيل الخصوصية منذ التصميم، أي تضمين حماية البيانات في نسيج أنظمة معالجة البيانات.

وتشير المادة 25 من اللائحة العامة لحماية البيانات، التي تعنى بحماية البيانات منذ التصميم ، صراحة إلى استخدام الأسماء المستعارة كمثال لتدبير تقني وتنظيمي ملائم يتعين على المراقبين اتباعه تفعيلاً لمبادئ حماية البيانات وإدماجاً للضمانات الضرورية. ومن خلال ذلك، سيستجيب المراقبون لمتطلبات اللائحة وسيحمون حقوق أصحاب البيانات أثناء معالجة بياناتهم.

يمكن أن يساعد الالتزام بمدونة سلوك معتمدة أو بآلية إصدار شهادات تصديق معتمدة في إثبات الامتثال لمتطلبات أمن المعالجة.[313] وفي رأي حول آثار حماية البيانات على معالجة سجلات أسماء الركاب، قدم مجلس أوروبا أمثلة أخرى على التدابير الأمنية المناسبة لحماية البيانات الشخصية في أنظمة تسجيل أسماء الركاب، وتشمل الاحتفاظ بالبيانات في بيئة مادية آمنة، وتقييد التحكم في الوصول بواسطة عمليات تسجيل الدخول ذات الطبقات وحماية ارسال البيانات بترميز قوي.[314]

[310] اللائحة العامة لحماية البيانات، الحيثية39 والمادة 5 (1) (و)؛ الاتفاقية 108 المحدثة، المادة 7.
[311] اللائحة العامة لحماية البيانات، المادة 32 (1)
[312] نفس المرجع السابق.
[313] نفس المرجع السابق، المادة 32 (3).
[314] مجلس أوروبا، لجنة الاتفاقية 108، رأي حول آثار حماية البيانات الشخصية على معالجة سجلات أسماء الركاب، 19 rev،18(2016)T-PD أغسطس 2016، ص. 9

مثال: تتيح مواقع الشبكات الاجتماعية ومقدمو خدمات البريد الإلكتروني للمستخدمين إمكانية إضافة طبقة إضافية من أمن البيانات إلى الخدمات التي يقدمونها من خلال تقديم المصادقة الثنائية. بالإضافة إلى إدخال كلمة مرور شخصية، يجب على المستخدمين إتمام تسجيل دخول ثانٍ للولوج لحساباتهم الشخصية. يمكن أن يكون هذا الأخير، على سبيل المثال، إدخال رمز أمني يتم إرساله إلى رقم الهاتف المحمول المتصل بالحساب الشخصي. وبهذه الطريقة، يوفر التحقق المكون من خطوتين حماية أفضل للمعلومات الشخصية ضد الوصول غير المصرح به إلى الحسابات الشخصية عبر القرصنة.

يقدم التقرير التفسيري للاتفاقية 108 المحدثة أمثلة إضافية للضمانات المناسبة، مثل تفعيل التزام السرية المهنية، أو اعتماد تدابير أمنية تقنية مؤهلة مثل تشفير البيانات.[315] أثناء وضع تدابير أمنية محددة، يجب أن يأخذ المراقب - أو، عند الاقتضاء، المعالج - بعين الاعتبار العديد من العناصر، ، مثل طبيعة وحجم البيانات الشخصية التي تتم معالجتها، والعواقب السلبية المحتملة على أصحاب البيانات، وضرورة تقييد الوصول إلى البيانات.[316] كما يجب مراعاة آخر المستجدات المتعلقة بأمن البيانات و أساليب وتقنيات معالجة البيانات اثناء تنفيذ التدابير الأمينة المناسبة. ويجب أن تكون تكلفة هذه التدابير متناسبة مع خطورة وإمكانية وقوع المخاطر المحتملة. ومن الضروري إجراء مراجعة منتظمة للإجراءات الأمنية حتى يتم تحديثها حسب الضرورة.[317]

في الحالات التي يحدث فيها خرق للبيانات الشخصية، تُلزم كل من الاتفاقية 108 المحدثة واللائحة العامة لحماية البيانات المراقب بإشعار الهيئة الإشرافية المختصة دون أي تأخير غير مبرر بوقوع ذلك الخرق وما يحمله من مخاطر قد تمس بحقوق الأفراد وحرياتهم.[318] كما يوجد التزام مماثل يتمثل في إشعار صاحب البيانات في حال كان خرق البيانات الشخصية قد يؤدي إلى مخاطر كبيرة على حقوقه وحرياته.[319] يجب أن يكون إشعار أصحاب البيانات بهذه الخروقات عن طريق لغة واضحة وصريحة.[320] وإذا علم المعالج بحدوث خرق للبيانات الشخصية، فيجب أن يخطر المراقب على الفور.[321] وفي حالات معينة، قد يُقيد الالتزام بالإشعار من خلال فرض بعض الاستثناءات. على سبيل المثال، لا يُطلب من المراقب إخطار الهيئة الإشرافية عندما يكون «من غير المحتمل أن يؤدي خرق البيانات الشخصية إلى خطر على حقوق وحريات الأشخاص الطبيعيين».[322] كما أنه ليس من الضروري إشعار صاحب البيانات أثناء تنفيذ التدابير الأمنية التي تجعل البيانات غير مفهومة للأشخاص غير المصرح لهم أو عندما تضمن التدابير اللاحقة أن المخاطر الكبرى لم يعد من المحتمل أن تقع.[323] إذا كان إشعار أصحاب البيانات باختراق شخصي ينطوي على قيام المراقب بجهد غير متناسب، يمكن أن يضمن اتصال عام أو إجراء مشابه «إشعار أصحاب البيانات بطريقة فعالة بنفس القدر».[324]

## 7.3. مبدأ المساءلة

### النقاط الرئيسية

- تقتضي المساءلة من المراقبين والمعالجين تفعيل التدابير بشكل نشط ومستمر لتعزيز و حماية البيانات في أنشطة المعالجة التي يقومون بها.
- يتحمل المراقبون والمعالجون مسؤولية امتثال عمليات المعالجة التي يقومون بها لقانون حماية البيانات والالتزامات الخاصة بكل واحد منهم.
- يجب على المراقبين أن يكونوا قادرين من إثبات الامتثال لمقتضيات حماية البيانات لأصحاب البيانات والعموم والهيئات الإشرافية في أي وقت. أما المعالجون، فيجب أن يمتثلوا لبعض الالتزامات المتعلقة بالمساءلة بشكل صارم (كالاحتفاظ بسجل عمليات المعالجة وتعيين مسؤول عن حماية البيانات).

تبين اللائحة العامة لحماية البيانات والاتفاقية 108 المحدثة أن المراقب مسؤول عن الامتثال لمبادئ معالجة البيانات الشخصية الواردة في هذا الفصل، ويجب عليه إثبات هذا الامتثال.[325] ولتحقيق هذه الغاية، يتعين على المراقب تنفيذ التدابير التقنية والتنظيمية الملائمة.[326] وبالرغم من أن مبدأ المساءلة الوارد في المادة 5 (2) من اللائحة العامة لحماية البيانات موجه فقط للمراقبين، فإنه من المتوقع كذلك مساءلة المعالجين، بالنظر إلى أنهم ملزمون بالامتثال لعدد من الالتزامات ولأنهم مرتبطون بشكل وثيق بالمساءلة.

[315] التقرير التفسيري للاتفاقية 108المحدثة، الفقرة 56.
[316] نفس المرجع السابق، الفقرة 62.
[317] نفس المرجع السابق، الفقرة 62.
[318] نفس المرجع السابق، الفقرة 63.
[319] الاتفاقية 108 المحدثة، المادة 7 (2)؛ اللائحة العامة لحماية البيانات، المادة 33 (1).
[320] اللائحة العامة لحماية البيانات، المادة 34 (2).
[321] نفس المرجع السابق، المادة 33 (1).
[322] نفس المرجع السابق.
[323] نفس المرجع السابق، المادة 34 (3) (أ) و(ب).
[324] نفس المرجع السابق، المادة 34 (3) (ج).
[325] نفس المرجع السابق، المادة 5 (2)؛ الاتفاقية 108 المحدثة، المادة 10 (1).
[326] اللائحة العامة لحماية البيانات، المادة 24.

تشير قوانين حماية البيانات الخاصة بالاتحاد الأوروبي ومجلس أوروبا كذلك إلى أن المراقب مسؤول عن الامتثال لمبادئ حماية البيانات الواردة في الجزأين 1.3 و6.3، [327] كما يجب أن يكون بمقدوره أن يضمن هذا الامتثال. ويشير فريق عمل المادة 29 إلى أن «نوع الإجراءات والآليات ستختلف باختلاف المخاطر التي تمثلها المعالجة ونوع البيانات».[328]

يمكن للمراقبين تسهيل الامتثال لهذا المطلب بطرق مختلفة، بما في ذلك:

- تسجيل أنشطة المعالجة وإتاحتها للهيئة الإشرافية عند الطلب؛[329]
- في حالات معينة، تعيين مسؤول عن حماية البيانات الذي يشارك في جميع الأمور المتعلقة بحماية البيانات الشخصية؛[330]
- إجراء تقييمات أثر حماية البيانات خاصة بأنواع المعالجة التي يحتمل أن تؤدي إلى مخاطر كبرى قد تمس بحقوق الأشخاص الطبيعيين وحرياتهم؛[331]
- ضمان حماية البيانات منذ التصميم وتلقائياً؛[332]
- تفعيل كيفيات وإجراءات خاصة لممارسة حقوق أصحاب البيانات؛[333]
- التقيد بمدونات قواعد السلوك المعتمدة أو بآليات شهادات التصديق.[334]

في حين أن مبدأ المساءلة في المادة 5 (2) من اللائحة العامة لحماية البيانات ليس موجهاً بشكل خاص إلى المعالجين، إلا أن هناك مقتضيات تخص المساءلة تضع أيضاً التزامات تعنيهم، مثل الاحتفاظ بسجل أنشطة المعالجة وتعيين مسؤول حماية بيانات خاص بأي أنشطة معالجة تتطلب هذا التعيين.[335] كما يجب على المعالجين التأكد من تنفيذ جميع التدابير اللازمة لضمان أمن البيانات.[336] ويجب أن ينص العقد الملزم قانوناً بين المراقب والمعالج على وجوب مساعدة المعالج للمراقب في تحقيق بعض متطلبات الامتثال، مثلاً عند إجراء تقييم أثر حماية البيانات أو إشعار المراقب بأي خرق للبيانات الشخصية بمجرد علمه به.[337]

اعتمدت منظمة التعاون الاقتصادي والتنمية مبادئ توجيهية بشأن الخصوصية في 2013 شددت على أن المراقبين لديهم دور مهم في نجاح حماية البيانات من الناحية العملية. وتشمل المبادئ التوجيهية مبدأ المساءلة حيث إن «مراقب البيانات مُعرض للمساءلة في شأن الامتثال للتدابير التي تعطي المبادئ [المادية] المشار إليها مفعولها.»[338]

مثال: يعد تعديل 2009 [339] للأمر التوجيهي بشأن الخصوصية الإلكترونية رقم EC/2002/58 خير مثال تشريعي على التشديد على مبدأ المساءلة. ووفقاً للمادة 4 في صيغتها المعدلة، يفرض الأمر التوجيهي التزاماً من أجل «ضمان تفعيل سياسة أمنية بخصوص معالجة البيانات الشخصية.» لذلك، فحسب المقتضيات الأمنية لهذا الأمر التوجيهي، قرر المشرع أنه من الضروري إدراج مُتَطَلَّب صريح بخصوص وضع سياسة أمنية وتفعيلها.

وفقاً لرأي فريق عامل المادة 29، [340] يتجلى جوهر المساءلة في التزام المراقب بـ:

- وضع تدابير ستضمن - في ظل الظروف العادية - الامتثال لقواعد حماية البيانات في سياق عمليات المعالجة؛
- إعداد الوثائق اللازمة التي تبين لأصحاب البيانات وللهيئات الإشرافية التدابير المتخذة للامتثال لقواعد حماية البيانات.

وعليه، يقتضي مبدأ المساءلة من المراقبين المبادرة بالبرهنة على الامتثال وليس الاكتفاء بانتظار ورود إشارات من جانب أصحاب البيانات أو الهيئات الإشرافية إلى أوجه قصور معينة.

[327] نفس المرجع السابق، المادة 5 (2)؛ الاتفاقية 108 المحدثة، المادة 10 (1).
[328] فريق عمل المادة 29، الرأي رقم 2010/3 بشأن مبدأ المساءلة، WP 173، بروكسل، 13 يوليو 2010، الفقرة 12.
[329] اللائحة العامة لحماية البيانات، المادة 30.
[330] نفس المرجع السابق، المواد 39-37.
[331] نفس المرجع السابق، المادة 35؛ الاتفاقية 108 المحدثة، المادة 10 (2).
[332] اللائحة العامة لحماية البيانات، المادة 25؛ الاتفاقية 108 المحدثة، المادة 10 (2) و(3).
[333] نفس المرجع السابق، المادتان 12 و24.
[334] نفس المرجع السابق، المادتان 40 و42.
[335] نفس المرجع السابق، المواد 5 (2)، 30 و37.
[336] نفس المرجع السابق، المادة 28 (3) ج.
[337] نفس المرجع السابق، المادة 28 (3) د.
[338] منظمة التعاون الاقتصادي والتنمية (2013)، المبادئ التوجيهية بشأن حماية الخصوصية وتدفقات البيانات الشخصية عبر الحدود، المادة 14.
[339] الأمر التوجيهي رقم EC/2009/136 الصادر عن البرلمان الأوروبي والمجلس بتاريخ 25 نوفمبر 2009 المعدل للأمر التوجيهي EC/2002/22 بشأن الخدمة الشاملة وحقوق المستخدمين المتعلقة بشبكات وخدمات الاتصالات الإلكترونية؛ الأمر التوجيهي EC/2002/58 بشأن معالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الإلكترونية؛ لائحة (المفوضية الأوروبية) رقم 2006/2004 بشأن التعاون بين الهيئات الوطنية المسؤولة عن إنفاذ قوانين حماية المستهلك، الجريدة الرسمية 337 L 2009 OJ، ص. 11.
[340] فريق عمل المادة 29، الرأي رقم 3/2010 حول مبدأ المساءلة، WP 173، بروكسل، 13 يوليو 2010.

# 4

# قواعـــد قانـــون حمايـــة البيانـــات الأوروبـــي

| الاتحاد الأوروبي | المسائل المتناولة | مجلس أوروبا |
|---|---|---|
| **قواعد بشأن المعالجة القانونية للبيانات** | | |
| اللائحة العامة لحماية البيانات، المادة 6 (1) (أ)<br>محكمة العدل التابعة للاتحاد الأوروبي، رقم C-543/09، شركة «دويتشه تيليكوم» ضد جمهورية ألمانيا الاتحادية، 2011<br>محكمة العدل التابعة للاتحاد الأوروبي، رقم C-536/15، شركة «تيلي 2» (هولندا) وآخرون ضد هيئة المستهلكين والأسواق، 2017 | الموافقة | توصية حول التنميط، المادتان 4.3 (ب) و6.3<br>الاتفاقية 108 المحدثة، المادة 5 (2) |
| اللائحة العامة لحماية البيانات، المادة 6 (1) (ب) | العلاقة (ما قبل) التعاقدية | توصية حول التنميط، المادة 4.3 (ب) |
| اللائحة العامة لحماية البيانات، المادة 6 (1) (ج) | الواجبات القانونية للمراقب | توصية حول التنميط، المادة 4.3 (أ) |
| اللائحة العامة لحماية البيانات، المادة 6 (1) (د) | المصالح الحيوية لصاحب البيانات | توصية حول التنميط، المادة 4.3 (ب) |
| اللائحة العامة لحماية البيانات، المادة 6 (1) (ه)<br>محكمة العدل التابعة للاتحاد الأوروبي، رقم C-524/06، هوبر ضد جمهورية ألمانيا الاتحادية [الغرفة الكبرى]، 2008 | المصلحة العامة وممارسة السلطة الرسمية | توصية حول التنميط، المادة 4.3 (ب) |

| | | |
|---|---|---|
| اللائحة العامة لحماية البيانات، المادة 6 (1) (و)<br>محكمة العدل التابعة للاتحاد الأوروبي، رقم C-13/16، إدارة الشرطة الإقليمية في ريغا ضد شركة «ريغاس ساتيكسمي» للنقل التابعة لبلدية ريغا، 2017<br>محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-468/10 وC-469/10، الرابطة الوطنية لمؤسسات الائتمان المالي (ASNEF) واتحاد التجارة الإلكترونية والتسويق المباشر (FECEMD) ضد إدارة الدولة | المصالح المشروعة للآخرين | توصية حول التنميط، المادة 4.3 (ب)<br>المحكمة الأوروبية لحقوق الإنسان، ي. ضد تركيا، رقم 648/10، 2015 |
| اللائحة العامة لحماية البيانات، المادة 6 (4) | استثناء بشأن حصر الغرض: معالجة إضافية لأغراض أخرى | الاتفاقية 108 المحدثة، المادة 5 (4) (ب) |
| قواعد بشأن المعالجة القانونية للبيانات الحساسة | | |
| اللائحة العامة لحماية البيانات، المادة 9 (1) | الحظر العام للمعالجة | الاتفاقية 108 المحدثة، المادة 6 |
| اللائحة العامة لحماية البيانات، المادة 9 (2) | الاعفاءات من الحظر العام | الاتفاقية 108 المحدثة، المادة 6 |
| **قواعد بشأن المعالجة الآمنة** | | |
| اللائحة العامة لحماية البيانات، المادة 32 | الالتزام بضمان المعالجة الآمنة | الاتفاقية 108 المحدثة، المادة 7 (1)<br>المحكمة الأوروبية لحقوق الانسان، إ. ضد فنلندا، رقم 20511/03، 2008 |
| اللائحة العامة لحماية البيانات، المادتان 28 و32 (1) (ب) | الالتزام بالسرية | الاتفاقية 108 المحدثة، المادة 7 (1) |
| اللائحة العامة لحماية البيانات، المادة 34<br>الأمر التوجيهي بشأن الخصوصية والاتصالات الالكترونية، المادة 4 (2) | إشعارات خرق البيانات | الاتفاقية 108 المحدثة، المادة 7 (2) |
| **قواعد بشأن المساءلة وتعزيز الامتثال** | | |
| اللائحة العامة لحماية البيانات، المواد 12 و13 و14 | الشفافية بشكل عام | الاتفاقية 108 المحدثة، المادة 8 |
| اللائحة العامة لحماية البيانات، المواد 37 و38 و39 | المسؤولون عن حماية البيانات | الاتفاقية 108 المحدثة، المادة 10 (1) |

| | | |
|---|---|---|
| اللائحة العامة لحماية البيانات، المادة 30 | سجلات أنشطة المعالجة | |
| اللائحة العامة لحماية البيانات، المادتان 35 و36 | تقييم الأثر والاستشارة القبلية | الاتفاقية 108 المحدثة، المادة 10 (2) |
| | | |
| اللائحة العامة لحماية البيانات، المادتان 33 و34<br>اللائحة العامة لحماية البيانات، المادتان 40 و41 | إشعارات خرق البيانات<br>مدونات قواعد السلوك | الاتفاقية 108 المحدثة، المادة 7 (2) |
| اللائحة العامة لحماية البيانات، المادتان 42 و43 | شهادات التصديق | |
| **حماية البيانات منذ التصميم وتلقائياً** | | |
| اللائحة العامة لحماية البيانات، المادة 25 (1) | حماية البيانات منذ التصميم | الاتفاقية 108 المحدثة، المادة 10 (2) |
| اللائحة العامة لحماية البيانات، المادة 25 (2) | حماية البيانات تلقائياً | الاتفاقية 108 المحدثة، المادة 10 (3) |

تظل المبادئ بالضرورة ذات طابع عام، ويترك تطبيقها في حالات محددة هامشاً معيناً من التفسير واختيار الوسائل. وبموجب **قانون مجلس أوروبا**، يُترك لأطراف الاتفاقية 108 المحدثة توضيح هامش التفسير هذا في قانونهم المحلي. ويختلف الوضع في **قانون الاتحاد الأوروبي**: لترسيخ حماية البيانات في السوق الداخلية، كان من الضروري وضع قواعد أكثر تفصيلاً على مستوى الاتحاد الأوروبي لمواءمة مستوى حماية البيانات للقوانين الوطنية للدول الأعضاء. وتحدد اللائحة العامة لحماية البيانات طبقة من القواعد التفصيلية، بموجب المبادئ المنصوص عليها في المادة 5، والتي تنطبق مباشرة على النظام القانوني الوطني. وتتناول الملاحظات التالية حول قواعد حماية البيانات المفصلة على المستوى الأوروبي في الغالب قانون الاتحاد الأوروبي.

## 1.4. قواعد بشأن المعالجة المشروعة

### النقاط الرئيسية

- يمكن لمعالجة البيانات الشخصية أن تتم بصفة مشروعة إذا استوفت أحد المعايير التالية:
  - حين ترتكز المعالجة على موافقة صاحب البيانات؛
  - حين تكون معالجة البيانات الشخصية من متطلبات إبرام علاقة تعاقدية؛
  - حين تكون المعالجة ضرورية للامتثال لالتزام قانوني ملقى على عاتق المراقب؛
  - حين تستدعي المصالح الحيوية لأصحاب البيانات أو لشخص آخر معالجة بياناتهم الشخصية؛
  - حين تكون المعالجة ضرورية لأداء مهمة تصب في المصلحة العامة؛
  - حين تكون المصالح المشروعة للمراقبين أو أطراف أخرى هي الدافع وراء المعالجة، شريطة ألا تبطلها المصالح أو الحقوق الأساسية لأصحاب البيانات.
- تخضع المعالجة المشروعة للبيانات الشخصية الحساسة لنظام خاص وأكثر صرامة.

### 1.1.4. الأسس المشروعة التي تجيز معالجة البيانات

ينص الفصل الثاني من اللائحة العامة لحماية البيانات، الذي يحمل عنوان «المبادئ»، على أن معالجة البيانات الشخصية يجب أن تمتثل أولا للمبادئ المتعلقة بجودة البيانات الواردة في المادة 5 من اللائحة العامة لحماية البيانات. ومن بين هذه المبادئ نجد أن البيانات الشخصية يجب أن «تتم معالجتها بشكل قانوني وعادل وبشفافية». ثانياً، لكي تتم معالجة البيانات بشكل قانوني، يجب أن تمتثل لأحد الأسباب القانونية التي تجعل معالجة البيانات أمراً مشروعاً، والتي ترد في المادة 6 [341] المتعلق بالبيانات الشخصية غير الحساسة، وفي المادة 9 بالنسبة للفئات الخاصة من البيانات (أو البيانات الحساسة). وعلى نحو مماثل، ينص الفصل الثاني من الاتفاقية 108 المحدثة التي تحدد «المبادئ الأساسية لحماية البيانات الشخصية»، على أنه لكي تتسم معالجة البيانات بالصبغة القانونية يتعين أن تكون «متناسبة مع الغرض المشروع المنشود منها».

وبعض النظر عن الأساس القانوني للمعالجة الذي يعتمد عليه المراقب للشروع في عملية معالجة البيانات الشخصية، يبقى دائماً لزاماً على المراقب تطبيق الضمانات المنصوص عليها في نظام اللائحة العامة لحماية البيانات.

**الموافقة**

**بموجب قانون مجلس أوروبا**، تمت الإشارة إلى الموافقة في المادة 5 (2) من الاتفاقية 108 المحدثة. كما يشار إليها في السوابق القضائية للمحكمة الأوروبية لحقوق الإنسان والعديد من توصيات مجلس أوروبا.[342] **وبموجب قانون الاتحاد الأوروبي**، تم تكريس الموافقة كأساس للمعالجة القانونية للبيانات في المادة 6 من اللائحة العامة لحماية البيانات، كما تمت الإشارة إليها صراحةً في المادة 8 من الميثاق. ويوجد شرح لمقومات الموافقة الصالحة في تعريف الموافقة ضمن المادة 4، في حين تُفصل المادة 7 في شروط الحصول على الموافقة الصالحة، فيما تبين المادة 8 من اللائحة العامة لحماية البيانات القواعد الخاصة التي تهم موافقة الطفل فيما يتعلق بخدمات مجتمع المعلومات.

وكما تم شرحه في الجزء 4.2، يجب أن تُعطى الموافقة بحرية، وأن تكون مستنيرة ومحددة وصريحة. ويجب أن تكون الموافقة عبارة عن تصريح أو فعل إيجابي واضح يدل على الموافقة على المعالجة، ويحق للشخص سحبها في أي وقت. ويقع على عاتق المراقبين واجب الاحتفاظ بسجل خاص بالموافقة يمكن التحقق منه.

---

[341] محكمة العدل التابعة للاتحاد الأوروبي، القضايا المضمومة C-465/00 و C-138/01 وC-139/01، «ديوان المحاسبة ضد الإذاعة النمساوية وآخرين» و«كريستا نوكوم وجوزيف لاورمان ضد الإذاعة النمساوية»، 20 مايو 2003، الفقرة 65؛ محكمة العدل التابعة للاتحاد الأوروبي، رقم C-524/06، «هاينز هيوبر ضد جمهورية ألمانيا الاتحادية» [الغرفة الكبرى]، 16 ديسمبر 2008، الفقرة 48؛ محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-468/10 وC-469/10، «الرابطة الوطنية لمؤسسات الائتمان المالي (ASNEF) واتحاد التجارة الإلكترونية والتسويق المباشر(FECEMD) ضد إدارة الدولة»، 24 نوفمبر 2011، الفقرة 26.

[342] انظر على سبيل المثال، مجلس أوروبا، لجنة الوزراء (2010)، توصية لجنة الوزراء (2010)13 للدول الأعضاء حول حماية الأفراد من المعالجة الآلية للبيانات الشخصية في سياق التنميط، 23 نوفمبر 2010، المادة 4.3 (ب).

**الموافقة الحرة**

في إطار عمل **مجلس أوروبا** الخاص بالاتفاقية 108 المحدثة، يجب أن «تمثل [موافقة صاحب البيانات] التعبير الحر عن الاختيار المراد»،[343] ولا تكون الموافقة الحرة صالحة إلا «إذا كان صاحب البيانات قادراً على ممارسة خيار حقيقي ولا تترتب مخاطر تتعلق بالخداع أو التخويف أو الإكراه أو عواقب سلبية كبيرة في حال لم يقدم موافقته». في هذا الصدد، ينص **قانون الاتحاد الأوروبي** على أن الموافقة لا تعتبر حرة «إذا لم يكن لصاحب البيانات خيار حقيقي أو حر أو كان غير قادر على رفض أو سحب الموافقة دون التعرض للضرر».[345] وتشدد اللائحة العامة لحماية البيانات على أنه «عند تقييم ما إذا كانت الموافقة قد منحت بحرية، يجب أن يولى أعلى قدر من الاعتبار، ضمن جملة من الأمور، لما إذا كان أداء العقد، بما في ذلك تقديم الخدمة، رهين بالموافقة على معالجة البيانات الشخصية التي ليست ضرورية لأداء هذا العقد»،[346] وينص التقرير التفسيري للاتفاقية 108 المحدثة على أنه «لا يجوز ممارسة أي تأثير أو ضغط غير مبرر (والذي يمكن أن يكون ذا طابع اقتصادي أو غير ذلك) سواء كان مباشراً أو غير مباشر، على صاحب البيانات ولا ينبغي اعتبار الموافقة على أنها حرة حين لا يكون لصاحب البيانات خيار حقيقي أو حين يكون غير قادر على رفض أو سحب الموافقة بدون ضرر».[347]

مثال: قررت بعض البلديات في الولاية «أ» إعداد بطاقات إقامة بشريحة مدمجة. وليس لازماً على المقيمين الحصول على تلك البطاقات الإلكترونية. ومع ذلك، فإن السكان الذين لا يمتلكون البطاقة لا يمكنهم الوصول إلى مجموعة من الخدمات الإدارية المهمة، مثل القدرة على دفع الضرائب البلدية عبر الإنترنت، وتقديم الشكايات إلكترونياً والتي ترد عليها الهيئة في مدة ثلاثة أيام، وحتى تخطي قوائم الانتظار، وشراء تذاكر منخفضة السعر عند زيارة قاعة الحفلات الموسيقية الخاصة بالبلدية واستخدام الماسحات الضوئية في المدخل.

لا يمكن أن تستند معالجة البلديات للبيانات الشخصية في هذا المثال إلى الموافقة. ونظراً لوجود ضغط غير مباشر على المقيمين للحصول على البطاقة الإلكترونية والموافقة على المعالجة، فإن الموافقة ليست حرة. وبالتالي ينبغي أن يستند وضع البلديات لنظام البطاقات الإلكترونية إلى أساس مشروع آخر يبرر المعالجة. وعلى سبيل المثال، يمكنهم الاحتجاج بأن المعالجة ضرورية لأداء مهمة تصب في المصلحة العامة، والتي تعد أساساً قانونياً للمعالجة وفقاً للمادة 6 (1) (هـ) من اللائحة العامة لحماية البيانات.[348]

يمكن أن تكون الموافقة الحرة أيضاً موضع شك في حالات التبعية، حيث يوجد خلل كبير في التوازن الاقتصادي أو غيره من الاختلال بين المراقب الذي يؤمن الموافقة وصاحب البيانات الذي يقدمها.[349] ولعل خير مثال على هذه الاختلالات والتبعية معالجة صاحب العمل للبيانات الشخصية في سياق علاقة العمل. ووفقاً لفريق عمل المادة 29، «لا يستطيع الموظفون مطلقاً إعطاء الموافقة أو رفضها أو سحبها بحرية، بالنظر إلى التبعية الناتجة عن العلاقة بين صاحب العمل والموظف. ونظراً لاختلال توازن القوى، لا يمكن للموظفين منح الموافقة الحرة إلا في ظروف استثنائية، عندما لا تكون هناك عواقب على الإطلاق مرتبطة بقبول أو رفض عرض ما».[350]

مثال: تخطط شركة كبيرة لإعداد دليل يحتوي على أسماء جميع الموظفين ووظائفهم في الشركة وعناوين عملهم، لغرض واحد يتمثل في تحسين الاتصالات الداخلية للشركة. ويقترح رئيس الموظفين إضافة صورة لكل موظف إلى الدليل لتسهيل التعرف على الزملاء في الاجتماعات، في حين يطالب ممثلو الموظفين بعدم القيام بذلك إلا بعد الحصول على موافقة الموظف.

في مثل هذه الحالة، يجب الإقرار بموافقة الموظف كأساس قانوني لمعالجة الصور في الدليل لأنه من المعقول أن الموظف لن يواجه أي عواقب على الإطلاق، سواء قرر الموافقة على نشر صورته في الدليل أم لا.

---

[343] التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 42.

[344] انظر أيضاً فريق عمل المادة 29 (2011)، الرأي رقم 15/2011 بشأن مفهوم الموافقة، WP 187، بروكسل، 13 يوليو 2011، ص. 12.

[345] اللائحة العامة لحماية البيانات، الحيثية42.

[346] نفس المرجع السابق، المادة 7 (4).

[347] التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 42.

[348] فريق عمل المادة 29، الرأي رقم 15/2011 بشأن تعريف الموافقة، WP 187، بروكسل، 13 يوليو 2011، ص. 16. يمكن إيجاد أمثلة إضافية في الصفحات من 14 إلى 17 من الرأي لحالات لا يمكن أن تقوم فيها معالجة البيانات على الموافقة، لكنها تتطلب أساساً قانونياً مختلفاً لجعل المعالجة مشروعة.

[349] انظر أيضاً فريق عمل المادة 29 (2001)، الرأي رقم 8/2001 بشأن معالجة البيانات الشخصية في سياق التوظيف، WP 48، بروكسل، 13 سبتمبر 2001؛ فريق عمل المادة 29 (2005)، وثيقة عمل حول التفسير المشترك للمادة 26 (1) من الأمر التوجيهي EC/95/46 بتاريخ 24 أكتوبر 1995، WP 114، بروكسل، 25 نوفمبر 2005؛ فريق عمل المادة 29 (2017)، الرأي رقم 2/2017 بشأن معالجة البيانات في العمل، WP 249، بروكسل، 8 يونيو 2017.

[350] فريق عمل المادة 29، الرأي رقم 2/2017 بشأن معالجة البيانات في العمل، WP 249، بروكسل، 8 يونيو 2017.

مثال: تخطط الشركة «أ» لعقد اجتماع بين ثلاثة من موظفيها ومديري الشركة «ب» لمناقشة التعاون المستقبلي المحتمل في أحد المشاريع. وسيعقد الاجتماع في مقر الشركة «ب»، التي تطلب من الشركة «أ» إرسال أسماء المشاركين في الاجتماع وسيرهم الذاتية وصورهم بالبريد الإلكتروني. وترى الشركة «ب» بأنها تحتاج إلى أسماء وصور المشاركين للسماح لموظفي الأمن بالتحقق من أنهم الأشخاص المناسبون عند مدخل المبنى، في حين أن السير الذاتية ستمكن المديرين من الاستعداد بشكل أفضل للاجتماع. في هذه الحالة، لا يمكن أن يستند نقل الشركة «أ» للبيانات الشخصية لموظفيها إلى الموافقة. ولا يمكن اعتبار الموافقة على أنها «ممنوحة بحرية»، لأنه من الممكن أن يواجه الموظفون عواقب سلبية إذا رفضوا العرض (على سبيل المثال، قد يتم استبدالهم بزملاء آخرين ليس فقط فيما يتعلق بحضور الاجتماع، ولكن أيضا فيما يخص الاتصال بالشركة «ب» والمساهمة في المشروع بشكل عام). لذلك، يجب أن تستند المعالجة إلى أساس قانوني آخر للمعالجة.

ومع ذلك، هذا لا يعني أن الموافقة لا يمكن أن تكون صالحة أبداً في الظروف التي قد يترتب فيها عن عدم الموافقة بعض الآثار السلبية. على سبيل المثال، إذا لم ينتج عن عدم الموافقة على الحصول على بطاقة عميل سوق كبرى سوى عدم تلقي تخفيض طفيف في سعر سلع معينة، فقد تكون الموافقة أساساً قانونياً صالحاً لمعالجة البيانات الشخصية للعملاء الذين وافقوا على الحصول على هذه البطاقة. فلا يوجد تبعية بين الشركة والعميل وعواقب عدم الموافقة ليست خطيرة بما يكفي لمنع الاختيار الحر لصاحب البيانات (بشرط أن يكون تخفيض السعر طفيفاً بما يكفي لعدم التأثير على اختياره الحر).

غير أنه في حال تعذر الحصول على السلع أو الخدمات إلا إذا تم الكشف عن بعض البيانات الشخصية لمراقب البيانات أو لأطراف أخرى بعد ذلك، فإن موافقة صاحب البيانات على الكشف عن بياناته، والتي لا تعد ضرورية بالنسبة للعقد، لا يمكن اعتبارها قراراً حراً ولذلك فهي غير صالحة بموجب قانون حماية البيانات.[351] وتعد اللائحة العامة لحماية البيانات صارمة إلى حد ما فيما يتعلق بحظر ربط الموافقة بتوفير السلع والخدمات،[352]

مثال: لا يمكن اعتبار اتفاق الركاب مع شركة طيران ترسل ما يسمى بسجلات أسماء الركاب (أي بيانات عن هوياتهم أو عاداتهم الغذائية أو مشاكلهم الصحية) إلى سلطات الهجرة في بلد أجنبي معين موافقة صالحة بموجب قانون حماية البيانات، حيث لا خيار أمام المسافرين إذا كانوا يرغبون في زيارة هذا البلد. إذا كان سيتم إرسال هذه البيانات بشكل قانوني، فمن الضروري وجود أساس قانوني آخر غير الموافقة، وعلى الأرجح قانون محدد.

**الموافقة المستنيرة**

يجب أن يكون لدى صاحب البيانات معلومات كافية قبل القيام باختياره. عادةً ما تشمل الموافقة المستنيرة وصفاً دقيقاً وسهل الفهم للموضوع الذي يتطلب الموافقة. كما يوضح فريق عمل المادة 29، فإن الموافقة يجب أن تستند على تقدير وفهم للحقائق والآثار المترتبة على إعطاء صاحب البيانات للموافقة على المعالجة. لذلك، «يجب أن يحصل الفرد المعني، بطريقة واضحة ومفهومة، على معلومات دقيقة وكاملة عن جميع الأمور ذات الصلة [...] مثل طبيعة البيانات المعالجة، وأغراض المعالجة، والجهات المتلقية المحتملة وحقوق صاحب البيانات».[353] ولكي تكون الموافقة مستنيرة، يجب أن يكون الأفراد أيضاً على دراية بعواقب عدم الموافقة على المعالجة.

ونظراً لمدى أهمية الموافقة المستنيرة، فإن كُلاً من اللائحة العامة لحماية البيانات والتقرير التفسيري للاتفاقية 108 المحدثة قد سعيا لتوضيح مفهومها، حيث تنص حيثيات اللائحة العامة لحماية البيانات على أن الموافقة المستنيرة تعني أن «صاحب البيانات يجب أن يدرك على الأقل هوية المراقب والأغراض [المنشودة] من معالجة البيانات الشخصية».[354]

في الحالة الاستثنائية التي يُلجأ فيها لموافقة صاحب البيانات على أنها الأساس القانوني لنقل البيانات عبر الحدود الدولية، يتعين على المراقب - وهذا شرط لكي تعتبر الموافقة صالحة - إبلاغ صاحب البيانات بالمخاطر المحتملة التي تكتنف عملية النقل هذه في ظل غياب قرار بشأن مدى كفاية الضمانات المرتبطة بحماية البيانات وغياب الاحتياطات المناسبة.[355]

---

[351] اللائحة العامة لحماية البيانات، المادة 7 (4).

[352] نفس المرجع السابق.

[353] فريق عمل المادة 29 (2017)، وثيقة العمل بشأن معالجة البيانات الشخصية المتعلقة بالصحة في السجلات الصحية الإلكترونية، WP 131، بروكسل، 15 فبراير 2007.

[354] اللائحة العامة لحماية البيانات، ديباجة القرار 42.

[355] نفس المرجع السابق، المادة 49 (1) (أ).

يؤكد التقرير التفسيري للاتفاقية 108 المحدثة على وجوب تقديم المعلومات المرتبطة بالآثار التي يمكن أن تترتب عن قرار صاحب البيانات، أي «ما يترتب عن فعل الموافقة والنطاق المشمول بالموافقة».[356]

تعد جودة المعلومات أمراً مهماً، ويقصد بها أن لغة المعلومات يجب أن تكون متكيفة مع الجهات المتلقية المتوقعة. كما يجب أن تكون المعلومات خالية من المصطلحات التقنية وتكون بلغة واضحة وبسيطة يكون بمقدور المستخدم العادي أن يفهمها.[357] هذا ويجب أن تتاح المعلومات بسهولة لصاحب البيانات ويمكن تقديمها شفهياً أو كتابة. وتعد إمكانية الوصول إلى المعلومات وإمكانية رؤيتها من العناصر المهمة: يجب أن تكون المعلومات واضحة وبارزة. أما في سياق الإنترنت، فقد تكون إشعارات المعلومات ذات الطبقات حلاً جيداً، لأنها تسمح لأصحاب البيانات باختيار ما إذا كانوا يريدون الوصول إلى نسخ موجزة أو أكثر تفصيلاً من المعلومات.

**الموافقة المحددة**

من أجل أن تكون الموافقة صالحة، يجب أن تكون محددة في إطار غرض المعالجة، الذي يجب أن يحدد بوضوح وبمصطلحات صريحة. ويتماشى هذا الأمر جنباً إلى جنب مع جودة المعلومات المتعلقة بالغرض من الموافقة. وفي هذا السياق، ستكون التوقعات المعقولة لصاحب بيانات عادٍ ذات موضوعية. ويجب طلب موافقة صاحب البيانات مجدداً إذا كانت سيتم القيام بعمليات معالجة إضافية أو تغييرها بطريقة لم تكن متوقعة بصورة معقولة عند تقديم الموافقة الأولية، وبذلك أدت إلى تغيير الغرض. وعندما تكون للمعالجة أغراض متعددة، يتعين إعطاء الموافقة عليها جميعاً.[358]

أمثلة: في قضية شركة «دوتشيه تيليكوم»،[359] نظرت محكمة العدل التابعة للاتحاد الأوروبي فيما إذا كان يتوجب على مقدم خدمة اتصالات ملزمٍ بتقديم البيانات الشخصية الخاصة بمشتركيه لغرض نشرها في دلائل الأرقام أن يحصل على الموافقة مجدداً من أصحاب البيانات،[360] بحكم أن الجهات المتلقية للبيانات لم تكن مُعرَّفة بالاسم وقت تقديم الموافقة.

ترى محكمة العدل أنه بموجب المادة 12 من الأمر التوجيهي بشأن الخصوصية والاتصالات الإلكترونية، لم يكن من الضروري تجديد الموافقة قبل تقديم البيانات. وبما أن أصحاب البيانات لم يملكوا سوى خيار الموافقة على غرض المعالجة - الذي يتجلى في نشر بياناتهم - فإنهم لم يتمكنوا من الاختيار من بين الدلائل المختلفة التي قد يتم نشر هذه البيانات فيها.

كما أكدت محكمة العدل بأنه «يظهر من تفسير سياقي ومنهجي للمادة 12 من الأمر التوجيهي بشأن الخصوصية والاتصالات الإلكترونية أن الموافقة بموجب المادة 12 (2) تتعلق بالغرض من نشر البيانات الشخصية في دليل عام وليس بهوية أي مزود دليل معين».[361] بالإضافة إلى ذلك، «إن نشر البيانات الشخصية في دليل عام لغرض محدد هو ما قد يكون مضراً بالمشترك»،[362] وليس هوية الناشر.

تعلقت قضية «تيلي 2 هولندا المحدودة' و'زيجو المحدودة' و'فودافون لبيبرتل المحدودة' ضد هيئة المستهلكين والأسواق (AMC)» بطلب شركة بلجيكية بأن يوفر لها مقدمو خدمات الاستفسار والأدلة للشركات التي تخصص أرقام الهواتف في هولندا لها إمكانية الوصول إلى البيانات المتعلقة بمشتركيها. واعتمدت الشركة البلجيكية في طلبها هذا على التزام بموجب الأمر التوجيهي المتعلق بالخدمات الشاملة.[364] يقتضي هذا الأخير من الشركات التي تخصص أرقام الهواتف أن تجعل الأرقام متاحة للأدلة التي تطلبها، إذا وافق المشتركون على أن يتم نشر أرقامهم. إلا أن الشركات الهولندية رفضت القيام بذلك، مشيرة إلى أنها غير مطالَبة بتقديم البيانات المعنية إلى مقاولة منشأة في دولة عضو أخرى. وقد جادلت الشركات الهولندية بأن المستخدمين وافقوا على نشر أرقامهم على أساس أنه سيتم نشرها في دليل هولندي. واعتبرت محكمة العدل التابعة للاتحاد الأوروبي أن الأمر التوجيهي المتعلق بالخدمات الشاملة يغطي

[356] التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 42.

[357] فريق عمل المادة 29 (2011)، الرأي رقم 15/2011 بشأن تعريف الموافقة، WP 187، بروكسل، 13 يوليو 2011، ص. 19.

[358] اللائحة العام لحماية البيانات، الحيثية32.

[359] محكمة العدل التابعة للاتحاد الأوروبي، رقم C-543/09، شركة «دوتشيه تيليكوم» ضد جمهورية ألمانيا الاتحادية، 5 مايو 2011، انظر الفقرتان 53 و54 على وجه الخصوص.

[360] الأمر التوجيهي رقم EC/2002/58 الصادر عن البرلمان الأوروبي والمجلس بتاريخ 12 يوليو 2002 بخصوص معالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الإلكترونية، الجريدة الرسمية 201 L 2002 0J، (الأمر التوجيهي بشأن الخصوصية والاتصالات الإلكترونية).

[361] محكمة العدل التابعة للاتحاد الأوروبي، رقم C-543/09، شركة «دوتشيه تيليكوم» ضد جمهورية ألمانيا الاتحادية، 5 مايو 2011؛ الفقرة 61.

[362] نفس المرجع السابق، الفقرة 62.

[363] محكمة العدل التابعة للاتحاد الأوروبي، C-536/15، قضية «تيلي 2 هولندا المحدودة 'وآخرون ضد هيئة المستهلكين والأسواق (AMC)»، 15 مارس 2017.

[364] الأمر التوجيهي EC/2002/22 للبرلمان الأوروبي والمجلس المؤرخ في 7 مارس 2002 المتعلق بحقوق مستخدمي الخدمات الشاملة المتعلقة بشبكات وخدمات الاتصالات الإلكترونية (الأمر التوجيهي المتعلق بالخدمات الشاملة)، الجريدة الرسميةOJ 20020 108 L ، ص. 51، كما تم تعديله بالأمر التوجيهي EC /2009/136 للبرلمان الأوروبي والمجلس المؤرخ في 25 نوفمبر 2009 (الأمر التوجيهي المتعلق بالخدمات الشاملة)، الجريدة الرسمية OJ 3372009 L، ص. 11.

جميع الطلبات المقدمة من المقاولات التي تقدم خدمات الدليل، بغض النظر عن الدولة العضو التي أُنشِأت فيها. كما اعتبرت محكمة العدل التابعة للاتحاد الأوروبي أن تمرير نفس البيانات إلى مقاولة أخرى، تعتزم نشر دليل عام دون الحصول على موافقة مجدداً من المشتركين، لا يمكن أن يخل بشكل جوهري بالحق في حماية البيانات الشخصية.[365] وبالتالي، ليس من الضروري للمقاولة التي تقوم بتخصيص أرقام الهواتف لمشتركيها أن تميِّز في طلب الموافقة الموجه إلى المشترك بناءً على الدولة العضو التي يمكن إرسال البيانات المتعلقة به إليها.[366]

**الموافقة الصريحة (التي لا لبس فيها)**

يجب أن تُعطى كل موافقة بطريقة جلية ولا لبس فيها.[367] وهذا يعني أنه لا ينبغي أن يكون هناك شك معقول في أن صاحب البيانات أراد التعبير عن موافقته على السماح بمعالجة بياناته. فمثلاً، لا يشير عدم قيام صاحب البيانات بشيء إلى موافقته الجلية.

وهذا هو الحال بالنسبة للمراقب الذي يحصل على الموافقة بواسطة التصريحات (statements) الواردة في سياسات الخصوصية الخاصة به، مثل: «باستخدام خدمتنا، فإنك توافق على معالجة بياناتك الشخصية». ففي هذه الحالة، قد يتعين على المراقب التأكد من موافقة المستخدم يدوياً وبشكل فردي على هذه السياسات.

وإذا تم منح الموافقة في صيغة كتابية تشكل جزءاً من عقد، فيجب أن تكون الموافقة على معالجة البيانات الشخصية موافقة منفردة، وفي كل الأحوال، «ينبغي أن تكفل الضمانات إدراك صاحب البيانات لفعل الموافقة [...] والنطاق المشمول بالموافقة.»[368]

**متطلبات الموافقة الخاصة بالأطفال**

توفر اللائحة العامة لحماية البيانات حماية خاصة للأطفال في سياق تقديم خدمات مجتمع المعلومات، لأنهم «قد يكونون أقل وعياً بالمخاطر والعواقب والضمانات ذات الصلة وبحقوقهم المرتبطة بمعالجة البيانات الشخصية».[369] لذلك، **بموجب قانون الاتحاد الأوروبي**، عندما يعالج مقدمو خدمات مجتمع المعلومات البيانات الشخصية للأطفال الذين تقل أعمارهم عن 16 عاماً على أساس الموافقة، فإن هذه المعالجة تكون قانونية «فقط إذا، وإلى الحد الذي يتم فيه، منح الموافقة أو الإذن بها من قبل صاحب المسؤولية الأبوية على الطفل».[370] ويجوز للدول الأعضاء أن تنص على سن أقل في قانونها الوطني، شريطة ألّا يقل عن 13 سنة.[371] ولا تكون موافقة صاحب المسؤولية الأبوية ضرورية «في سياق الخدمات الوقائية أو الاستشارية المقدمة مباشرة إلى الطفل».[372] ويجب أن تكون المعلومات والتواصل بشأن المعالجة التي تعني الأطفال بلغة واضحة وبسيطة يسهل على الطفل فهمها.[373]

**الحق في سحب الموافقة في أي وقت**

يتضمن القانون العام لحماية البيانات حقاً عاماً في سحب الموافقة في أي وقت.[374] يجب إبلاغ صاحب البيانات بهذا الحق قبل أن يمنح موافقته ويمكنه ممارسة هذا الحق حسب تقديره. ويجب ألا يكون هناك شرط لإبداء أسباب سحب الموافقة و ألا تكون هناك مخاطر من العواقب السلبية فيما عدا إنهاء أي فوائد قد تكون مستمدة من استخدام البيانات المتفق عليه مسبقاً. يجب أن يكون سحب الموافقة بنفس قدر سهولة إعطائها.[375] ولا يمكن أن تكون هناك موافقة حرة إذا كان صاحب البيانات غير قادر على سحب موافقته دون ضرر أو إذا لم يكن سحب الموافقة سهلاً كما كان إعطاؤها.[376]

---

[365] محكمة العدل التابعة للاتحاد الأوروبي، C-536/15، قضية «"تيلي 2 هولندا المحدودة 'وآخرون ضد هيئة المستهلكين والأسواق (AMC)»، 15 مارس 2017، الفقرة 36.
[366] نفس المرجع السابق، الفقرتان 41-40.
[367] اللائحة العامة لحماية البيانات، المادة 4 (11).
[368] نفس المرجع السابق، الحيثية 42.
[369] نفس المرجع السابق، الحيثية 38.
[370] نفس المرجع السابق، الشق الأول من المادة 8 (1). يقع تعريف مفهوم خدمات مجتمع المعلومات في المادة 4 (25) من اللائحة العامة لحماية البيانات.
[371] اللائحة العامة لحماية البيانات، الشق الثاني من المادة 8 (1).
[372] نفس المرجع السابق، الحيثية 38.
[373] نفس المرجع السابق، الحيثية 58. انظر أيضاً الاتفاقية 108 المحدثة، المادة 15 (2) (هـ). التقرير التفسيري للاتفاقية 108 المحدثة، الفقرتان 68 و125.
[374] اللائحة العامة لحماية البيانات، المادة 7 (3). التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 45.
[375] اللائحة العامة لحماية البيانات، المادة 7 (3).
[376] اللائحة العامة لحماية البيانات، الحيثية 42؛ التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 42.

مثال: وافق عميل على تلقي الرسائل الإلكترونية الترويجية على عنوان قدمه إلى مراقب البيانات. في حالة سحب العميل موافقته، يجب على المراقب التوقف فوراً عن إرسال تلك الرسائل الترويجية. ولا ينبغي فرض أي عواقب عقابية مثل الرسوم. وينطبق ذلك السحب من تلك اللحظة فصاعداً، ولا يكون له أثر رجعي. لذلك فقد كانت الفترة التي تمت فيها معالجة البيانات الشخصية للعميل بشكل مشروع - بحكم موافقة العميل السابقة - فترةً شرعية. وبفعل سحب الموافقة تُمنع أي معالجة لاحقة لتلك البيانات، عدا إذا كانت هذه المعالجة متوافقة مع حق المرء في أن تُمحى بياناته.[377]

### الضرورة المرتبطة بتنفيذ عقد

**بموجب قانون الاتحاد الأوروبي**، تتيح المادة 6 (1) (ب) من اللائحة العامة لحماية البيانات أساساً آخر للمعالجة المشروعة، وهو إذا كانت المعالجة «ضرورية لتنفيذ عقد يكون صاحب البيانات طرفاً فيه». ويغطي هذا المقتضى أيضاً العلاقات ما قبل التعاقد. على سبيل المثال، في الحالات التي ينوي فيها أحد الأطراف إبرام عقد، ولكنه لم يفعل ذلك بعد، ربما لأنه لم يتم بعد استكمال بعض عمليات التحقق التي يتعين إجراؤها. وإذا احتاج أحد الأطراف إلى معالجة البيانات لهذا الغرض، فإن هذه المعالجة تكون مشروعة طالما أنها «ضرورية من أجل اتخاذ إجراءات بناءً على طلب صاحب البيانات قبل إبرام عقد».[378]

يشمل مفهوم معالجة البيانات «كأساس شرعي منصوص عليه في القانون» الوارد في المادة 5 (2) من الاتفاقية 108 المحدثة أيضاً «معالجة البيانات من أجل الوفاء بتنفيذ عقد (أو تدابير ما قبل العقد بناءً على طلب صاحب البيانات) يكون صاحب البيانات طرفاً فيه».[379]

### واجبات المراقب القانونية

ينص **قانون الاتحاد الأوروبي** على أساس آخر لجعل معالجة البيانات مشروعة، وهو إذا «كان ذلك ضرورياً للامتثال لالتزام قانوني يكون المراقب خاضعاً له» (المادة 6 (1) (ج) من اللائحة العامة لحماية البيانات). ويشير هذا المقتضى إلى المراقبين العاملين في كل من القطاعين العام والخاص؛ ويمكن أيضاً أن تندرج الالتزامات القانونية لمراقبي البيانات في القطاع العام ضمن المادة 6 (1) (هـ) من القانون العام لحماية البيانات. هناك العديد من الأمثلة على المواقف التي يُلزِم فيها القانون مراقبي القطاع الخاص بمعالجة البيانات المتعلقة بأصحاب بيانات محددين. فعلى سبيل المثال، يجب على أصحاب العمل معالجة البيانات المتعلقة بموظفيهم لأسباب تتعلق بالضمان الاجتماعي والضرائب، كما يجب على الشركات معالجة البيانات المتعلقة بعملائها لأغراض ضريبية.

يمكن أن ينشأ الالتزام القانوني في قانون الاتحاد الأوروبي أو قانون الدولة العضو، والذي يمكن أن يشكل أساساً لعملية معالجة واحدة أو متعددة. يجب أن يكون القانون هو ما يحدد الغرض من المعالجة، ويضعّ المواصفات لتحديد المراقب ونوع البيانات الشخصية الخاضعة للمعالجة وأصحاب البيانات المعنيين والجهات التي يمكن الكشف عن البيانات لها وحدود الغرض من المعالجة وفترة التخزين وغيرها من التدابير لضمان أن تكون المعالجة قانونية وعادلة.[380] ويجب أن يتوافق أي قانون يمثل أساساً لمعالجة البيانات الشخصية مع المادتين 7 و8 من ميثاق الحقوق الأساسية للاتحاد الأوروبي والمادة 8 من الاتفاقية الأوروبية لحقوق الإنسان.

تعمل الالتزامات القانونية للمراقب أيضاً كأساس للمعالجة المشروعة للبيانات **بموجب قانون مجلس أوروبا**.[381] وكما أشرنا سابقاً، فإن الالتزامات القانونية لمراقبي القطاع الخاص ليست سوى حالة واحدة محددة للمصالح المشروعة للآخرين، كما هو مذكور في المادة 8 (2) من الاتفاقية الأوروبية لحقوق الإنسان. وبالتالي، فإن المثال الخاص بمعالجة أصحاب العمل لبيانات موظفيهم له صلة أيضاً بقانون مجلس أوروبا.

### المصالح الحيوية لصاحب البيانات أو لشخص طبيعي آخر

**بموجب قانون الاتحاد الأوروبي**، تنص المادة 6 (1) (د) من اللائحة العامة لحماية البيانات على أن معالجة البيانات الشخصية تكون قانونية إذا كانت «ضرورية لحماية المصالح الحيوية لصاحب البيانات أو لشخص طبيعي آخر». ولا يجوز التذرع بهذا الأساس المشروع إلا لمعالجة البيانات الشخصية بناءً على المصالح الحيوية لشخص طبيعي آخر، ، إذا كانت هذه المعالجة «لا يمكن أن تستند بجلاء إلى أساس قانوني آخر».[382]

---

[377] اللائحة العامة لحماية البيانات، المادة 17 (1) (ب).

[378] نفس المرجع السابق، المادة 6 (1) (ب).

[379] التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 46؛ مجلس أوروبا، لجنة الوزراء (2010)، التوصية CM/Rec(2010)13 من لجنة الوزراء للدول الأعضاء بشأن حماية الأفراد فيما يتعلق المعالجة الآلية للبيانات الشخصية في سياق التنميط، 23 نوفمبر 2010، المادة 4.3 (ب).

[380] اللائحة العامة لحماية البيانات، الحيثية 45.

[381] مجلس أوروبا، لجنة الوزراء (2010)، التوصية CM/Rec(2010)13 من لجنة الوزراء للدول الأعضاء بشأن حماية الأفراد فيما يتعلق المعالجة الآلية للبيانات الشخصية في سياق التنميط، 23 نوفمبر 2010، المادة 4.3 (أ)

[382] اللائحة العامة لحماية البيانات، الحيثية 46.

ففي بعض الأحيان، قد يعتمد نوع المعالجة على أسس المصلحة العامة والمصالح الحيوية لصاحب البيانات أو لشخص آخر. وهذا هو الحال، على سبيل المثال، عند مراقبة الأوبئة وتطورها، أو عند وجود حالة طوارئ إنسانية.

**بموجب قانون مجلس أوروبا**، لم يتم ذكر المصالح الحيوية لصاحب البيانات في المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان. ومع ذلك، تُعتبر المصالح الحيوية لصاحب البيانات متضمّنة في مفهوم 'الأساس المشروع' للمادة 5 (2) من الاتفاقية 108 المحدثة، والتي تتناول مسألة شرعية معالجة البيانات الشخصية.[383]

**المصلحة العامة وممارسة السلطة الرسمية**

نظراً للطرق المتعددة الممكن اتباعها لتنظيم الشؤون العامة، تنص المادة 6 (1) (هـ) من اللائحة العامة لحماية البيانات على أنه يمكن معالجة البيانات الشخصية بشكل قانوني إذا كانت «ضرورية لأداء مهمة يتم تنفيذها للمصلحة العامة أو في إطار ممارسة السلطة الرسمية المخولة للمراقب [...]»،[384]

مثال: في قضية «هوبر ضد جمهورية ألمانيا الاتحادية»،[385] طلب السيد هوبر، وهو مواطن نمساوي مقيم في ألمانيا، من المكتب الفيدرالي للهجرة واللاجئين حذف البيانات المتعلقة به في السجل المركزي للأجانب ('AZR'). إن هذا السجل، الذي يحتوي على بيانات شخصية عن مواطني الاتحاد الأوروبي غير الألمان المقيمين في ألمانيا لأكثر من ثلاثة أشهر، يُستخدم للأغراض الإحصائية ومن قبل سلطات إنفاذ القانون والسلطات القضائية عند التحقيق في الأنشطة الإجرامية أو تلك التي تهدد الأمن العام وفي مقاضاة مرتكبيها. وتساءلت المحكمة التي قامت بإحالة القضية عما إذا كانت معالجة البيانات الشخصية التي يتم إجراؤها في سجل مثل السجل المركزي للأجانب - الذي يمكن للسلطات العامة الأخرى الوصول إليه أيضاً - متوافقة مع قانون الاتحاد الأوروبي نظراً لعدم وجود مثل هذا السجل للمواطنين الألمان.

رأت محكمة العدل التابعة للاتحاد الأوروبي أنه وفقاً للمادة 7 (هـ) من الأمر التوجيهي 95/46، [386] يمكن معالجة البيانات الشخصية بشكل قانوني إذا كان ذلك ضرورياً لأداء مهمة يتم تنفيذها خدمةً للمصلحة العامة أو في إطار ممارسة سلطة رسمية.

ووفقاً لمحكمة العدل التابعة للاتحاد الأوروبي، فإنه «مع مراعاة الهدف المتمثل في ضمان مستوىً مكافئ من الحماية في جميع الدول الأعضاء، لا يمكن أن يكون لمفهوم الضرورة المنصوص عليه في المادة 7 (هـ) من الأمر التوجيهي 95/46 [387] [...] معنىً يختلف بين الدول الأعضاء. وبالتالي، يترتب على ذلك أن ما هو محل النقاش هو مفهوم له معناه المستقل الخاص به في قانون الاتحاد الأوروبي والذي يجب تفسيره بطريقة تعكس تماماً هدف ذلك الأمر التوجيهي، على النحو المنصوص عليه في المادة 1 (1) منه».[388]

لاحظت محكمة العدل التابعة للاتحاد الأوروبي أن الحق في حرية التنقل لمواطن ينتمي للاتحاد الأوروبي، في أراضي دولة عضو ليس من رعاياها، ليس غير مشروط وقد يخضع لقيود وشروط تفرضها المعاهدة المؤسسة للجماعة الأوروبية والتدابير المعتمدة لتفعيلها. وبالتالي، إذا كان من المشروع من حيث المبدأ، لدولة عضو استخدام سجل مثل السجل المركزي للأجانب لدعم السلطات المسؤولة عن تطبيق التشريعات المتعلقة بحق الإقامة، فإنه يجب ألا يحتوي هذا السجل على أي معلومات غير تلك اللازمة لتحقيق هذا الغرض بالذات. وخلصت محكمة العدل التابعة للاتحاد الأوروبي إلى أن مثل هذا النظام المُستخدَم لمعالجة البيانات الشخصية يتوافق مع قانون الاتحاد الأوروبي إذا كان يحتوي فقط على البيانات اللازمة لتطبيق هذا التشريع وإذا كانت طبيعته المركزية تجعل تطبيق هذا التشريع أكثر فعالية. ويجب على المحكمة الوطنية أن تتحقق مما إذا كانت هذه الشروط مستوفاة في هذه الحالة بالذات. وإذا لم يكن الأمر كذلك، فإن تخزين ومعالجة البيانات الشخصية في سجل مثل السجل المركزي للأجانب للأغراض الإحصائية لا يمكن، على أي أساس، اعتباره ضرورياً بالمعنى المقصود في المادة 7 (هـ)[389] من الأمر التوجيهي 95/46. [390]

[383] التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 46.
[384] انظر اللائحة العامة لحماية البيانات، الحيثية 45.
[385] محكمة العدل التابعة للاتحاد الأوروبي، C-524/06، قضية «'هاينز هيوبر 'ضد جمهورية ألمانيا الاتحادية» [الغرفة الكبرى]، 16 ديسمبر 2008.
[386] الأمر التوجيهي المتعلق بحماية البيانات، المادة 7 (هـ) سابقاً، أصبحت الآن المادة 6 (1) (هـ) من اللائحة العامة لحماية البيانات.
[387] نفس المرجع السابق.
[388] محكمة العدل التابعة للاتحاد الأوروبي، C-524/06، قضية «'هاينز هيوبر 'ضد جمهورية ألمانيا الاتحادية» [الغرفة الكبرى]، 16 ديسمبر 2008، الفقرة 52.
[389] الأمر التوجيهي المتعلق بحماية البيانات، المادة 7 (هـ) سابقاً، أصبحت الآن المادة 6 (1) (هـ) من اللائحة العامة لحماية البيانات.
[390] محكمة العدل التابعة للاتحاد الأوروبي، C-524/06، قضية «'هاينز هيوبر 'ضد جمهورية ألمانيا الاتحادية» [الغرفة الكبرى]، 16 ديسمبر 2008، الفقرات 54 و59-58 و68-66.

أخيراً، وفيما يتعلق بمسألة استخدام البيانات الواردة في السجل لأغراض مكافحة الجريمة، رأت محكمة العدل التابعة للاتحاد الأوروبي أن هذا الهدف «ينطوي بالضرورة على مقاضاة الجرائم والمخالفات المرتكبة، بغض النظر عن جنسية مرتكبيها». ولا يحتوي السجل المعني على بيانات شخصية تتعلق بمواطني الدولة العضو المعنية، ويشكل هذا الاختلاف في المعاملة تمييزاً محظوراً بموجب المادة 18 من المعاهدة المتعلقة بسير عمل الاتحاد الأوروبي. وبالتالي، وجدت محكمة العدل التابعة للاتحاد الأوروبي أن هذا البند «يحول دون قيام دولة عضو، بغرض مكافحة الجريمة، بوضع نظام لمعالجة البيانات الشخصية الخاصة بمواطني الاتحاد الذين ليسوا من مواطني تلك الدولة العضو.»[391]

يخضع استخدام البيانات الشخصية من قبل السلطات التي تعمل في المجال العام أيضاً للمادة 8 من **الاتفاقية الأوروبية لحقوق الإنسان** ومن المفترض أن تتم تغطيته، عند الاقتضاء، بموجب المادة 5 (2) من الاتفاقية 108 المحدثة.[392]

**المصالح المشروعة التي يسعى إليها المراقب أو طرف ثالث**

بموجب **قانون الاتحاد الأوروبي**، لا يُعتبر صاحب البيانات هو الشخص الوحيد الذي لديه مصالح مشروعة، إذ تنص المادة 6 (1) (و) من اللائحة العامة لحماية البيانات على مشروعية معالجة البيانات الشخصية إذا كانت المعالجة «ضرورية لأغراض المصالح المشروعة التي يسعى إليها المراقب أو الطرف أو الأطراف الثالثة [باستثناء السلطات العامة في إطار أداء مهامها] التي يتم الكشف عن البيانات لصالحها، ماعدا الحالات التي تَبطل فيها هذه المصالح بفعل أسبقية مصالح صاحب البيانات أو حقوقه وحرياته الأساسية التي تتطلب الحماية [...]».[393]

يجب تقييم وجود مصلحة مشروعة بعناية في كل حالة على حدة.[394] إذا تم تحديد المصالح المشروعة للمراقب، فيجب إجراء عملية موازنة بين تلك المصالح والمصالح أو الحقوق والحريات الأساسية لصاحب البيانات.[395] ويجب مراعاة التوقعات المعقولة لصاحب البيانات أثناء هذا التقييم للتأكد مما إذا كانت مصالح المراقب تطغى على المصالح أو الحقوق الأساسية لصاحب البيانات.[396] فإذا طغت حقوق صاحب البيانات على المصالح المشروعة للمراقب، يمكن للمراقب اتخاذ التدابير وتفعيل الضمانات الكفيلة بتقليل الأثر على حقوق صاحب البيانات (مثل استخدام اسم مستعار للبيانات)، وعكس 'التوازن' قبل التمكن بشكل قانوني من الاعتماد على هذا الأساس الشرعي للمعالجة. وقد أكد فريق عمل المادة 29، في رأيه حول مفهوم المصالح المشروعة لمراقب البيانات، على الدور الحاسم للمساءلة والشفافية، وحقوق صاحب البيانات في الاعتراض على معالجة بياناته أو الوصول إليها وتعديلها أو حذفها أو نقلها، عند الموازنة بين المصالح المشروعة للمراقب ومصالح الحقوق الأساسية لصاحب البيانات.[397]

وتأتي حيثيات اللائحة العامة لحماية البيانات على بعض الأمثلة لما يشكل مصلحة مشروعة لمراقب البيانات المعني. فعلى سبيل المثال، يُسمح بمعالجة البيانات الشخصية دون موافقة صاحب البيانات عندما يتم ذلك لأغراض التسويق المباشر أو عندما تكون هذه المعالجة «ضرورية تماماً لأغراض منع الاحتيال».[398]

ولقد وسعت محكمة العدل التابعة للاتحاد الأوروبي في سوابقها القضائية نطاق الاختبار الذي يرم إجراؤه لتحديد ما يشكل مصلحة مشروعة.

[391] نفس المرجع السابق، الفقرتان 78 و81.
[392] التقرير التفسيري للاتفاقية 108 المحدثة، الفقرتان 46 و47.
[393] مقارنة بالأمر التوجيهي 95/46. توفر اللائحة العامة لحماية البيانات أمثلة أكثر عن الحالات التي تُعتبر أنها تشكل مصلحة مشروعة.
[394] اللائحة العامة لحماية البيانات، الديباجة، الحيثية 47.
[395] لفريق عمل المادة 29 (2014)، الرأي 06/2014 بشأن مفهوم المصالح المشروعة لمراقب البيانات بموجب المادة 7 من الأمر التوجيهي EC، 4/95/46 أبريل 2014.
[396] نفس المرجع السابق.
[397] نفس المرجع السابق.
[398] اللائحة العامة لحماية البيانات، الديباجة، الحيثية 47.

مثال: تتعلق قضية «إدارة الشرطة الإقليمية في ريغا»[399] بأضرار لحقت بحافلة تابعة لشركة «ريغاس ساتيكسمي» للنقل بسبب قيام أحد الركاب بفتح باب سيارة أجرة فجأة. أرادت شركة النقل مقاضاة الراكب عن الأضرار، ولكن الشرطة اكتفت بتقديم اسم الراكب ورفضت أن تفصح عن رقم هويته وعنوانه، بحجة أن الكشف عن تلك المعلومات سيكون مخالفاً للقانون بموجب التشريعات الوطنية المتعلقة بحماية البيانات. يُذكر أن المحكمة اللاتفية التي قامت بإحالة القضية على محكمة العدل التابعة للاتحاد الأوروبي قد طلبت من هذه الأخيرة إصدار حكم تمهيدي بشأن ما إذا كان قانون حماية البيانات في الاتحاد الأوروبي يفرض التزاماً بالكشف عن جميع البيانات الشخصية اللازمة لتحريك الإجراءات المدنية ضد الشخص الذي يُزعم أنه مسؤول عن مخالفة إدارية.[400]

أوضحت محكمة العدل التابعة للاتحاد الأوروبي أن قانون حماية البيانات في الاتحاد الأوروبي يتضمن إمكانية - وليس التزاماً - لتقديم البيانات إلى طرف ثالث لأغراض المصالح المشروعة التي يسعى إليها هذا الطرف.[401] وحددت محكمة العدل التابعة للاتحاد الأوروبي ثلاثة شروط تراكمية يجب استيفاؤها حتى تكون معالجة البيانات الشخصية قانونية على أساس 'المصالح المشروعة'.[402] أولاً، يجب على الطرف الثالث الذي يتم الكشف عن البيانات له السعي وراء مصلحة مشروعة. في هذه الحالة المحددة، يعني هذا أن طلب معلومات شخصية لمقاضاة شخص ما بسبب إلحاقه ضرراً بالممتلكات يشكل مصلحة مشروعة لطرف ثالث. ثانياً، يجب أن تكون معالجة البيانات الشخصية ضرورية لأغراض المصالح المشروعة المنشودة. في هذه الحالة، يُعد الحصول على معلومات شخصية مثل العنوان و / أو رقم الهوية أمراً ضرورياً للغاية لتحديد هوية هذا الشخص. ثالثاً، يجب ألا تكون الحقوق والحريات الأساسية لصاحب البيانات طاغية على المصالح المشروعة للمراقب أو الأطراف الثالثة. يجب أن يتم تحقيق توازن المصالح على أساس كل حالة على حدة، مع مراعاة عناصر مثل خطورة التعدي على حقوق صاحب البيانات أو حتى سنّه في ظروف معينة. إلا أنه في هذه الحالة المحددة، لم تعتبر محكمة العدل التابعة للاتحاد الأوروبي رفض الكشف مُبرَّراً لمجرد أن صاحب البيانات كان قاصراً.

في حكم قضية «الرابطة الوطنية لمؤسسات الائتمان المالي (ASNEF) واتحاد التجارة الإلكترونية والتسويق المباشر (FECEMD)»، قضت محكمة العدل التابعة للاتحاد الأوروبي صراحة في مسألة معالجة البيانات مستندةً إلى الأساس القانوني المتمثل في 'المصالح المشروعة'، والذي تم تكريسه في ذلك الوقت في المادة 7 (و) من الأمر التوجيهي المتعلق بحماية البيانات.[403]

مثال: في قضية «الرابطة الوطنية لمؤسسات الائتمان المالي (ASNEF) واتحاد التجارة الإلكترونية والتسويق المباشر (FECEMD)»،[404] أوضحت محكمة العدل التابعة للاتحاد الأوروبي أن القانون الوطني غير مسموح له بإضافة شروط لتلك المذكورة في المادة 7 (و) من الأمر التوجيهي المتعلق بالمعالجة القانونية للبيانات.[405] ويشير هذا إلى حالة احتوى فيها قانون حماية البيانات الإسباني على مقتضىً يمكن بموجبه لأطراف خاصة أخرى المطالبة بمصلحة مشروعة في معالجة البيانات الشخصية فقط إذا كانت المعلومات قد سبق وأن ظهرت في مصادر عامة.

لاحظت محكمة العدل التابعة للاتحاد الأوروبي أولاً أن الأمر التوجيهي 95/46 [406] يهدف إلى ضمان أن يكون مستوى حماية حقوق وحريات الأفراد فيما يتعلق بمعالجة البيانات الشخصية متساوٍ في جميع الدول الأعضاء. كما يجب ألا يؤدي تقريب القوانين الوطنية المطبقة في هذا المجال إلى أي انخفاض في الحماية التي توفرها، ويجب أن تسعى بدلاً من ذلك إلى ضمان مستوىً عالٍ من الحماية في الاتحاد الأوروبي.[407] وبناءً على ذلك، ارتأت محكمة العدل التابعة للاتحاد الأوروبي أنه «تماشياً مع الهدف المتمثل في ضمان مستوىً مكافئ من الحماية في جميع الدول الأعضاء فإن المادة 7 من الأمر التوجيهي 95/46 [408] تحدد قائمة شاملة ومحصورة للحالات التي يمكن فيها اعتبار معالجة البيانات الشخصية مسألة مشروعة». علاوة على ذلك، «لا يمكن للدول الأعضاء إدخال مبادئ جديدة تتعلق بمشروعية معالجة البيانات الشخصية على المادة 7 من الأمر التوجيهي 95/46 [409] أو فرض متطلبات إضافية يكون لها أثر تعديل نطاق أحد المبادئ الستة المنصوص عليها» في المادة 7.[410] أقرت محكمة العدل التابعة للاتحاد الأوروبي بأنه فيما يتعلق بالموازنة الضرورية وفقاً

[399] محكمة العدل التابعة للاتحاد الأوروبي، C13-16، قضية «إدارة الشرطة الإقليمية في ريغا ضد شركة 'ريغاس ساتيكسمي' للنقل التابعة لبلدية ريغا» 4 مايو 2017

[400] نفس المرجع السابق، الفقرة 23.

[401] نفس المرجع السابق، الفقرة 26.

[402] نفس المرجع السابق، الفقرات 34-28.

[403] الأمر التوجيهي المتعلق بحماية البيانات، المادة 7 (و) سابقاً، أصبحت الآن المادة 6 (1) (و) من اللائحة العامة لحماية البيانات.

[404] محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-468/10 وC-469/10، الرابطة الوطنية لمؤسسات الائتمان المالي (ASNEF) واتحاد التجارة الإلكترونية والتسويق المباشر (FECEMD) ضد إدارة الدولة، 24 نوفمبر 2011.

[405] الأمر التوجيهي المتعلق بحماية البيانات، المادة 7 (و) سابقاً، أصبحت الآن المادة 6 (1) (و) من اللائحة العامة لحماية البيانات.

[406] الأمر التوجيهي المتعلق بحماية البيانات، سابقاً، أصبح الآن اللائحة العامة لحماية البيانات.

[407] محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-468/10 وC-469/10، الرابطة الوطنية لمؤسسات الائتمان المالي (ASNEF) واتحاد التجارة الإلكترونية والتسويق المباشر (FECEMD) ضد إدارة الدولة، 24 نوفمبر 2011، الفقرة 28. انظر الأمر التوجيهي المتعلق بحماية البيانات، الحيثيتان 8 و10.

[408] الأمر التوجيهي المتعلق بحماية البيانات، المادة 7 سابقاً، أصبحت الآن المادة 6 (1) (و) من اللائحة العامة لحماية البيانات.

[409] الأمر التوجيهي المتعلق بحماية البيانات، المادة 7 سابقاً، أصبحت الآن المادة 6 من اللائحة العامة لحماية البيانات.

[410] نفس المرجع السابق.

للمادة 7 (و) من الأمر التوجيهي EC/95/46، من الممكن الأخذ في الاعتبار خطورة التعدي على الحقوق الأساسية لصاحب البيانات بسبب المعالجة قد يختلف حسب الحالة، اعتماداً على ما إذا كانت البيانات المعنية تظهر مسبقاً في المصادر العامة أم لا.
ومع ذلك، فإن المادة 7 (و) من الأمر التوجيهي «تمنع الدولة العضو من استبعاد إمكانية معالجة فئات معينة من البيانات الشخصية، بطريقة قاطعة ومعممة، دون السماح بالموازنة بين الحقوق والمصالح المتعارضة محل النزاع في تلك الحالة المعينة».
في ضوء هذه الاعتبارات، خلصت محكمة العدل التابعة للاتحاد الأوروبي إلى أن المادة 7 (و) من الأمر التوجيهي 95/46 [411] يجب تفسيرها «على أنها تستبعد القواعد الوطنية التي، في حالة عدم موافقة صاحب البيانات، ومن أجل السماح بمعالجة تلك البيانات الشخصية الخاصة بصاحب البيانات المعني كما هو ضروري من أجل السعي إلى مصلحة مشروعة لمراقب البيانات أو الطرف أو الأطراف الثالثة الذين يتم الكشف عن هذه البيانات لهم، لا تتطلب فقط احترام الحقوق والحريات الأساسية لصاحب البيانات، ولكن أيضاً أن تكون البيانات تظهر في المصادر العامة، وبالتالي فإنها تستبعد، بطريقة قاطعة ومعممة، أي معالجة للبيانات لا تظهر في هذه المصادر».[412]

عندما تتم معالجة البيانات الشخصية وفقًا لأساس 'المصالح المشروعة'، يحق للفرد الاعتراض في أي وقت على المعالجة، على أسس تتعلق بوضعه الخاص، وفقاً للمادة 21 (1) من اللائحة العامة لحماية البيانات. ويجب أن يوقف المراقب المعالجة، ما لم يقدم أسباباً مشروعة واضطرارية لمواصلة المعالجة.

فيما يتعلق **بقانون مجلس أوروبا**، يمكن العثور على صيغ مماثلة في الاتفاقية 108 المحدثة[413] وتوصيات مجلس أوروبا. وتقر التوصية المتعلقة بالتنميط بأن معالجة البيانات الشخصية لأغراض التنميط مشروعة إذا لزم الأمر لتحقيق المصالح المشروعة للآخرين، «باستثناء الحالات التي تَبطل فيها هذه المصالح بحكم أسبقية حقوق أصحاب البيانات وحرياتهم الأساسية»،[414] بالإضافة إلى ذلك، تمت الإشارة إلى «حماية حقوق وحريات الآخرين» في المادة 8 (2) من الاتفاقية الأوروبية لحقوق الإنسان كأحد الأسس المشروعة للحد من الحق في حماية البيانات.

مثال: في قضية «ي. ضد تركيا»،[415] كان المدعي مصاباً بفيروس نقص المناعة البشرية. ونظراً لأنه كان فاقداً للوعي أثناء وصوله إلى المستشفى، أبلغ طاقم الإسعاف طاقم المستشفى أنه مصاب بفيروس نقص المناعة البشرية. جادل المدعي أمام المحكمة الأوروبية لحقوق الإنسان بأن الكشف عن هذه المعلومات قد شكل انتهاكاً لحقه في احترام الحياة الخاصة. ولكن، نظراً لضرورة حماية سلامة موظفي المستشفى، فإن الكشف عن هذه المعلومة لهم لم يُنظر إليه على أنه انتهاك لحقوقه.

## 2.1.4. معالجة فئات خاصة من البيانات (البيانات الحساسة)

يترك **قانون مجلس أوروبا** للقانون المحلي مهمة وضع تدابير الحماية المناسبة لاستخدام البيانات الحساسة، شريطة استيفاء شروط المادة 6 من الاتفاقية 108 المحدثة، لا سيما التنصيص القانوني على الضمانات المناسبة التي تكمل باقي مقتضيات الاتفاقية. ويحتوي **قانون الاتحاد الأوروبي**، في المادة 9 من اللائحة العامة لحماية البيانات، على نظام تفصيلي لمعالجة فئات خاصة من البيانات (تسمى أيضاً 'البيانات الحساسة')، تكشف هذه البيانات عن الأصل العرقي أو الإثني، والآراء السياسية، والمعتقدات الدينية أو الفلسفية، والعضوية النقابية، وكذلك البيانات الجينية والبيومترية التي يمكن قد تُعالَج لأغراض تحديد هوية الشخص الطبيعي بشكل فريد، والبيانات المتعلقة بالصحة أو الحياة الجنسية أو التوجه الجنسي للشخص. إن معالجة البيانات الحساسة محظورة من حيث المبدأ،[416]

[411] الأمر التوجيهي المتعلق بحماية البيانات، المادة 7 (و) سابقاً، أصبحت الآن المادة 6 (1) (و) من اللائحة العامة لحماية البيانات.
[412] محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-468/10 وC-469/10، «الرابطة الوطنية لمؤسسات الائتمان المالي (ASNEF) واتحاد التجارة الإلكترونية والتسويق المباشر (FECEMD) ضد إدارة الدولة»، 24 نوفمبر 2011، الفقرات 40 و44 و48-49.
[413] التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 46.
[414] مجلس أوروبا، لجنة الوزراء (2010)، التوصية CM/Rec(2010)13 والمذكرة التفسيرية بشأن حماية الأفراد فيما يتعلق بالمعالجة الآلية لبياناتهم الشخصية في سياق التنميط، 23 نوفمبر 2010، المادة 4.3 (ب) (التوصية بشأن التنميط).
[415] المحكمة الأوروبية لحقوق الإنسان، قضية «ي. ضد تركيا»، رقم 648/10، 17 فبراير 2015.
[416] الأمر التوجيهي المتعلق بحماية البيانات، المادة 7 (و) سابقاً، الآن المادة 9 (1) من اللائحة العامة لحماية البيانات.

ومع ذلك، هناك قائمة شاملة للإعفاءات من هذا الحظر، والتي يمكن العثور عليها في المادة 9 (2) من اللائحة، وهي ترقى لأن تشكل أسساً قانونية لمعالجة البيانات الحساسة. تشمل هذه الاستثناءات الحالات التالية:

- موافقة صاحب البيانات صراحة على معالجة البيانات؛
- تتم المعالجة من قبل هيئة غير ربحية ذات أغراض سياسية أو فلسفية أو دينية أو نقابية في سياق أنشطتها المشروعة وتتعلق فقط بأعضائها (السابقين) أو بالأشخاص الذين لديهم اتصال منتظم بها لهذه الأغراض؛
- تتعلق المعالجة بالبيانات التي تم نشرها صراحةً من قبل صاحب البيانات؛
- تكون المعالجة ضرورية:

- لتنفيذ الالتزامات وممارسة الحقوق المحددة للمراقب أو صاحب البيانات في سياق التوظيف والضمان الاجتماعي والحماية الاجتماعية؛
- لحماية المصالح الحيوية لصاحب البيانات أو أي شخص طبيعي آخر (عندما لا يستطيع صاحب البيانات إعطاء الموافقة)؛
- لإقامة الدعاوى القانونية أو ممارستها أو الدفاع عنها أو عندما تتصرف المحاكم بصفتها القضائية؛
- لأغراض الطب الوقائي أو المهني: «لتقييم القدرة الموظف على العمل، والتشخيص الطبي، وتوفير الرعاية الصحية أو الاجتماعية أو العلاج، أو إدارة أنظمة وخدمات الرعاية الصحية أو الاجتماعية على أساس قانون الاتحاد أو الدولة العضو أو بموجب عقد مع مهني في مجال الصحة»؛
- لأغراض الأرشفة للمصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو للأغراض الإحصائية؛
- لأسباب تتعلق بالمصلحة العامة في مجال الصحة العامة؛
- لأسباب جوهرية تتعلق بالمصلحة العامة.

لمعالجة فئات خاصة من البيانات، لا يُنظر إلى العلاقة التعاقدية مع صاحب البيانات إذا كأساس قانوني للمعالجة المشروعة للبيانات الحساسة، باستثناء عقد مع أخصائي صحي يخضع لالتزام السرية المهنية.[417]

**الموافقة الصريحة لصاحب البيانات**

بموجب **قانون الاتحاد الأوروبي**، فإن أول أساس ممكن للمعالجة القانونية لأي بيانات، بغض النظر عما إذا كانت بيانات حساسة أو غير حساسة، هو موافقة صاحب البيانات. في حالة البيانات الحساسة، يجب أن تكون هذه الموافقة صريحة. إلا أنه يمكن لقانون الاتحاد أو الدول الأعضاء أن ينص على أنه لا يجوز للفرد رفع الحظر المفروض على معالجة الفئات الخاصة من البيانات.[418] وقد يكون هذا هو الحال، على سبيل المثال، عندما تنطوي المعالجة على مخاطر غير عادية لصاحب البيانات.

**قانون العمل أو قانون الضمان الاجتماعي والحماية الاجتماعية**

بموجب **قانون الاتحاد الأوروبي**، يمكن رفع الحظر الوارد في الفقرة 1 من المادة 9 إذا كانت المعالجة ضرورية لتنفيذ التزامات أو حقوق المراقب أو صاحب البيانات في مجال العمل أو الضمان الاجتماعي. إلا أنه يجب أن تتم هذه المعالجة بموجب قانون الاتحاد الأوروبي أو القانون الوطني أو اتفاقية جماعية بموجب القانون الوطني، والتي توفر الضمانات المناسبة للحقوق الأساسية لصاحب البيانات ومصالحه.[419] ويمكن أن تتضمن سجلات التوظيف التي تحتفظ بها منظمة ما بيانات شخصية حساسة في ظل ظروف معينة محددة في اللائحة العامة لحماية البيانات والقانون الوطني ذي الصلة. من بين الأمثلة على البيانات الحساسة، يمكن أن نجد البيانات المتعلقة بعضوية النقابات العمالية أو المعلومات المتعلقة بصحة الفرد.

**المصالح الحيوية لصاحب البيانات أو شخص آخر**

بموجب **قانون الاتحاد الأوروبي**، وكما هو الحال بالنسبة للبيانات غير الحساسة، يمكن معالجة البيانات الحساسة بسبب المصالح الحيوية لصاحب البيانات أو شخص طبيعي آخر،[420] وحيثما تكون المعالجة مستندة إلى المصالح الحيوية لشخص آخر، فلا يجوز التذرع بهذا الأساس

[417] اللائحة العامة لحماية البيانات، المادة 9 (2) (ج) و(ط).
[418] نفس المرجع السابق، المادة 9 (2) (أ).
[419] اللائحة العامة لحماية البيانات، المادة 9 (2) (ب).
[420] نفس المرجع السابق، المادة 9 (2) (ج).

المشروع إلا إذا كانت هذه المعالجة «لا يمكن أن تستند جلياً إلى أساس قانوني آخر».[421] في بعض الحالات، قد تحمي معالجة البيانات الشخصية المصالح الفردية والعامة، مثلاً عندما تكون المعالجة ضرورية للأغراض الإنسانية.[422]

لكي تكون معالجة البيانات الحساسة مشروعة على هذا الأساس، يجب أن يكون من المستحيل طلب الموافقة من صاحب البيانات، لأنه على سبيل المثال، قد يكون صاحب البيانات فاقداً للوعي أو يكون غائباً ولا يمكن الوصول إليه. بمعنىً آخر، عندما يكون الشخص غير قادر جسدياً أو قانونياً على إعطاء الموافقة.

**الجمعيات الخيرية أو الهيئات غير الهادفة للربح**

يُسمح أيضاً بمعالجة البيانات الشخصية في سياق الأنشطة المشروعة للمؤسسات أو الجمعيات أو غيرها من الهيئات غير الهادفة للربح التي تسعى إلى هدف سياسي أو فلسفي أو ديني أو نقابي. غير أنه يجب أن تتعلق المعالجة فقط بالأعضاء أو الأعضاء السابقين في الهيئة، أو أولئك الذين لديهم اتصال منتظم بها.[423] ولا يمكن الكشف عن البيانات الحساسة لجهات خارج تلك الهيئات دون موافقة صاحب البيانات.

**البيانات المتاحة للعموم بجلاء من طرف صاحب البيانات**

تنص المادة 9 (2) (هـ) من اللائحة العامة لحماية البيانات على أن المعالجة لا تكون محظورة إذا كانت تتعلق بالبيانات التي تمت إتاحتها للعموم جلياً من طرف صاحب البيانات. فعلى الرغم من أن معنى «الإتاحة للعموم جلياً من طرف صاحب البيانات» لم يتم تعريفه في اللائحة، بما أنه يشكل استثناءً لحظر معالجة البيانات الحساسة، فيجب تفسيره بدقة وعلى أنه يتطلب من صاحب البيانات أن يتيح بياناته للعموم بشكل متعمَّد. وبالتالي، عندما يبث التلفزيون مقطع فيديو مأخوذاً من كاميرا مراقبة بالفيديو، يظهر، من بين أشياء أخرى، إصابة رجل إطفاء أثناء محاولته إخلاء مبنى، فلا يمكن اعتبار أن رجل الإطفاء قد أتاح تلك البيانات للعموم جلياً. من ناحية أخرى، إذا قرر رجل الإطفاء وصف الحادث ونشر الفيديو والصور على صفحة إنترنت عامة، يُعتبر أنه قد قام بعمل إيجابي متعمد لإتاحة البيانات الشخصية للعموم. من المهم ملاحظة أن إتاحة الشخص بياناته الشخصية للعموم لا يمثل موافقة، ولكنه يُعد إذناً آخر لمعالجة فئات خاصة من البيانات.

إن كون صاحب البيانات قد أتاح البيانات الشخصية المعالجة للعموم لا يعفي المراقبين من التزاماتهم بموجب قانون حماية البيانات. فعلى سبيل المثال، يستمر العمل بمبدأ حصر الغرض على البيانات الشخصية حتى ولو كانت هذه البيانات متاحة للجمهور.[424]

**الدعاوى القانونية**

يُسمح أيضاً بمعالجة فئات خاصة من البيانات «اللازمة لإقامة الدعاوى القانونية أو ممارستها أو الدفاع عنها»، سواء في إجراءات المحكمة أو في إجراءات إدارية أو خارج المحكمة،[425] بموجب اللائحة العامة لحماية البيانات.[426] في هذه الحالة، يجب أن تكون المعالجة ذات صلة بدعوى قانونية محددة وممارستها أو الدفاع عنها على التوالي، ويمكن أن يطلبها أي من الأطراف المتنازعة.

عندما تتصرف المحاكم بصفتها القضائية، يجوز لها معالجة فئات خاصة من البيانات في سياق حل نزاع قانوني.[427] يمكن أن تشمل الأمثلة على هذه الفئات الخاصة من البيانات التي تتم معالجتها في هذا السياق، على سبيل المثال، البيانات الجينية عند إثبات النسب، أو الحالة الصحية عندما يتعلق جزء من الدليل بتفاصيل الضرر الذي لحق بضحية جريمة.

**أسباب المصلحة العامة الجوهرية**

وفقاً للمادة 9 (2) (ز) من اللائحة العامة لحماية البيانات، يجوز للدول الأعضاء وضع المزيد من الظروف التي يمكن فيها معالجة البيانات الحساسة، طالما:

- تتم معالجة البيانات لأسباب تتعلق بمصلحة عامة جوهرية؛
- ينص عليه القانون الأوروبي أو الوطني؛
- يكون القانون الأوروبي أو الوطني متناسباً ويحترم الحق في حماية البيانات ويوفر تدابير مناسبة ومحددة لحماية حقوق ومصالح صاحب البيانات.[428]

---

[421] نفس المرجع السابق، الحيثية 46.
[422] نفس المرجع السابق.
[423] نفس المرجع السابق، المادة 9 (2) (د).
[424] لفريق عمل المادة 29 (2013)، الرأي 3/13 بشأن حصر الغرض، WP 203، بروكسل، 2 أبريل 2013، ص. 14.
[425] اللائحة العامة لحماية البيانات، الديباجة، الحيثية 52.
[426] نفس المرجع السابق، المادة 9 (2) (و).
[427] نفس المرجع السابق.
[428] نفس المرجع السابق، المادة 9 (2) (ز).

من الأمثلة البارزة، نذكر أنظمة الملفات الصحية الإلكترونية، إذ تسمح هذه الأنظمة بإتاحة البيانات الصحية التي يتم جمعها من قبل مقدمي خدمات الرعاية الصحية أثناء علاج المريض، لمقدمي خدمات الرعاية الصحية الآخرين لهذا المريض على نطاق واسع، وعادة ما يكون يتم ذلك على الصعيد الوطني.

خلص فريق عمل المادة 29 إلى أن إنشاء مثل هذه الأنظمة لا يمكن أن يحدث بموجب القواعد القانونية الحالية لمعالجة البيانات المتعلقة بالمرضى.[429] ومع ذلك، من الممكن أن توجد أنظمة الملفات الصحية الإلكترونية إذا كانت تستند إلى «أسباب تتعلق بمصلح عامة جوهرية».[430] ويتطلب ذلك أساساً قانونياً صريحاً لإنشائها، والذي يُفترض أن يحتوي أيضاً على الضمانات اللازمة لضمان تشغيل النظام بشكل آمن.[431]

**أسس أخرى لمعالجة البيانات الحساسة**

تنص اللائحة العامة لحماية البيانات على إمكانية معالجة البيانات الحساسة في الحالات التي تكون المعالجة فيها ضرورية من أجل:[432]

- أغراض الطب الوقائي أو المهني، لتقييم القدرة الموظف على العمل، أو التشخيص الطبي، أو تقديم الرعاية الصحية أو الاجتماعية أو العلاج، أو إدارة أنظمة وخدمات الرعاية الصحية أو الاجتماعية على أساس قانون الاتحاد الأوروبي أو الدولة العضو، أو بموجب عقد مع مهني في مجال الصحة؛
- أسباب متعلقة بالمصلحة العامة في مجال الصحة العامة، مثل الحماية من التهديدات الخطيرة للصحة العابرة للحدود، أو ضمان معايير عالية لجودة وسلامة الرعاية الصحية والمنتجات أو الأجهزة الطبية، على أساس قانون الاتحاد الأوروبي أو الدولة العضو. ويجب أن ينص القانون على تدابير مناسبة ومحددة لحماية حقوق أصحاب البيانات؛
- الأرشفة أو البحث العلمي أو التاريخي أو الأغراض الإحصائية على أساس قانون الاتحاد الأوروبي أو الدولة العضو. ويجب أن يكون القانون متناسباً مع الهدف المنشود، وأن يحترم جوهر الحق في حماية البيانات، وأن ينص على تدابير مناسبة ومحددة لحماية حقوق ومصالح صاحب البيانات.

**شروط إضافية بموجب التشريع الوطني**

تسمح اللائحة العامة لحماية البيانات أيضاً للدول الأعضاء بتقديم شروط إضافية أو المحافظة عليها، بما في ذلك القيود على معالجة البيانات الجينية والبيومترية والمتعلقة بالصحة.[433]

## 2.4. قواعد أمن المعالجة

### النقاط الرئيسية

- تُلزِم القواعد المتعلقة بأمان المعالجة المراقب والمعالج بتنفيذ التدابير التقنية والتنظيمية المناسبة لمنع أي تدخل غير مصرح به في عمليات معالجة البيانات.
- يتم تحديد المستوى اللازم لأمن البيانات من خلال:
  - الخصائص الأمنية المتوفرة في السوق لأي نوع معين من المعالجة؛
  - التكاليف؛
  - المخاطر التي تشكلها معالجة البيانات على الحقوق والحريات الأساسية لأصحاب البيانات.
- إن ضمان سرية البيانات الشخصية هو جزء من مبدأ عام معترف به في اللائحة العامة لحماية البيانات.

[429] فريق عمل المادة 29 (2007)، وثيقة العمل المتعلقة بمعالجة البيانات الشخصية المتعلقة بالصحة في سجلات الصحة الإلكترونية (EHR)، WP 131، بروكسل، 15 فبراير 2007، انظر أيضاً اللائحة العامة لحماية البيانات، المادة 9 (3).

[430] اللائحة العامة لحماية البيانات، المادة 9 (2) (ز).

[431] فريق عمل المادة 29 (2007)، وثيقة العمل المتعلقة بمعالجة البيانات الشخصية المتعلقة بالصحة في سجلات الصحة الإلكترونية (EHR)، WP 131، بروكسل، 15 فبراير 2007.

[432] اللائحة العامة لحماية البيانات، المادة 9 (2) (ج) و(ط) و(ي).

[433] نفس المرجع السابق، المادة 9 (2) (ج) و9 (4).

بموجب كل من **قانون الاتحاد الأوروبي** و**قانون مجلس أوروبا**، يلتزم المراقبون بشكل عام بالشفافية والمساءلة عند معالجة البيانات الشخصية، وعلى وجه الخصوص، فيما يخص خروقات البيانات عند حدوثها. ففي حالة حدوث خروقات للبيانات الشخصية، يجب على المراقبين إخطار الهيئات الإشرافية، ما عدا في الحالات التي يكون فيها من غير المحتمل أن يؤدي الخرق إلى خطر على حقوق وحريات الأشخاص الطبيعيين. ويجب أيضاً إبلاغ أصحاب البيانات بشأن خرق البيانات الشخصية عندما يُحتمل أن يؤدي إلى مخاطر عالية على حقوق وحريات الأشخاص الطبيعيين.

## 1.2.4. عناصر أمن البيانات

وفقاً للمقتضيات ذات الصلة في **قانون الاتحاد الأوروبي**:

«مع مراعاة أحدث التطورات وتكاليف التنفيذ وطبيعة المعالجة ونطاقها وسياقها وأغراضها، فضلاً عن مخاطر ذات الاحتمالية والشدة المتغيرتين فيما يتعلق بحقوق وحريات الأشخاص الطبيعيين، يتعين على المراقب والمعالج تنفيذ التدابير التقنية والتنظيمية المناسبة لضمان مستوى الأمان المناسب للمخاطر [...].»[434]

تشمل هذه التدابير، من جملة أمور أخرى:

- استعمال اسم مستعار للبيانات الشخصية وتشفيرها؛[435]
- ضمان أن يحافظ نظام وخدمة المعالجة على السرية والسلامة والتوافر والمرونة؛[436]
- استرجاع توافر البيانات الشخصية والوصول إليها في حالة فقدان البيانات، في الوقت المناسب؛[437]
- وضع عملية لاختبار وتقييم فعالية التدابير لضمان أمن المعالجة.[438]

يشمل **قانون مجلس أوروبا** مقتضىً مماثلاً أيضاً:

«يجب على كل طرف أن ينص على أن المراقب، وعند الاقتضاء، المعالج، يتخذ تدابير أمنية مناسبة ضد المخاطر مثل الوصول إلى البيانات الشخصية أو إتلافها أو فقدانها أو استخدامها أو تعديلها أو الكشف عنها بشكل عرضي أو غير مصرح به.»[439]

بموجب **قانون الاتحاد الأوروبي** و**قانون مجلس أوروبا**، فإن خرق البيانات الذي قد يكون له أثر على حقوق وحريات الأفراد يُلزِم المراقب بإخطار الهيئة الإشرافية بذلك الخرق (انظر الجزء 4.2.3).

في كثير من الأحيان، هناك أيضاً معايير صناعية ووطنية ودولية تم تطويرها لمعالجة البيانات بشكل آمن. يُعد «ختم الخصوصية الأوروبي» (EuroPriSe)، على سبيل المثال، أحد مشاريع «شبكات الاتصالات عبر أوروبا» (eTEN) التابعة للاتحاد الأوروبي، والذي يستكشف إمكانيات اعتماد المنتجات، وخاصة البرمجيات، كوسائل لتسهيل الامتثال لقانون حماية البيانات الأوروبي. كما تم إنشاء «الوكالة الأوروبية لأمن الشبكات والمعلومات» (ENISA) لتعزيز قدرة الاتحاد الأوروبي والدول الأعضاء في الاتحاد الأوروبي ومجتمع الأعمال على منع مشاكل أمن الشبكات والمعلومات ومعالجتها والاستجابة لها.[440] وتنشر «الوكالة الأوروبية لأمن الشبكات والمعلومات» بانتظام تحليلات للتهديدات الأمنية الحالية ونصائح حول كيفية معالجتها.[441]

---

[434] نفس المرجع السابق، المادة 32 (1).

[435] نفس المرجع السابق، المادة 32 (1) (أ).

[436] نفس المرجع السابق، المادة 32 (1) (ب).

[437] نفس المرجع السابق، المادة 32 (1) (ج).

[438] نفس المرجع السابق، المادة 32 (1) (د).

[439] الاتفاقية 108 المحدثة، المادة 7 (1).

[440] اللائحة (الجماعة الأوروبية) رقم 526/2013 للبرلمان الأوروبي والمجلس المؤرخة في 21 مايو 2013 المتعلقة بوكالة الاتحاد الأوروبي لأمن الشبكات والمعلومات (ENISA) والملغية للائحة (الجماعة الأوروبية) 460/2004، الجريدة الرسمية L 165/2013041.

[441] على سبيل المثال، وكالة الاتحاد الأوروبي لأمن الشبكات والمعلومات (ENISA)، الأمن السيبراني ومرونة السيارات الذكية. ممارسات جيدة وتوصيات؛ وكالة الاتحاد الأوروبي لأمن الشبكات والمعلومات (2016) (ENISA)، أمن المدفوعات بواسطة المحمول والمحافظ الرقمية.

لا يتم تحقيق أمن البيانات فقط من خلال التوفر على المعدات المناسبة - أجهزة وبرمجيات. فذلك يتطلب أيضاً قواعد تنظيمية داخلية مناسبة. ومن الناحية المثالية، يُفترض أن تغطي هذه القواعد الداخلية الجوانب التالية:

- توفير المعلومات بانتظام لجميع الموظفين حول قواعد أمن البيانات والتزاماتهم بموجب قانون حماية البيانات، لا سيما فيما يتعلق بالتزامات السرية الخاصة بهم؛
- التوزيع الواضح للمسؤوليات والتحديد الواضح للكفاءات في مسائل معالجة البيانات، لا سيما فيما يتعلق بقرارات معالجة البيانات الشخصية ونقل البيانات إلى أطراف ثالثة أو لأصحاب البيانات؛
- استخدام البيانات الشخصية فقط وفقاً لتعليمات الشخص المختص أو وفقاً للقواعد الموضوعة بشكل عام؛
- حماية الوصول إلى المواقع والأجهزة والبرمجيات من طرف المراقب أو المعالج، بما في ذلك عمليات التحقق من التصريح بالوصول؛
- التأكد من أن تصاريح الوصول إلى البيانات الشخصية قد تم منحها من قبل الشخص المختص وأنها تتطلب تقديم الوثائق المناسبة؛
- البروتوكولات الآلية بشأن الوصول الإلكتروني إلى البيانات الشخصية وعمليات الفحص المنتظمة لهذه البروتوكولات من قبل المكتب الإشرافي الداخلي (وبالتالي ضرورة تسجيل جميع أنشطة معالجة البيانات)؛
- التوثيق الدقيق لأشكال الكشف الأخرى غير الوصول الآلي إلى البيانات، وذلك لإثبات عدم حدوث أي عمليات نقل غير قانونية للبيانات.

إن تزويد الموظفين بالتدريب والتعليم المناسبين في مجال أمن البيانات يُعد عنصراً مهماً كذلك ضمن الاحتياطات الأمنية الفعالة. ويجب أيضاً إرساء إجراءات التحقق لضمان ألّا تكون التدابير المناسبة موجودة على الورق فحسب، بل أن تُنفَّذ وتعطي نتيجة في الممارسة العملية أيضاً (مثل عمليات التدقيق الداخلية أو الخارجية).

تتضمن تدابير تحسين مستوى أمن المراقب أو المعالج وسائل مختلفة منها مسؤولي حماية البيانات الشخصية و دورات التثقيف الأمني للموظفين وعمليات التدقيق المنتظمة واختبارات الاختراق وأختام الجودة.

مثال: في قضية «إ. ضد فنلندا»،[442] لم تتمكن المدعية من إثبات أنه قد تم الوصول إلى سجلات الصحة الخاصة بها بطريقة غير مشروعة من قبل موظفين آخرين في المستشفى الذي كانت تعمل فيه. وبالتالي، رفضت المحاكم المحلية ادعاءها بانتهاك حقها في حماية البيانات. ولكن المحكمة الأوروبية لحقوق الإنسان خلصت إلى حدوث انتهاك للمادة 8 من الاتفاقية الأوروبية لحقوق الإنسان، حيث إن نظام تسجيل ملفات الصحة بالمستشفى «كان من النوع الذي لا يسمح بالتحقق من استخدامات سجلات المرضى بأثر رجعي لأنه يكشف فقط عن أحدث خمس ملفات تم الاطلاع عليها و أن هذه المعلومات تُحذف بمجرد إعادة الملف إلى الأرشيف». فبالنسبة للمحكمة، كان من الأمور الحاسمة أن نظام السجلات المعمول به في المستشفى لم يتماشى بوضوح مع المتطلبات القانونية الواردة في القانون المحلي، وهي حقيقة لم تعطها المحاكم المحلية الاعتبار الواجب.

وضع الاتحاد الأوروبي الأمر التوجيهي المتعلق بأمن الشبكات وأنظمة المعلومات،[443] والذي يُعد أول صك قانوني على مستوى الاتحاد الأوروبي بشأن الأمن السيبراني. ويهدف هذا الأمر التوجيهي إلى تحسين الأمن السيبراني على المستوى الوطني من ناحية، وزيادة مستوى التعاون داخل الاتحاد الأوروبي من ناحية أخرى. كما يفرض التزامات على مشغلي الخدمات الأساسية (بما في ذلك المشغلون في قطاعات الطاقة والصحة والمصارف والنقل والبنية التحتية الرقمية وما إلى ذلك) ومقدمي الخدمات الرقمية لإدارة المخاطر وضمان أمن شبكاتهم وأنظمة المعلومات الخاصة بهم والإبلاغ عن حوادث أمنية.

**الآفاق**

في سبتمبر 2017، اقترحت المفوضية الأوروبية مشروع لائحة تهدف إلى إصلاح تفويض «الوكالة الأوروبية لأمن الشبكات والمعلومات»، لتأخذ في الاعتبار الصلاحيات والمسؤوليات الجديدة للوكالة بموجب الأمر التوجيهي المتعلق بأمن الشبكات وأنظمة المعلومات. ويتمثل الهدف من اللائحة المقترحة في تطوير مهام «الوكالة الأوروبية لأمن الشبكات والمعلومات» وتعزيز دورها «كنقطة مرجعية في النظام البيئي للأمن

[442] المحكمة الأوروبية لحقوق الإنسان، قضية «إ. ضد فنلندا»، رقم 20511/03، 17 يوليو 2008.

[443] الأمر التوجيهي (الاتحاد الأوروبي) 2016/1148 للبرلمان الأوروبي والمجلس المؤرخ في 6 يوليو 2016 المتعلق بالتدابير من أجل مستوىً عالٍ ومشترك لأمن أنظمة الشبكات والمعلومات على امتداد الاتحاد، الجريدة الرسمية 194 L 2016 ،0J.

السيبراني في الاتحاد الأوروبي»،[444] ينبغي ألّا تخل اللائحة المقترحة بمبادئ اللائحة العامة لحماية البيانات، كما أنه من خلال توضيح العناصر الضرورية التي تتألف منها برامج إصدار شهادات التصديق الأوروبية في مجال الأمن السيبراني، ينبغي أن تعمل هذه اللائحة المقترحة أيضاً على تعزيز أمن البيانات الشخصية. بالتوازي مع ذلك، في سبتمبر 2017، اقترحت المفوضية الأوروبية مسودة لائحة تنفيذية تحدد العناصر التي يجب أن يأخذها مقدمو الخدمات الرقمية في الاعتبار لضمان أمن شبكاتهم وأنظمة المعلومات الخاصة بهم، كما هو مطلوب بموجب المادة 16 (8) من الأمر التوجيهي المتعلق بأمن الشبكات وأنظمة المعلومات. وقد كانت المناقشات حول هذين الاقتراحين جارية وقت صياغة هذا الدليل.

## 2.2.4. السرية

بموجب **قانون الاتحاد الأوروبي**، تقر اللائحة العامة لحماية البيانات بسرية البيانات الشخصية كجزء من مبدأ عام.[445] ويحتاج مقدمو خدمات الاتصالات الإلكترونية المتاحة للجمهور إلى ضمان السرية. كما أنهم ملزمون بالحفاظ على أمن خدماتهم.[446]

مثال: تلقت موظفة في شركة تأمين مكالمة هاتفية في مكان عملها من شخص يقول إنه عميل، ويطلب معلومات تتعلق بعقد التأمين الخاص به. يتطلب واجب الحفاظ على سرية بيانات العملاء أن تقوم الموظفة بتطبيق الحد الأدنى من الإجراءات الأمنية على الأقل قبل الكشف عن البيانات الشخصية. ويمكن القيام بذلك، على سبيل المثال، من خلال عرض إعادة المكالمة إلى رقم هاتف موثق في ملف العميل.

وفقاً للمادة 5 (1) (و)، يجب معالجة البيانات الشخصية بطريقة تضمن الأمن المناسب للبيانات الشخصية، بما في ذلك الحماية ضد المعالجة غير المصرح بها أو غير القانونية وضد الضياع أو الدمار أو التلف العرضيين، باستخدام التدابير التقنية أو التنظيمية المناسبة ("السلامة والسرية").

بموجب المادة 32، يجب على المراقب والمعالج تنفيذ التدابير التقنية والتنظيمية لضمان مستوىً عالٍ من الأمن. وتشمل هذه التدابير، من بين أمور أخرى، استخدام الأسماء المستعارة وتشفير البيانات الشخصية، والقدرة على ضمان السرية والسلامة والتوافر والمرونة المستمرة في المعالجة، وتقييم واختبار فعالية التدابير، والقدرة على استعادة المعالجة في حالة وقوع حادث مادي أو تقني. بالإضافة إلى ذلك، يمكن استخدام الالتزام بمدونة سلوك معتمدة أو بآلية شهادات تصديق معتمدة كعنصر لإثبات الامتثال لمبدأ السلامة والسرية. علاوة على ذلك، وفقًا للمادة 28 من اللائحة العامة لحماية البيانات، يجب أن ينص العقد المبرم بين المراقب والمعالج على أن المعالج يضمن أن الأشخاص المصرح لهم بمعالجة البيانات الشخصية قد التزموا بالسرية أو أنهم يخضعون لالتزام قانوني مناسب بالسرية.

لا يمتد واجب السرية ليشمل المواقف التي يطلع فيها على البيانات فرد بصفته الشخصية وليس كموظف يعمل لدى مراقب أو معالج. في هذه الحالة، لا تنطبق المادتان 32 و 28 من اللائحة العامة لحماية البيانات، حيث إن استخدام البيانات الشخصية من قبل الأفراد الخاصين يكون معفىً تماماً من اختصاص اللائحة عندما يقع هذا الاستخدام ضمن حدود ما يسمى بالإعفاء المنزلي.[447] ويعني هذا الإعفاء المنزلي استخدام البيانات الشخصية «من قبل شخص طبيعي في سياق نشاط شخصي أو منزلي بحت».[448] ومنذ صدور قرار محكمة العدل التابعة للاتحاد الأوروبي في قضية «بوديل لينداغفيست»،[449] أصبح من الواجب تفسير هذا الإعفاء بشكل ضيق، لا سيما فيما يتعلق بالكشف عن البيانات. وعلى وجه الخصوص، لا يمتد الإعفاء المنزلي ليشمل نشر البيانات الشخصية لعدد غير محدود من المستلمين على الإنترنت أو معالجة البيانات التي لها جوانب مهنية أو تجارية (لمزيد من التفاصيل حول القضية، انظر الأجزاء 2.1.2، 2.2.2 و 2.3.1).

تُعد «سرية الاتصالات» جانباً آخر من جوانب السرية، والتي تخضع لقاعدة التخصيص. وتتطلب القواعد الخاصة لضمان سرية الاتصالات الإلكترونية بموجب الأمر التوجيهي المتعلق بالخصوصية الإلكترونية من الدول الأعضاء منع أي أشخاص باستثناء المستخدمين، أو ليست لديه

[444] مقترح بشأن لائحة للبرلمان الأوروبي والمجلس بشأن وكالة الاتحاد الأوروبي لأمن الشبكات والمعلومات (ENISA)، «وكالة الاتحاد الأوروبي للأمن السيبراني»، والمَلغية للائحة (الاتحاد الأوروبي) 526/2013، والمتعلقة بشهادات الأمن السيبراني في مجال تكنولوجيا المعلومات والاتصال (قانون الأمن السيبراني)، 13 ،477(2017)COM سبتمبر 2017، ص. 6.

[445] اللائحة العامة لحماية البيانات، المادة 5 (1) (و).

[446] الأمر التوجيهي المتعلق بالخصوصية والاتصالات الإلكترونية، المادة 5 (1).

[447] اللائحة العامة لحماية البيانات، المادة 2 (2) (ج).

[448] نفس المرجع السابق.

[449] محكمة العدل التابعة للاتحاد الأوروبي، C-101/01، قضية الدعوى الجنائية في حق بوديل لينداغفيست، 6 نوفمبر 2003.

موافقة المستخدمين، من الاستماع أو التنصت أو التخزين أو أنواع أخرى من اعتراض الاتصالات أو مراقبتها هي والبيانات الوصفية المتعلقة بها.[450] ويجوز للقانون الوطني أن يجيز استثناءات من هذا المبدأ فقط لأسباب تتعلق بالأمن القومي أو الدفاع أو الوقاية أو الكشف عن الجرائم، وفقط إذا كانت هذه التدابير ضرورية ومتناسبة مع الأهداف المنشودة.[451] وسيتم تطبيق نفس القواعد بموجب لائحة الخصوصية الإلكترونية المستقبلية، ومع ذلك سيتم توسيع نطاق النص القانوني بشأن الخصوصية الإلكترونية من خدمات الاتصالات الإلكترونية المتاحة للجمهور ليشمل أيضاً الاتصالات التي تتم من خلال خدمات الاتصال المباشر عبر الإنترنت (مثل تطبيقات الهاتف المحمول).

بموجب **قانون مجلس أوروبا**، فإن الالتزام بالسرية متضمن في مفهوم أمن البيانات في المادة 7 (1) من الاتفاقية 108 المحدثة التي تتناول أمن البيانات.

بالنسبة للمعالجين، تعني السرية أنه لا يجوز لهم الكشف عن البيانات لأطراف ثالثة أو مستلمين آخرين دون إذن. وبالنسبة للموظفين لدى مراقب أو معالج، تتطلب السرية ألا يستخدموا البيانات الشخصية إلا وفقاً لتعليمات رؤسائهم المختصين.

يجب تضمين التزام السرية في أي عقد بين المراقبين ومعالجيهم. بالإضافة إلى ذلك، يتعين على المراقبين والمعالجين اتخاذ تدابير محددة لإرساء واجب قانوني يتعلق بالسرية لموظفيهم، والذي يتم تحقيقه عادة من خلال تضمين بنود السرية في عقد العمل الخاص بالموظف.

يعاقب القانون الجنائي على انتهاك واجب السرية المهني في العديد من الدول الأعضاء في الاتحاد الأوروبي والأطراف في الاتفاقية 108.

## 3.2.4. إشعارات خرق البيانات الشخصية

يشير خرق البيانات الشخصية إلى خرق أمني يؤدي إلى التدمير أو الضياع أو التغيير أو الكشف غير المصرح به أو الوصول إلى البيانات الشخصية المعالجة بشكل عرضي أو غير قانوني.[452] وفي حين أن التقنيات الجديدة، مثل التشفير، توفر الآن المزيد من الإمكانيات لضمان أمن المعالجة، ما تزال خروقات البيانات ظاهرة شائعة. وتتراوح أسباب خرق البيانات بين الأخطاء العرضية التي يرتكبها الأشخاص العاملون داخل مؤسسة ما إلى حد التهديدات الخارجية على يد المخترقين مثلاً أو المنظمات الإجرامية السيبرانية.

من الوارد أن يكون لخرق البيانات بالغ الضرر على حقوق الخصوصية وحماية البيانات بالنسبة للأفراد الذين يفقدون السيطرة على بياناتهم الشخصية نتيجة لهذا الخرق. قد تؤدي مثل هذه الخروقات إلى سرقة الهوية أو الاحتيال أو الخسارة المالية أو الأضرار المادية وفقدان سرية البيانات الشخصية المحمية بالسرية المهنية والإضرار بسمعة صاحب البيانات. ويوضح فريق عمل المادة 29 في إرشاداته بشأن إشعار خرق البيانات الشخصية بموجب اللائحة 2016/679 أن الخروقات قد يكون لها ثلاثة أنواع من الأثر على البيانات الشخصية: الكشف و / أو الضياع و / أو التغيير.[453] وبالإضافة إلى الالتزام باتخاذ تدابير لضمان أمن المعالجة، كما هو موضح في الجزء 2.4، فإنه من المهم بنفس القدر التأكد من أنه عند حدوث خروقات، يقوم المراقبون بمعالجتها بطريقة مناسبة وفي الوقت المناسب.

يُذكر أنه غالباً ما لا تكون الهيئات الإشرافية ولا الأفراد على دراية بحدوث خرق للبيانات وذلك يمنع الأفراد من اتخاذ الإجراءات الكفيلة بحماية أنفسهم من عواقبه السيئة. وتأييداً لحقوق الأفراد وللتقليل من أثر خروقات البيانات، يفرض **الاتحاد الأوروبي ومجلس أوروبا** على المراقبين شرط الإشعار في ظروف معينة.

فبموجب **اتفاقية مجلس أوروبا** المحدثة 108، يتعين على الأطراف المتعاقدة، على الأقل، أن تشترط على المراقبين إشعار الهيئة الإشرافية المختصة بخروقات البيانات التي قد تشكل تدخلاً كبيرا في حقوق أصحاب البيانات. وينبغي لذلك الإشعار أن يُنجز 'دون تأخير'.[454]

---

[450] الأمر التوجيهي المتعلق الخصوصية والاتصالات الإلكترونية، المادة 5 (1).

[451] نفس المرجع السابق، المادة 15 (1).

[452] اللائحة العامة لحماية البيانات، المادة 4 (12)؛ انظر أيضاً فريق عمل المادة 29 (2017)، مبادئ توجيهية بشأن إشعار خرق البيانات الشخصية بموجب اللائحة 2016/679، WP 250، 3 أكتوبر 2017، ص. 8.

فريق عمل المادة 29 (2017)، مبادئ توجيهية بشأن إشعار خرق البيانات الشخصية بموجب اللائحة 2016/679، 3 WP 250 أكتوبر 2017، ص. 6.

[453] الاتفاقية المحدثة 108، المادة 7 (2)؛ التقرير التفسيري الملحق بالاتفاقية المحدثة 108، الفقرات 64-66.

[454] اللائحة العامة لحماية البيانات، المادتان 33 و34.

يضع **قانون الاتحاد الأوروبي** نظاماً مفصلاً ينظم توقيت الإشعارات ومحتوياتها.[455] واستناداً إلى ذلك النظام، يجب على المراقبين إشعار الهيئات الإشرافية ببعض خروقات البيانات دون تأخير لا موجب له، و حيث أمكن، في غضون 72 ساعة من اللحظة التي يعلمون فيها بحدوث الخرق. وإذا تجاوزوا الإطار الزمني المحدد في 72 ساعة، يحتاج الإشعار إلى إرفاقه بتفسير للتأخير. ويُعفى المراقبون من شرط الإشعار فقط عندما يستطيعون إثبات أن خرق البيانات من المرجح أن لا يعرض للخطر حقوق الأفراد المعنيين وحرياتهم.

تحدد اللائحة القدر الأدنى من المعلومات التي يجب إدراجها في الإشعار لتمكين الهيئة الإشرافية من اتخاذ الإجراءات الضرورية.[456] ويجب تضمين الإشعار، على الأقل، وصفاً لطبيعة خرق البيانات وللأعداد التقريبية من أصحاب البيانات المتضررين وفئاتهم، ووصفاً للعواقب الممكنة لذلك الخرق وللتدابير التي نفذها المراقب لمعالجة عواقبه والتخفيف من شدتها. علاوة على ذلك، تنبغي إتاحة اسم وبيانات الاتصال الخاصة بالمسؤول عن حماية البيانات أو جهة اتصال أخرى لتمكين الهيئة الإشرافية المختصة من الحصول على مزيد من المعلومات عند الاقتضاء. إذا كان خرق للبيانات من المرجح أن يُعرض حقوق الأفراد وحرياتهم لمخاطر شديدة، يجب على المراقبين أن يخبروا هؤلاء الأفراد (أصحاب البيانات) بالخرق الذي وقع دون تأخير لا مبرر له.[457] ويجب أن يصاغ الإخبار الموجه إلى أصحاب البيانات، والذي يشتمل على وصف لخرق البيانات، بلغة واضحة ومفهومة، وأن يتضمن معلومات مشابهة لتلك المطلوبة في الإشعارات الموجهة إلى الهيئات الإشرافية. في ظروف معينة، قد يُعفى المراقبون من واجب إشعار أصحاب البيانات بتلك الخروقات، وتنطبق الإعفاءات عندما يكون المراقب قد نفذ التدابير الحمائية التقنية والتنظيمية المناسبة، وحينما تكون تلك التدابير قد طُبقت على البيانات الشخصية المتضررة من الخرق، لا سيما منها تلك التي تجعل البيانات الشخصية غير مفهومة بالنسبة لأي شخص غير مرخص له الولوج إليها، مثل التشفير. إن الإجراءات التي يتخذها المراقب بعد الخرق للتأكد أن الضرر بحقوق أصحاب البيانات لن يتحقق قد تعفيه أيضاً من إشعار أصحاب البيانات. وأخيراً، إذا كان الإشعار يستدعي مجهوداً غير متناسب من جانب المراقب، يمكن إخبار أصحاب البيانات بالخرق الذي وقع من خلال وسائل أخرى مثل بلاغ عام موجه للجمهور أو تدابير مشابهة.[458]

إن واجب إخطار الهيئات الإشرافية وأصحاب البيانات بوقوع خروقات للبيانات موجه إلى المراقبين، غير أن خروقات البيانات قد تحدث بغض النظر عما إذا كان المراقب أو المعالج هو من نفذ المعالجة. ولذلك السبب، يُعد أمراً ضرورياً التيقن من أن المعالجين يُطلب منهم أيضاً الإبلاغ عن خروقات البيانات. في هذه الحالة، يجب على المعالجين إخبار المراقب بخروقات البيانات دون تأخير لا موجب له.[459] ويكون المراقب آنذاك مسؤولاً عن إشعار الهيئات الإشرافية وأصحاب البيانات المتضررين، شريطة مراعاة القواعد والإطار الزمني السالف الذكر.

## 3.4. قواعد المساءلة وتعزيز الامتثال

### النقاط الرئيسية

- لضمان المساءلة في مجال معالجة البيانات الشخصية، يجب على المراقبين والمعالجين الاحتفاظ بسجلات لأنشطة المعالجة التي يقمون بها في نطاق مسؤوليتهم وتزويد الهيئات الإشرافية بها عندما تُطلب منهم.
- تنص اللائحة العامة لحماية البيانات على عدة صكوك لتعزيز الامتثال:
  - تعيين المسؤولين عن حماية البيانات في حالات معينة؛
  - إجراء تقييم الأثر قبل الشروع في أنشطة المعالجة التي من المرجح أن تعرض حقوق الأفراد وحرياتهم لمخاطر شديدة؛
  - التشاور المسبق مع الهيئة الإشرافية المعنية إذا كان تقييم الأثر يدل على أن المعالجة تمثل مخاطر لا يمكن التخفيف من شدتها؛
  - مدونات السلوك خاصة بالمراقبين والمعالجين تحدد تطبيق اللائحة في مختلف قطاعات المعالجة؛
  - إصدار شهادات التصديق، والأختام، والعلامات.
- يقترح قانون مجلس أوروبا صكوكاً مشابهة لتعزيز الامتثال في الاتفاقية المحدثة 108.

[455] نفس المرجع السابق، المادة 33 (3).
[457] نفس المرجع السابق، المادة 34.
[458] نفس المرجع السابق، المادة 34 (3) (ج).
[459] نفس المرجع السابق، المادة 33 (2).

يكتسي مبدأ المساءلة أهمية خاصة في سبيل ضمان تنفيذ قواعد حماية البيانات في أوروبا. ويُعد المراقب مسؤولاً عن الامتثال لقواعد حماية البيانات، ويتعين عليه أن يكون قادراً على إثبات ذلك. ولا ينبغي انتظار حدوث خرق للبيانات لتفعيل مبدأ المساءلة، ذلك أن المراقبين لديهم التزام استباقي باتباع سياسات ملائمة في إدارة البيانات خلال جميع مراحل معالجة البيانات. ويشترط قانون حماية البيانات الأوروبي على المراقبين تنفيذ التدابير التقنية والتنظيمية لضمان تنفيذ المعالجة وفقاً للقانون مع القدرة على إثبات ذلك. وتشمل تلك التدابير تعيين المسؤولين عن حماية البيانات، والاحتفاظ بالسجلات والوثائق ذات الصلة بالمعالجة، وإجراء تقييمات الأثر على الخصوصية.

## 1.3.4. المسؤولون عن حماية البيانات

إن المسؤولين عن حماية البيانات (DPOs) هم أشخاص يسدون المشورة بشأن الامتثال لقواعد حماية البيانات في المؤسسات التي تتعهد بمعالجة البيانات، وهم يُعدون 'الركن الأساسي للمساءلة' لأنهم ييسرون الامتثال، في حين أنهم يتصرفون أيضا بصفتهم وسطاء بين الهيئات الإشرافية وأصحاب البيانات والمؤسسة التي عينتهم.

**بموجب قانون مجلس أوروبا**، تُحمل المادة 10 (1) من الاتفاقية المحدثة 108 مسؤولية المحاسبة العامة للمراقبين والمعالجين. ويقتضي ذلك من المراقبين والمعالجين اتخاذ جميع التدابير المناسبة للامتثال لقواعد حماية البيانات المنصوص عليها في الاتفاقية، والقدرة على إثبات امتثال المعالجة التي تتم في نطاق مراقبتهم لمقتضيات الاتفاقية. وعلى الرغم من أن الاتفاقية لا تحدد التدابير الملموسة التي ينبغي للمراقبين والمعالجين اعتمادها، يشير التقرير التفسيري الملحق بالاتفاقية المحدثة 108 إلى أن تعيين مسؤول عن حماية البيانات يُعتبر من بين التدابير الممكن اعتمادها للمساعدة على إثبات الامتثال. وينبغي تزويد المسؤولين عن حماية البيانات بجميع الوسائل الضرورية للقيام بالمهام الموكلة إليهم.[460]

خلافاً لقانون مجلس أوروبا، فإنه **في الاتحاد الأوروبي** لا يخضع تعيين المسؤول عن حماية البيانات دائماً لتقدير المراقبين والمعالجين لكنه يكون ضرورياً في ظروف معينة. تقر اللائحة العامة لحماية البيانات بالدور الرئيسي الذي يقوم به المسؤول عن حماية البيانات في نظام الحكامة الجديد وتشتمل على مقتضيات مفصلة تتعلق بالتعيين والمنصب والواجبات والمهام.[461]

تُلزم اللائحة العامة لحماية البيانات بضرورة تعيين مسؤول عن حماية البيانات في ثلاث حالات محددة: عند تنفيذ سلطة أو هيئة عامة لعملية المعالجة؛ وعندما تكون الأنشطة الأساسية التي يقوم بها المراقب أو المعالج تشمل عمليات المعالجة التي تتطلب المراقبة المنتظمة والمنهجية لأصحاب البيانات على نطاق واسع أو عندما تكون الأنشطة الأساسية تشمل معالجة واسعة النطاق لفئات خاصة من البيانات أو البيانات الشخصية المتعلقة بالإدانات والجرائم الجنائية.[462] على الرغم من أن مصطلحات مثل 'المراقبة المنهجية على نطاق واسع' و'الأنشطة الأساسية' لم يتم تعريفها في اللائحة، أصدر فريق عمل المادة 29 مبادئ توجيهية بخصوص كيفية تفسيرها.[463]

مثال: من المرجح أن تُحتسب شركات وسائل التواصل الاجتماعي ومحركات البحث في عِداد المراقبين الذين تستدعي عمليات المعالجة التي يقومون بها رصداً منهجياً ومنتظماً لأصحاب البيانات على نطاق واسع. ويقوم النموذج التجاري لتلك الشركات على معالجة كميات ضخمة من البيانات الشخصية، وهي تحقق عائدات كبيرة من خلال تقديم خدمات الإعلانات المستهدِفة ومن خلال السماح للشركات بوضع إعلاناتها على المواقع. وتُعد الإعلانات المستهدِفة طريقة من طرق وضع الإعلانات استناداً إلى خصائص ديموغرافية وإلى سلوك المستهلك أو سجله الشرائي، ولذلك فإنها تتطلب مراقبة منهجية للعادات والسلوكات الإلكترونية لأصحاب البيانات.

مثال: يُعد المستشفى وشركة التأمين الصحية مثالين نموذجيين من المراقبين الذين تشتمل أنشطتهم على المعالجة الواسعة النطاق لفئات خاصة من البيانات الشخصية. وتشكل البيانات التي تكشف عن معلومات تتعلق بصحة الفرد فئات خاصة من البيانات بمقتضى كل من قانون مجلس أوروبا وقانون الاتحاد الأوروبي، ولذلك فإنها تستحق حماية معززة. ويقر قانون الاتحاد الأوروبي أيضاً بكون البيانات الجينية و البيومترية هي بدورها فئات خاصة من البيانات. وما دامت المؤسسات الطبية وشركات التأمين تعالج تلك البيانات على نطاق واسع، فإنها مطالبة بموجب اللائحة العامة لحماية البيانات بتعيين مسؤول عن حماية البيانات.

[460] التقرير التفسيري الملحق بالاتفاقية المحدثة 108، الفقرة 87.

[461] اللائحة العامة لحماية البيانات، المواد 37-39.

[462] نفس المرجع السابق، المادة 37 (1).

[463] لفريق عمل المادة 29 (2017)، المبادئ التوجيهية المتعلقة بالمسؤولين عن حماية البيانات (WP243، DPOs) المراجعة رقم 01، كما تمت مراجعتها واعتمادها آخر مرة في 05 أبريل 2017.

إضافةً إلى ذلك، تنص المادة 37 (4) من اللائحة العامة لحماية البيانات على أنه في حالات عدا الحالات الثلاث الإلزامية بموجب المادة 37 (1) يجوز للمراقب أو للمعالج أو للجمعيات وباقي الجهات التي تمثل فئات من المراقبين أو المعالجين - بل ويتوجب عليهم ذلك إن كان منصوصاً عليه بمقتضى قانون الاتحاد الأوروبي أو قانون إحدى دوله الأعضاء - تعيين مسؤول عن حماية البيانات.

لا تكون جميع المنظمات الأخرى ملزمة قانوناً بتعيين مسؤول عن حماية البيانات. غير أن اللائحة العامة لحماية البيانات تنص على أن المراقبين والمعالجين يجوز لهم تعيين مسؤول عن حماية البيانات طوعاً، فيما تسمح أيضاً للدول الأعضاء بجعل ذلك التعيين ضرورياً بالنسبة لأنواع أخرى من المنظمات عدا تلك المنصوص عليها في اللائحة.[464]

فور تعيين المراقب للمسؤول عن حماية البيانات، يجب عليه أن يتحقق من أنه «يشارك، بطريقة سليمة وفي الوقت المناسب، في جميع القضايا التي تتعلق بحماية البيانات الشخصية» داخل المؤسسة.[465] على سبيل المثال، ينبغي للمسؤولين عن حماية البيانات أن يشاركوا في إسداء المشورة بشأن إجراء تقييمات الأثر على حماية البيانات، وفي إنشاء سجلات أنشطة المعالجة والاحتفاظ بها في المؤسسة. لتمكين المسؤولين عن حماية البيانات من القيام بمهامهم بفعالية، يجب على المراقبين والمعالجين أن يزودوهم بالموارد الضرورية، بما في ذلك الموارد المالية، والبنى التحتية والمعدات. وتشمل المعدات الإضافية تزويد المسؤولين عن حماية البيانات بالوقت الكافي للقيام بوظائفهم والتدريب المستمر لتمكينهم من تطوير خبرتهم ومسايرة تطورات قانون حماية البيانات.[466]

تحدد اللائحة العامة لحماية البيانات بعضاً من الضمانات الأساسية لتضمن تصرف المسؤولين عن حماية البيانات بطريقة مستقلة. يجب على المراقبين والمعالجين أن يثبقنوا من عدم تلقي المسؤولين عن حماية البيانات، عند ممارسة مهامهم المتعلقة بحماية البيانات، لأي تعليمات من الشركة، بما في ذلك الأشخاص الذين يوجدون في أعلى المستويات الإدارية. علاوة على ذلك، لا يجب فصلهم أو عقابهم إطلاقاً لأداء مهامهم.[467] خذ، على سبيل المثال، حالة ينصح فيها المسؤول عن حماية البيانات المراقب أو المعالج بإجراء تقييم الأثر على حماية البيانات لأنه يرى أنه من المرجح أن تفضي المعالجة إلى تعريض أصحاب البيانات لخطر كبير. لا تتفق الشركة مع نصائح المسؤول عن حماية البيانات، ولا تعتقد أنها تستند إلى أساس سليم ولذلك لا تقرر المضي قدماً في إجراء التقييم. ويمكن للشركة أن تتجاهل النصائح لكن لا يمكن لها أن تفصل المسؤول عن حماية البيانات أو تعاقبه لتزويدها بها.

وأخيراً، فقد فصَّلت المادة 39 من اللائحة العامة لحماية البيانات في مهام وواجبات المسؤولين عن حماية البيانات. ويشمل ذلك متطلبات إخبار وإحاطة الشركات والموظفين الذين ينفذون المعالجة بالتزاماتهم وفقاً للتشريعات ورصد الامتثال لقواعد الاتحاد الأوروبي والقواعد الوطنية المتعلقة بحماية البيانات، من خلال إجراء عمليات التدقيق وتدريب الموظفين المشاركين في عمليات المعالجة. ويجب على المسؤولين عن حماية البيانات التعاون مع الهيئة الإشرافية والتصرف بصفتهم جهة الاتصال مع هذه الأخيرة حول الشؤون المرتبطة بمعالجة البيانات مثل خرق البيانات.

فيما يتعلق بالبيانات الشخصية التي تتناولها مؤسسات الاتحاد الأوروبي وهيئاته، تنص اللائحة 45/2001 على أنه يجب على كل مؤسسة وهيئة تابعة للاتحاد الأوروبي تعيين مسؤول عن حماية البيانات. ويعهد إلى المسؤول عن حماية البيانات بضمان تطبيق مقتضيات اللائحة تطبيقاً صحيحاً داخل مؤسسات الاتحاد الأوروبي وهيئاته وإخبار أصحاب البيانات والمراقبين بحقوقهم وواجباتهم.[468] ويتحمل أيضاً مسؤولية الاستجابة للطلبات الواردة من المشرف الأوروبي على حماية البيانات والتعاون معه عند الاقتضاء. وعلى غرار اللائحة العامة لحماية البيانات، تتضمن اللائحة 45/2001 مقتضيات بشأن استقلالية المسؤولين عن حماية البيانات في القيام بمهامهم، والحاجة إلى تزويدهم بالموارد والكفاءات الضرورية.[469] ويجب إشعار المسؤولين عن حماية البيانات قبل قيام مؤسسة أو هيئة تابعة للاتحاد الأوروبي (أو قيام إحدى الإدارات أو الأقسام داخلها) بأي عملية من عمليات المعالجة ويجب عليهم الاحتفاظ بسجل لجميع عمليات المعالجة التي تم الإشعار بها.[470]

---

[464] اللائحة العامة لحماية البيانات، المادة 37 (3) و(4).

[465] نفس المرجع السابق، المادة 38 (1).

[466] فريق عمل المادة 29 (2017)، المبادئ التوجيهية المتعلقة بالمسؤولين عن حماية البيانات (DPOs)، WP 243 المراجعة رقم 01، كما تمت مراجعتها واعتمادها آخر مرة في 05 أبريل 2017، الفقرة 1.3.

[467] اللائحة العامة لحماية البيانات، المادة 38 (2) و(3).

[468] إطلع على المادة 24 (1) من لائحة المجلس (الجماعة الأوروبية) رقم 45/2001 بخصوص القائمة الكاملة بمهام المسؤولين عن حماية البيانات.

[469] توصية المجلس (الجماعة الأوروبية) رقم 45/2001، المادة 24 (6) و(7).

[470] نفس المرجع السابق، المادتان 25 و26.

## 2.3.4. سجلات معالجة البيانات

للتمكن من إثبات الامتثال وللخضوع للمساءلة، تكون الشركات ملزمة قانوناً بتوثيق أنشطتها وتسجيلها، ومن بين الأمثلة على ذلك قانون الضرائب ومراجعة الحسابات التي تشترط على جميع الشركات الاحتفاظ بوثائق وسجلات مستفيضة. ويُعد مهماً أيضاً تحديد مقتضيات مماثلة في مجالات أخرى من القانون، لا سيما قانون حماية البيانات، لأن الاحتفاظ بالسجلات طريقة مهمة لتيسير الامتثال لقواعد حماية البيانات. ولذلك، ينص **قانون الاتحاد الأوروبي** على أن المراقبين، أو ممثليهم، يجب عليهم الاحتفاظ بسجل لأنشطة المعالجة التي يقومون بها في نطاق مسؤوليتهم.[471] ويُقصد بذلك الالتزام ضمان توفر السلطات الإشرفية، عند الاقتضاء، على الوثائق الضرورية لتمكينها من تأكيد قانونية المعالجة.

تشتمل المعلومات التي يتعين توثيقها على ما يلي:

- اسم وبيانات الاتصال الخاصة بكل من المراقب والمراقب المشترك وممثل المراقب والمسؤول عن حماية البيانات، حيثما أمكن؛
- وأغراض المعالجة؛
- ووصفاً لفئات أصحاب البيانات ولفئات البيانات الشخصية المتعلقة بالمعالجة؛
- ومعلومات عن فئات المستلمين الذين كُشف لهم، أو سيُكشف لهم، عن البيانات؛
- معلومات عما إذا كانت عمليات نقل البيانات الشخصية إلى بلدان ثالثة أو منظمات دولية قد تمت، أو ستتم؛
- وحيثما أمكن، الآجال المتوقعة لحذف مختلف الفئات من البيانات الشخصية، بالإضافة إلى لمحة عامة إلى التدابير التقنية التي تم اعتمادها لضمان أمن المعالجة.[472]

لا يتعلق الالتزام بالاحتفاظ بسجلات لأنشطة المعالجة بالمراقبين فحسب بموجب اللائحة العامة لحماية البيانات، وإنما أيضاً بالمعالجين. ويُعد ذلك تطوراً مهماً لأنه، قبل اعتماد اللائحة، شملت التزامات المعالج في المقام الأول العقد المبرم بين المراقب والمعالج. وتم التنصيص حالياً مباشرة على التزامهم بالاحتفاظ بالسجلات بموجب القانون.

تنص اللائحة العامة لحماية البيانات على استثناء من ذلك الالتزام. ولا ينطبق شرط الاحتفاظ بالسجلات على مؤسسة أو منظمة (معالجة أو مراقبة) توظف أقل من 250 شخصاً. إلا أن الاستثناء يخضع لمقتضيات تشترط عدم قيام المؤسسة المعنية بمعالجة من المحتمل أن تفضي إلى تهديد حقوق أصحاب البيانات وحرياتهم، والقيام بالمعالجة بطريقة عرضية فحسب و أن لا تشمل فئات خاصة من البيانات كما هو مشار إليه في المادة 9 (1) أو البيانات الشخصية المتعلقة بالإدانات أو الجرائم الجنائية المشار إليها في المادة 10.

إن الاحتفاظ بسجلات أنشطة المعالجة ينبغي أن يُمكِّن المراقبين والمعالجين من إثبات امتثالهم للائحة، كما ينبغي له أن يُمكِّن الهيئات الإشرافية من رصد مشروعية المعالجة. وعندما تطلب هيئة إشرافية الاطلاع على تلك السجلات، يكون من المفروض على المراقبين والمعالجين أن يبدوا روح التعاون وأن يضعوها رهن إشارتها.

## 3.3.4. تقييم الأثر على حماية البيانات والتشاور المسبق

تمثل عمليات المعالجة بعض الأخطار على حقوق الأفراد. فقد تضيع البيانات الشخصية، أو تُكشف لأطراف غير مرخص لها أو تُعالج بطريقة غير قانونية. بطبيعة الحال، تختلف الأخطار باختلاف طبيعة المعالجة ونطاقها. وتنطوي العمليات المتعلقة بمعالجة البيانات الحساسة على نطاق واسع على درجة أعلى بكثير من الخطر على أصحاب البيانات مقارنة بالأخطار الممكنة عندما تعالج شركة صغيرة عناوين موظفيها أو أرقام الهواتف الشخصية الخاصة بهم.

مع ظهور التكنولوجيات الجديدة وتزايد تعقد المعالجة، يجب على المراقبين التصدي لتلك الأخطار بتدارس الأثر المحتمل للمعالجة المزمع القيام بها قبل الشروع في عملية المعالجة. وذلك يمكن المنظمات من تحديد الأخطار والتصدي لها والتقليل منها بطريقة لائقة مسبقاً، ما يحد بشكل كبير من احتمالية حدوث تأثير سيء على الأفراد نتيجة للمعالجة.

[471] اللائحة العامة لحماية البيانات، المادة 30.
[472] نفس المرجع السابق، المادة 30 (1).
[473] اللائحة العامة لحماية البيانات، الديباجة، الحيثية 75.
[474] نفس المرجع السابق، المادة 35 (4) و (5).

ينص كل من **قانون مجلس أوروبا وقانون الاتحاد الأوروبي** على تقييمات الأثر على حماية البيانات. في الإطار القانوني لمجلس أوروبا، تقتضي المادة 10 (2) من الاتفاقية المحدثة 108 من الأطراف المتعاقدة ضمان أن المراقبين والمعالجين «يتدارسون الأثر المحتمل للمعالجة المزمع القيام بها على حقوق أصحاب البيانات وحرياتهم الأساسية قبل الشروع في تلك المعالجة» ويسعون، عقب التقييم، إلى تصميم المعالجة بما يقي من الأخطار المرتبطة بالمعالجة والتقليل منها إلى أدنى حد.

يفرض قانون الاتحاد الأوروبي التزاماً مشابهاً وأكثر تفصيلاً على المراقبين الذين يقعون ضمن نطاق اللائحة العامة لحماية البيانات. وتنص المادة 35 على وجوب إجراء تقييم الأثر عندما يكون من المحتمل أن تفضي المعالجة إلى خطر كبير على حقوق الأفراد وحرياتهم. لا تحدد اللائحة كيفية تقييم احتمالية حدوث الخطر لكنها، بدلاً عن ذلك، تدل على ماهية تلك الأخطار.[473] وتتضمن اللائحة قائمة بعمليات المعالجة التي تُعد خطراً كبيراً والتي تستوجب تقييماً مسبقاً للأثر بصورة خاصة، وهي الحالات التالية:

- عندما تُعالج البيانات الشخصية لغرض اتخاذ قرارات متعلقة بالأشخاص الطبيعيين، عقب أي تقييم منهجي واسع النطاق للجوانب الشخصية المتعلقة بالأفراد (التنميط)؛
- وعندما تُعالج البيانات الحساسة أو البيانات الشخصية المتعلقة بالإدانات والجرائم الجنائية على نطاق واسع؛
- وعندما تتعلق المعالجة بالمراقبة الواسعة النطاق والمنهجية للأماكن العامة.

يتعين على الهيئات الإشرافية اعتماد ونشر قائمة بنوع عمليات المعالجة التي تحتاج إلى الخضوع لتقييمات الأثر. وقد تنشئ أيضاً قائمة بعمليات المعالجة التي تُعفى من ذلك الالتزام.[474]

عندما يكون تقييم الأثر مطلوباً، يجب على المراقبين تقييم ضرورة المعالجة وتناسبها والأخطار الممكنة على حقوق الأفراد. ويجب أن يحتوي تقييم الأثر أيضاً على التدابير الأمنية المخطط لها للتصدي للأخطار التي تم تحديدها. لإنشاء القوائم، يُطلب من الهيئات الإشرافية التابعة للدول الأعضاء التعاون بعضها مع بعض ومع مجلس حماية البيانات الأوروبي. سيضمن ذلك اتباع مقاربة متسقة في جميع أنحاء الاتحاد الأوروبي فيما يخص تلك العمليات التي تتطلب تقييم الأثر وسيواجه المراقبون شروطاً مشابهة بغض النظر عن موقعهم.

إذا بدا، عقب تقييم الأثر، أن المعالجة ستفضي إلى حدوث خطر كبير على حقوق الأفراد ولم تُعتمد تدابير للتقليل من الخطر، يجب على المراقب أن يتشاور مع الهيئة الإشرافية قبل الشروع في عملية المعالجة.[475]

أصدر فريق عمل المادة 29 مبادئ توجيهية حول تقييمات الأثر على حماية البيانات وكيفية تحديد ما إذا كانت المعالجة من المحتمل أن تفضي إلى خطر كبير أم لا.[476] وضع فريق العمل تسعة معايير للمساعدة على تحديد ما إذا كان تقييم الأثر على حماية البيانات مطلوباً في حالة معينة:[477] (1) التقييم أو التنقيط؛ و(2) اتخاذ قرارات آلية ذات مفعول قانوني أو مفعول وازن مشابه؛ و(3) الرصد المنهجي؛ و(4) البيانات الحساسة؛ و(5) البيانات التي تُعالج على نطاق واسع؛ و(6) مجموعات البيانات التي تم التوليف بينها ودمجها مع بعضها بعضاً؛ و(7) البيانات المتعلقة بأشخاص في وضعية هشة؛ و(8) تطبيق مبتكر أو استخدام للحلول التكنولوجية أو التنظيمية؛ و(9) عندما «تمنع المعالجة في حد ذاتها أصحاب البيانات من ممارسة حق، أو الاستفادة من خدمة أو عقد». واعتمد فريق عمل المادة 29 القاعدة العامة التي تقول بأن عمليات المعالجة التي تستوفي أقل من معيارين تمثل مستويات أدنى من الخطر ولا تتطلب تقييم حماية البيانات، في حين أن البيانات التي تستوفي معيارين أو أكثر ستتطلب ذلك التقييم. في الحالات التي لا يتضح فيها ما إذا كان تقييم الأثر على البيانات مطلوباً، يوصي فريق عمل المادة 29 بإجراء ذلك التقييم لأنه يُعد «أداة مفيدة يستعين بها مراقبو البيانات على الامتثال لقانون حماية البيانات».[478] عندما يتم اعتماد تكنولوجيا جديدة لمعالجة البيانات، يكون من المهم أن يتم إجراء تقييم الأثر على حماية البيانات.[479]

---

[475] نفس المرجع السابق، المادة 36 (1)؛ فريق عمل المادة 29 (2017)، المبادئ التوجيهية المتعلقة بتقييم الأثر على حماية البيانات (DPIA) والتي تحدد ما إذا كانت المعالجة «من المحتمل أن تفضي إلى خطر كبير» بالنسبة لأغراض اللائحة 2016/679، WP 248 المراجعة رقم 01، بروكسيل، 04 أكتوبر 2017.

[476] فريق عمل المادة 29 (2017)، المبادئ التوجيهية المتعلقة بتقييم الأثر على حماية البيانات (DPIA) والتي تحدد ما إذا كانت المعالجة «من المحتمل أن تفضي إلى خطر كبير» بالنسبة لأغراض اللائحة 2016/679، WP 248 المراجعة رقم 01، بروكسيل، 04 أكتوبر 2017.

[477] نفس المرجع السابق،الصفحات 9-11.

[478] نفس المرجع السابق، الصفحة 9.

[479] نفس المرجع السابق.

## 4.3.4. مدونات السلوك

يراد من مدونات (قواعد) السلوك استخدامها في عدة قطاعات لبيان وتحديد تطبيق اللائحة العامة لحماية البيانات في قطاعاتها المعينة. فيما يخص مراقبي ومعالجي البيانات الشخصية، فإن إيجاد تلك القواعد قد يحسن الامتثال ويعزز تنفيذ قواعد الاتحاد الأوروبي لحماية البيانات على نحو ملحوظ. وستشجع خبرة أعضاء القطاع على إيجاد حلول عملية و، بالتالي، من المرجح اتباعها. بالإقرار بأهمية تلك القواعد في التطبيق الفعال لقانون حماية البيانات، تدعو اللائحة العامة لحماية البيانات الدول الأعضاء والهيئات الإشرافية والمفوضية ومجلس حماية البيانات الأوروبي إلى التشجيع على وضع قواعد السلوك التي يُتوخى منها المساهمة في التطبيق اللائق للائحة في جميع أنحاء الاتحاد الأوروبي.[480] ويمكن للقواعد أن تحدد تطبيق اللائحة في قطاعات معينة، بما في ذلك شؤوناً مثل جمع البيانات الشخصية، والمعلومات التي تتعين إتاحتها لأصحاب البيانات ولعموم الجمهور، وممارسة أصحاب البيانات لحقوقهم.

لضمان امتثال مدونات السلوك للقواعد المنصوص عليها في إطار اللائحة العامة لحماية البيانات، يجب تقديم مدونات السلوك إلى الهيئة الإشرافية المختصة قبل اعتمادها. وبعد ذلك تبدي الهيئة الإشرافية رأيها بشأن ما إذا كان مشروع المدونة يعزز الامتثال للائحة وتقوم باعتماده إذا استنتجت أن مدونة قواعد السلوك تتيح ضمانات مناسبة.[481] يجب على الهيئات الإشرافية نشر مدونات السلوك التي تمت الموافقة عليها بالإضافة إلى المعايير التي استُند إليها للموافقة عليها. عندما يتعلق مشروع مدونة السلوك بأنشطة المعالجة في عدة دول أعضاء، تقدم الهيئة الإشرافية المختصة، قبل الموافقة على مشروع مدونة السلوك، أوتعديلها أو توسيعها، المدونة إلى مجلس حماية البيانات الأوروبي الذي يبدي رأيه بشأن امتثال المدونة للائحة العامة لحماية البيانات. وتقرر المفوضية، عن طريق تنفيذ القوانين، أن مدونة السلوك التي تمت الموافقة عليها والتي تم تقديمها إليها لها صلاحية عامة داخل الاتحاد.

يتيح الالتزام بمدونة السلوك مزايا مهمة لكل من أصحاب البيانات والمراقبين والمعالجين. وتقدم تلك القواعد إرشادات مفصلة تكيف المقتضيات القانونية مع قطاعات معينة وتعزز شفافية أنشطة المعالجة. وقد يلجأ المراقبون والمعالجون أيضاً إلى الالتزام بالقواعد بوصفه دليلاً عملياً على امتثالهم لقانون الاتحاد الأوروبي ووسيلة لتحسين صورتهم لدى العامة بصفتهم مؤسسات تمنح الأولوية لحماية البيانات وتلتزم بها في عملياتها. وقد تُستخدم مدونات قواعد السلوك الموافق عليها، بالإضافة إلى التعهدات الملزمة والواجبة التنفيذ، بوصفها ضمانات مناسبة لنقل البيانات إلى بلدان ثالثة. للتيقن من أن المؤسسات الملتزمة بمدونات السلوك تمتثل لها حقاً، قد تُعين هيئة خاصة (معتمدة من قبل الهيئة الإشرافية المعنية) لمراقبة الامتثال وضمانه. ولكي تتمكن الهيئة من أداء مهامها بفعالية، يجب أن تكون مستقلة، وتملك خبرة مشهود لها في الشؤون التي تنظمها مدونة السلوك، وتكون لها إجراءات وهياكل شفافة تسمح لها بتناول الشكاوى المتعلقة بانتهاكات المدونة.[482]

بموجب **قانون مجلس أوروبا**، تنص الاتفاقية المحدثة 108 على أن مستوى حماية البيانات الذي يضمنه القانون الوطني قد يكون من المفيد تقويته بتدابير تنظيمية طوعية مثل مدونة الممارسات الجيدة أو مدونة السلوك المهني. ومع ذلك، فإنها لا تمثل سوى تدابير طوعية بموجب الاتفاقية المحدثة 108: لا يمكن للمرء أن يستمد أي التزام قانوني لاتخاذ تلك التدابير، على الرغم من أنه يُنصح بها، ولا تُعد تلك التدابير، في حد ذاتها، كافية لضمان الامتثال التام للاتفاقية.[483]

## 5.3.4. شهادات التصديق

بالإضافة إلى مدونة قواعد السلوك، تُعد آليات شهادات التصديق وأختام حماية البيانات وعلاماتها من بين الوسائل الأخرى التي تمكن المراقبين والمعالجين من إثبات الامتثال للائحة العامة لحماية البيانات. لتحقيق تلك الغاية، تنص اللائحة على نظام التصديق الطوعي الذي بموجبه قد تصدر جهات معينة أو هيئات إشرافية شهادات التصديق. وقد يكتسب المراقبون والمعالجون الذين يختارون الالتزام بآلية التصديق شفافية ومصداقية أكبر، لأن التصديقات والأختام والعلامات تسمح لأصحاب البيانات بالتقييم السريع لمستوى حماية المؤسسات لعملية معالجة البيانات. يجدر القول إن امتلاك المراقب أو المعالج لمثل هذه التصديقات لا يحد من واجباته أو مسؤولياته في الامتثال لمقتضيات اللائحة.

---

[480] اللائحة العامة لحماية البيانات، المادة 40 (1).

[481] نفس المرجع السابق، المادة 40 (5).

[482] نفس المرجع السابق، المادة 41 (1) و(2).

[483] التقرير التفسيري الملحق بالاتفاقية المحدثة 108، الفقرة 33.

[486] الاتفاقية المحدثة 108، المادة 10 (2) و(3)، التقرير التفسيري الملحق بالاتفاقية المحدثة 108، الفقرة 89.

# 4.4. حماية البيانات منذ التصميم وتلقائياً

**حماية البيانات منذ التصميم**

يشترط **قانون الاتحاد الأوروبي** على المراقبين اتخاذ تدابير للتنفيذ الفعال لمبادئ حماية البيانات وإدماج الضمانات الضرورية لاستيفاء مقتضيات اللائحة وحماية حقوق أصحاب البيانات.[484] وينبغي لتلك التدابير تنفيذها وقت المعالجة وعند تحديد وسائل المعالجة على حد سواء. وعند تنفيذ تلك التدابير، يحتاج المراقب إلى مراعاة آخر المستجدات التقنية، وتكاليف تنفيذها، وطبيعة معالجة البيانات ونطاقها وأغراضها وأخطارها وفداحتها على حقوق أصحاب البيانات وحرياتهم.[485]

يقتضي **قانون مجلس أوروبا** من المراقبين والمعالجين تقييم الأثر المحتمل لمعالجة البيانات الشخصية على حقوق أصحاب البيانات وحرياتهم قبل الشروع في المعالجة. علاوة على ذلك، يلتزم المراقبون والمعالجون بتصميم معالجة البيانات بما يمنع من تهديد تلك الحقوق والحريات أو يقلل من حدة التدخل فيها إلى أدنى حد، وبتنفيذ التدابير التقنية والتنظيمية التي تراعي الآثار المترتبة عن الحق في حماية البيانات الشخصية في جميع مراحل معالجة البيانات.[486]

**حماية البيانات تلقائياً**

يقتضي **قانون الاتحاد الأوروبي** من المراقبين تنفيذ التدابير المناسبة لضمان أن البيانات الشخصية الضرورية لأغراض المعالجة هي وحدها ما سيتم معالجته تلقائياً. وينطبق ذلك الالتزام على مجموع البيانات الشخصية التي تم جمعها، ومدى معالجتها، ومدة تخزينها وإمكانية الولوج إليها.[487] ويجب أن يضمن ذلك التدبير، على سبيل المثال، عدم ولوج جميع موظفي المراقبين إلى البيانات الشخصية للمعنيين بها. وأعد المشرف الأوروبي على حماية البيانات المزيد من الإرشادات في «مجموعة الأدوات المتعلقة بالضرورة».[488]

يشترط **قانون مجلس أوروبا** على المراقبين والمعالجين تنفيذ التدابير التقنية والتنظيمية لتدارس الآثار المترتبة عن الحق في حماية البيانات، وتنفيذ التدابير التقنية والتنظيمية التي تراعي الآثار المترتبة عن الحق في حماية البيانات الشخصية في جميع مراحل معالجة البيانات.[489]

نشرت الوكالة الأوروبية لأمن الشبكات والمعلومات في 2016 تقريراً عن أدوات وخدمات الخصوصية المتاحة. من بين اعتبارات أخرى، يتيح ذلك التقييم دليلاً من المعايير والمقاييس التي تُعد مؤشرات على ممارسات الخصوصية الرديئة والجيدة. في حين تتعلق بعض المعايير مباشرة بمقتضيات اللائحة العامة لحماية البيانات - مثل استخدام الأسماء المستعارة وآليات شهادات التصديق المعتمدة - يتيح البعض الآخر مبادرات مبتكرة لضمان الخصوصية منذ التصميم وتلقائيا. على سبيل المثال، قد يعزز معيار قابلية الاستخدام الخصوصية، رغم عدم ارتباطه مباشرة بالخصوصية، لأنه بإمكانه أن يسمح باعتماد أداة أو خدمة لحفظ الخصوصية على نطاق أوسع. في الواقع، إن أدوات حفظ الخصوصية التي يصعب تنفيذها عملياً قد يكون لها مستويات متدنية جداً من الاعتماد من قبل عامة الناس، على الرغم من أنها تتيح ضمانات خصوصية قوية جداً. بالإضافة إلى ذلك، فإن معيار نضج أداة الخصوصية واستقرارها - أي الطريقة التي تتطور بها الأداة مع مضي الوقت وكيفية استجابتها للتحديات الحالية أو الجديدة المتعلقة بالخصوصية - يُعد أمراً في غاية الأهمية. وتشمل تكنولوجيات تعزيز الخصوصية الأخرى، على سبيل المثال، في سياق الاتصالات الآمنة، التشفير من طرف إلى طرف (الاتصال الذي يكون فيه الأشخاص المتصلون وحدهم من يستطيعون قراءة الرسائل)؛ وتشفير الاتصال بين الخادم والعميل (تشفير قناة الاتصال التي تُقام بين العميل والخادم)؛ والتحقق من الهوية (التحقق من هويات الأطراف المتصلة)؛ والاتصال المجهول الهوية (لا طرف ثالث يستطيع تحديد هوية الأطراف المتصلة).

---

[484] اللائحة العامة لحماية البيانات، المادة 25 (1).

[485] انظر فريق عمل المادة 29 (2017)، المبادئ التوجيهية المتعلقة بتقييم الأثر على حماية البيانات (DPIA) وتحديد ما إذا كانت المعالجة «من المحتمل أن تفضي إلى خطر كبير» بالنسبة لأغراض اللائحة 2016/679، WP 248 المراجعة رقم 01، 04 أكتوبر 2017. اطلع أيضاً على الوكالة الأوروبية لأمن الشبكات والمعلومات (2015)، حماية البيانات والخصوصية منذ التصميم - من السياسة إلى الهندسة، 12 يناير 2015.

[482] نفس المرجع السابق، المادة 41 (1) و(2).

[483] التقرير التفسيري الملحق بالاتفاقية المحدثة 108، الفقرة 33.

[484] اللائحة العامة لحماية البيانات، المادة 25 (1).

[485] انظر فريق عمل المادة 29 (2017)، المبادئ التوجيهية المتعلقة بتقييم الأثر على حماية البيانات (DPIA) وتحديد ما إذا كانت المعالجة «من المحتمل أن تفضي إلى خطر كبير» بالنسبة لأغراض اللائحة 2016/679، WP 248 المراجعة رقم 01، 04 أكتوبر 2017. اطلع أيضاً على الوكالة الأوروبية لأمن الشبكات والمعلومات (2015)، حماية البيانات والخصوصية منذ التصميم - من السياسة إلى الهندسة، 12 يناير 2015.

[486] الاتفاقية المحدثة 108، المادة 10 (2) و(3)، التقرير التفسيري الملحق بالاتفاقية المحدثة 108، الفقرة 89.

[487] اللائحة العامة لحماية البيانات، المادة 25 (2).

[488] المشرف الأوروبي على حماية البيانات (2017)، (EDPS)، «مجموعة الأدوات المتعلقة بالضرورة»، بروكسيل، 11 أبريل 2017.

[489] الاتفاقية المحدثة 108، المادة 10 (3)، التقرير التفسيري الملحق بالاتفاقية المحدثة 108، الفقرة 89.

[490] الوكالة الأوروبية لأمن الشبكات والمعلومات، مصفوفة الضوابط الخاصة بتكنولوجيا تعزيز الخصوصية: مقاربة منهجية لتقييم أدوات الخصوصية على الإنترنت والمحمول، 20 ديسمبر 2016.

# 5 الإشـــراف المستقـــــل

| الاتحاد الأوروبي | المسائل المتناولة | مجلس أوروبا |
|---|---|---|
| الميثاق، المادة 8 (3)<br>المعاهدة المنظمة لعمل الاتحاد الأوروبي، المادة 16 (2)<br>اللائحة العامة لحماية البيانات، المواد 51-59<br>محكمة العدل التابعة للاتحاد الأوروبي، القضية C-518/07، المفوضية الأوروبية ضد جمهورية ألمانيا الاتحادية [الغرفة الكبرى]، 2010<br>محكمة العدل التابعة للاتحاد الأوروبي، القضية C-614/10، المفوضية الأوروبية ضد جمهورية النمسا [الغرفة الكبرى]، 2012<br>محكمة العدل التابعة للاتحاد الأوروبي، القضية C-288/12، المفوضية الأوروبية ضد المجر [الغرفة الكبرى]، 2014<br>محكمة العدل التابعة للاتحاد الأوروبي، القضية C-362/14، ماكسيميليان شريمز ضد مفوض حماية البيانات [الغرفة الكبرى]، 2015 | الهيئات الإشرافية | الاتفاقية المحدثة 108، المادة 15 |
| اللائحة العامة لحماية البيانات، المواد 60-67 | التعاون بين الهيئات الإشرافية | الاتفاقية المحدثة 108، المواد 16-21 |
| اللائحة العامة لحماية البيانات، المواد 68-76 | مجلس حماية البيانات الأوروبي | |

## النقاط الرئيسية

1. يُعد الإشراف المستقل عنصراً جوهرياً من قانون حماية البيانات الأوروبي وتم تكريسه في المادة 8 (3) من الميثاق.
2. لضمان حماية البيانات الفعلية، يجب أن ينص القانون الوطني على الهيئات الإشرافية المستقلة.
3. يتعين على الهيئات الإشرافية التصرف باستقلالية تامة، وهو ما يجب أن يضمنه القانون التأسيسي ويتجلى في البنية التنظيمية المحددة للهيئة الإشرافية.
4. للهيئات الإشرافية صلاحيات ومهام معينة تشمل، من بين ما تشمله، ما يلي:
    1. مراقبة حماية البيانات وتعزيزها على الصعيد الوطني؛
    2. وإسداء المشورة لأصحاب البيانات والمراقبين بالإضافة إلى الحكومة وعموم الجمهور؛
    3. وتلقي الشكاوى ودعم أصحاب البيانات الذين يُزعم انتهاك حقهم في حماية البيانات؛
    4. والإشراف على المراقبين والمعالجين.

5. تتمتع الهيئات الإشرافية أيضاً بصلاحية التدخل عند الضرورة من خلال:
    1. التحذير أو التوبيخ أو حتى تغريم المراقبين والمعالجين؛
    2. والأمر بتصحيح البيانات أو حجبها أو حذفها؛
    3. وفرض الحظر على المعالجة أو غرامة إدارية؛
    4. وإحالة القضايا إلى المحكمة.
6. نظراً إلى أن معالجة البيانات الشخصية غالباً ما تتعلق بالمراقبين والمعالجين وأصحاب البيانات الموجودين في دول مختلفة، يُطلب من الهيئات الإشرافية التعاون البعض منها مع البعض في القضايا العابرة للحدود لضمان الحماية الفعلية للأفراد في أوروبا.
7. في الاتحاد الأوروبي، تنشئ اللائحة العامة لحماية البيانات آلية نقطة الخدمات الموحدة (الشباك الوحيد) بالنسبة للحالات التي تكون فيها المعالجة عابرة للحدود. تقوم بعض الشركات بأنشطة المعالجة العابرة للحدود بسبب معالجة البيانات الشخصية في سياق أنشطة مؤسسات في أكثر من دولة عضو واحدة أو في سياق مؤسسة وحيدة في الاتحاد لكنها تؤثر في أصحاب البيانات تأثيراً ملموساً في أكثر من دولة عضو. بموجب هذه الآلية، لن يتعين على هذه الشركات سوى التعامل مع هيئة إشرافية وطنية واحدة خاصة بحماية البيانات.
8. ستسمح آلية الاتساق والتعاون بمقاربة منسقة بين جميع الهيئات الإشرافية المعنية بالقضية. ستقدم الهيئة الإشرافية الرائدة - المعنية بالمؤسسة الرئيسية أو المؤسسة الوحيدة - مشروع القرار الخاص بها بعد التشاور مع غيرها من الهيئات الإشرافية المعنية.
9. على غرار فريق عمل المادة 29 الحالي، ستكون الهيئة الإشرافية لكل دولة عضو والمشرف الأوروبي على حماية البيانات (EDPS) جزءاً من مجلس حماية البيانات الأوروبي.
10. تشمل مهام مجلس حماية البيانات الأوروبي، على سبيل المثال، مراقبة التطبيق الصحيح للائحة، وإسداء المشورة إلى المفوضية في القضايا ذات الصلة، وإبداء الآراء وإصدار المبادئ التوجيهية أو الممارسات الفضلى في مواضيع متنوعة.
11. يتمثل الفرق الأساسي في أن مجلس حماية البيانات الأوروبي لن يبدي الآراء فحسب، كما هو الشأن بموجب الأمر التوجيهي EC/95/46، ولكنه سيصدر أيضاً قرارات ملزمة تتعلق بالحالات التي تثير فيها الهيئة الإشرافية اعتراضاً معللاً وذا صلة موضوعية بحالات تهم نقاط الخدمات الموحدة (الشباك الوحيد)؛ وعندما يكون هناك تضارب في الآراء حول أيٍّ من الهيئات الإشرافية هي الموجودة في الريادة؛ وأخيراً عندما لا تطلب الهيئة الإشرافية المختصة رأي مجلس حماية البيانات الأوروبي أو لا تأخذ به. ويكون الهدف المتوخى من ذلك ضمان التطبيق المتسق للائحة في جميع الدول الأعضاء.

يُعد الإشراف المستقل مكوناً جوهرياً في قانون حماية البيانات الأوروبي. ويرى كل من قانون الاتحاد الأوروبي وقانون مجلس أوروبا وجود الهيئات الإشرافية المستقلة أمراً لا غنى عنه للحماية الفعلية لحقوق الأفراد وحرياتهم فيما يتعلق بمعالجة بياناتهم الشخصية. ونظراً إلى أن

معالجة البيانات تُعد حالياً دائمة الوجود ويزداد تعقد فهمها على الأفراد، فإن تلك السلطات تُعد حراس العصر الرقمي. في الاتحاد الأوروبي، يُعد وجود الهيئات الإشرافية المستقلة من بين أكثر العناصر أهمية في الحق في حماية البيانات الشخصية المكرس في قانون الاتحاد الأوروبي الأساسي. وتقر المادة 8 (3) من ميثاق الحقوق الأساسية للاتحاد الأوروبي والمادة 16 (2) من المعاهدة المنظمة لعمل الاتحاد الأوروبي بحماية البيانات الشخصية حقاً أساسياً وتشدد على أن الامتثال لقواعد حماية البيانات يجب أن يكون خاضعاً لمراقبة الهيئة الإشرافية. للإشارة فإن الاجتهادات القضائية تقر أيضاً بأهمية الإشراف المستقل بالنسبة لقانون حماية البيانات.

مثال: في قضية «شريمز»،[491] كانت المحكمة معنية بما إذا كان نقل البيانات الشخصية إلى الولايات المتحدة (US) بموجب اتفاق الملاذ الآمن الأول بين الاتحاد الأوروبي والولايات المتحدة يتوافق مع قانون حماية البيانات الأوروبي، في ضوء تسريبات إدوارد سنودن بشأن قيام وكالة الأمن القومي الأمريكية بالمراقبة الجماعية (أي مراقبة الجماهير على نطاق واسع). واستند نقل البيانات الشخصية إلى الولايات المتحدة إلى قرار صادر عن المفوضية الأوروبية تم اعتماده سنة 2000، والذي يسمح بنقل البيانات الشخصية من الاتحاد الأوروبي إلى منظمات الولايات المتحدة التي تقوم بالمصادقة الذاتية بموجب مخطط الملاذ الآمن، على أساس أن المخطط يضمن مستوىً ملائماً من حماية البيانات الشخصية. وعندما طُلب من الهيئة الإشرافية الإيرلندية التحقيق في الشكوى التي رفعها المدعي فيما يتعلق بقانونية عمليات نقل البيانات بعد تسريبات سنودن، رفضت الهيئة الإشرافية الشكوى بحجة أن وجود قرار المفوضية بشأن ملاءمة نظام حماية البيانات الأمريكي المتجلي في مبادئ الملاذ الآمن («قرار الملاذ الآمن») منعها من مواصلة التحقيق في الشكوى.

ومع ذلك رأت محكمة العدل التابعة للاتحاد الأوروبي بأن وجود قرار صادر عن المفوضية يسمح بعمليات نقل البيانات إلى بلدان ثالثة تضمن مستويات ملائمة من الحماية لا يلغي صلاحيات الهيئات الإشرافية الوطنية أو يقلصها. وأشارت محكمة العدل التابعة للاتحاد الأوروبي إلى أن صلاحيات تلك السلطات لمراقبة وضمان الامتثال لقواعد الاتحاد الأوروبي لحماية البيانات تُستمد من قانون الاتحاد الأوروبي الأساسي، لا سيما المادة 8 (3) من الميثاق والمادة 16 (2) من المعاهدة المنظمة لعمل الاتحاد الأوروبي. «ولذلك يُعد تأسيس هيئات إشرافية مستقلة مكوناً جوهرياً من حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية.»[492]

ولذلك قررت محكمة العدل التابعة للاتحاد الأوروبي أنه حتى عندما يكون نقل البيانات الشخصية قد خضع لقرار الملاءمة الصادر عن المفوضية، حينما تودع شكوى لدى هيئة إشرافية وطنية، يجب على الهيئة دراسة الشكوى بإمعان. ويجوز للهيئة الإشرافية أن ترفض الشكوى إذا استنتجت عدم استنادها إلى أسس سليمة. في تلك القضية، شددت محكمة العدل التابعة للاتحاد الأوروبي على أن الحق في الانتصاف القضائي الفعال يتطلب من الأفراد أن يكونوا قادرين على الطعن في ذلك القرار أمام المحاكم الوطنية التي قد تحيل القضية إلى محكمة العدل التابعة للاتحاد الأوروبي لاستصدار حكم تمهيدي بشأن صلاحية قرار المفوضية. حينما ترى الهيئة الإشرافية أن الشكوى تستند إلى أسس سليمة، يجب أن تكون قادرة على المشاركة في الدعوى القضائية وعرض القضية على المحاكم الوطنية. وقد تحيل المحاكم الوطنية القضية على محكمة العدل التابعة للاتحاد الأوروبي لأنها الهيئة الوحيدة التي لها صلاحية البت في صلاحية قرار الملاءمة الصادر عن المفوضية.[493]

ثم درست محكمة العدل التابعة للاتحاد الأوروبي صلاحية قرار الملاذ الآمن لتحديد ما إذا كان نظام عمليات النقل يتوافق مع قواعد الاتحاد الأوروبي لحماية البيانات. واستنتجت أن المادة 3 من قرار الملاذ الآمن قيدت صلاحيات الهيئات الإشرافية الوطنية (المخولة بموجب الأمر التوجيهي المتعلق بحماية البيانات) لاتخاذ إجراءات لمنع عمليات نقل البيانات في حالة عدم ملاءمة مستوى حماية البيانات الشخصية في الولايات المتحدة. بالنظر إلى أهمية الهيئات الإشرافية المستقلة في ضمان الامتثال لقانون حماية البيانات، رأت محكمة العدل التابعة للاتحاد الأوروبي أنه، بمقتضى الأمر التوجيهي المتعلق بحماية البيانات حين يُقرأ في ضوء الميثاق، لا تملك المفوضية صلاحية تقييد صلاحيات الهيئات الإشرافية المستقلة بتلك الطريقة. وكان تقييد صلاحيات الهيئات الإشرافية من بين الأسباب التي جعلت محكمة العدل التابعة للاتحاد الأوروبي تقضي ببطلان قرار الملاذ الآمن.

لذلك يقتضي القانون الأوروبي وجود الإشراف المستقل بوصفه آلية مهمة لضمان الحماية الفعلية للبيانات. وتُعد الهيئات الإشرافية المستقلة أول جهة اتصال بالنسبة لأصحاب البيانات في حالات خرق الخصوصية.[494] بموجب قانون الاتحاد الأوروبي وقانون مجلس أوروبا، يُعد تأسيس الهيئات

[491] محكمة العدل التابعة للاتحاد الأوروبي، القضية C-362/14، ماكسيميليان شريمز ضد مفوض حماية البيانات [الغرفة الكبرى]، 06 أكتوبر 2015.
[492] محكمة العدل التابعة للاتحاد الأوروبي، القضية C-362/14، ماكسيميليان شريمز ضد مفوض حماية البيانات [الغرفة الكبرى]، 06 أكتوبر 2015، الفقرة 41.
[493] نفس المرجع السابق، الفقرات 66-53.
[494] اللائحة العامة لحماية البيانات، المادة 13 (2) (د).

الإشرافية أمراً إجبارياً. يصف كلا الإطاران القانونيان مهامّ تلك السلطات وصلاحياتها بطريقة مشابهة لتلك التي تشتمل عليها اللائحة العامة لحماية البيانات. ولذلك ينبغي، من حيث المبدأ، للهيئات الإشرافية أن تعمل بنفس الطريقة بموجب قانون الاتحاد الأوروبي وقانون مجلس أوروبا.[495]

## 1.5. الاستقلالية

يقتضي كل من **قانون الاتحاد الأوروبي وقانون مجلس أوروبا** من كل هيئة إشرافية أن تتصرف باستقلالية تامة في أداء مهامها وعند ممارسة صلاحياتها.[496] وتُعد استقلالية الهيئة الإشرافية وأعضائها وموظفيها عن التأثيرات الخارجية المباشرة وغير المباشرة أمراً أساسياً لضمان الموضوعية التامة عند البت في قضايا حماية البيانات. ولا يجب أن يتضمن القانون الذي يستند إليه تأسيس هيئة إشرافية مقتضيات تضمن الاستقلالية خصيصاً فحسب، وإنما يجب أن تثبت البنية التنظيمية للهيئة الإشرافية تلك الاستقلالية أيضاً. في 2010، تدارست محكمة العدل التابعة للاتحاد الأوروبي - لأول مرة - إلى أي مدى تكون السلطات المشرفة على حماية البيانات مطالبةً بالتحلي بالاستقلالية.[497] وتوضح الأمثلة التي تم إبرازها تعريف محكمة العدل التابعة للاتحاد الأوروبي لمعنى 'الاستقلالية التامة'.

مثال: في قضية «المفوضية الأوروبية ضد جمهورية ألمانيا الاتحادية»،[498] طلبت المفوضية الأوروبية من محكمة العدل التابعة للاتحاد الأوروبي أن تقضي بأن ألمانيا قد أعملت بطريقة خاطئة شرط 'الاستقلالية التامة' للهيئات الإشرافية المسؤولة عن ضمان حماية البيانات وأنها بذلك قد أخفقت في الوفاء بالتزاماتها بموجب المادة 28 (1) من الأمر التوجيهي المتعلق بحماية البيانات. ذلك أنه في رأي المفوضية، فإن إقدام ألمانيا على إخضاع الهيئات الإشرافية التي تراقب معالجة البيانات الشخصية في مختلف الولايات الاتحادية (Länder) لمراقبة الدولة لضمان الامتثال لقانون حماية البيانات قد انتهك شرط الاستقلالية.

أبرزت محكمة العدل التابعة للاتحاد الأوروبي على أن عبارة 'باستقلالية تامة' يجب أن تُفسر استناداً إلى النص الفعلي لذلك المقتضى وأهداف قانون حماية البيانات الأوروبي ومخططه.[499] وشددت محكمة العدل التابعة للاتحاد الأوروبي على أن الهيئات الإشرافية تُعد 'حراس' الحقوق المتعلقة بمعالجة البيانات الشخصية. ولذلك فإن تأسيسها في الدول الأعضاء يُعد «مكوناً أساسياً من حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية»،[500] وخلصت محكمة العدل التابعة للاتحاد الأوروبي إلى أنه «عندما تؤدي الهيئات الإشرافية مهامها، يجب عليها التصرف بالموضوعية والحياد. وتحقيقاً لذلك الغرض، يجب عليها أن تظل بمنأى عن أي تأثير خارجي، بما في ذلك التأثير المباشر أو غير المباشر للسلطات العامة»،[501]

رأت محكمة العدل التابعة للاتحاد الأوروبي أيضاً أن معنى 'الاستقلالية التامة' ينبغي أن يُفسر في ضوء استقلالية المشرف الأوروبي على حماية البيانات كما هو محدد في لائحة حماية البيانات الخاصة بمؤسسات الاتحاد الأوروبي. في تلك اللائحة، يقتضي مفهوم الاستقلالية أن المشرف الأوروبي على حماية البيانات لا يجوز له تلقي تعليمات أو طلبها من أي كان.

استناداً إلى ذلك، رأت محكمة العدل التابعة للاتحاد الأوروبي أن الهيئات الإشرافية في ألمانيا لم تكن مستقلة تماماً بمفهوم قانون حماية البيانات الأوروبي نظراً إلى إشراف السلطات العامة عليها.

مثال: في قضية «المفوضية الأوروبية ضد جمهورية النمسا»،[502] أبرزت محكمة العدل التابعة للاتحاد الأوروبي مشاكل مشابهة تتعلق باستقلالية بعض أعضاء وموظفي هيئة حماية البيانات النمساوية (Data Protection Commission, DSK). وخلصت محكمة العدل التابعة للاتحاد الأوروبي إلى أن تزويد المستشارية الاتحادية الهيئة الإشرافية بالقوى العاملة نال من مقتضى الاستقلالية المنصوص عليه في قانون حماية البيانات الأوروبي. ورأت محكمة العدل التابعة للاتحاد الأوروبي أيضاً أن شرط إخبار الهيئة الإشرافية للمستشارية بعملها في جميع الأوقات ألغى الاستقلالية التامة للهيئة الإشرافية.

[495] نفس المرجع السابق، المادة 51؛ الاتفاقية المحدثة 108، المادة 15.

[496] اللائحة العامة لحماية البيانات، المادة 52 (1)؛ الاتفاقية المحدثة 108، المادة 15 (5).

[497] وكالة الاتحاد الأوروبي للحقوق الأساسية (2010)، الحقوق الأساسية: التحديات والإنجازات في سنة 2010، التقرير السنوي لسنة 2010، ص. 59؛ وكالة الاتحاد الأوروبي للحقوق الأساسية (2010)، حماية البيانات في الاتحاد الأوروبي: دور السلطات الوطنية لحماية البيانات، مايو 2010.

[498] محكمة العدل التابعة للاتحاد الأوروبي، القضية C-518/07، المفوضية الأوروبية ضد جمهورية ألمانيا الاتحادية [الغرفة الكبرى]، 09 مارس 2010، الفقرة 27.

[499] نفس المرجع السابق، الفقرتان 17 و29.

[500] نفس المرجع السابق، الفقرة 23.

[501] نفس المرجع السابق، الفقرة 25.

[502] محكمة العدل التابعة للاتحاد الأوروبي، القضية C-614/10، المفوضية الأوروبية ضد جمهورية النمسا [الغرفة الكبرى]، 16 أكتوبر 2012، الفقرتان 59 و63.

مثال: في قضية «المفوضية الأوروبية ضد المجر»،[503] تم حظر نفس الممارسات الوطنية التي تمس باستقلالية القوى العاملة. وأشارت محكمة العدل التابعة للاتحاد الأوروبي إلى أن «المقتضى الذي يستوجب ضمان أن تكون كل هيئة إشرافية قادرة على أداء المهام الموكلة إليها في استقلالية تامة يستوجب التزام الدولة العضو المعنية بالسماح لتلك الهيئة بأن تضطلع بولايتها كاملة «. ورأت محكمة العدل أيضاً أنه «بإنهاء الوظيفة التي تضطلع بها الهيئة الإشرافية على حماية البيانات الشخصية قبل الأوان، فشلت المجر في الوفاء بالتزاماتها بموجب الأمر التوجيهي EC/95/46 [...]»

تنص اللائحة العامة لحماية البيانات حالياً صراحة على مفهوم 'الاستقلالية التامة' ومعاييرها، وتدمج المبادئ الواردة في الأحكام الصادرة عن محكمة العدل التابعة للاتحاد الأوروبي التي تم سردها. فوفقاً للائحة، تستلزم الاستقلالية التامة في أداء الهيئات الإشرافية لمهامها وممارسة صلاحياتها ما يلي:[504]

1. يجب على أعضاء الهيئة الإشرافية أن يظلوا بمنأى عن التأثير الخارجي - سواء كان مباشراً أو غير مباشر - ولا يجب عليهم تلقي تعليمات من أي كان؛
2. يجب على أعضاء كل هيئة إشرافية الإمساك عن أي عمل يخالف مهامهم للحيلولة دون تضارب المصالح؛
3. يجب على الدول الأعضاء تزويد كل هيئة إشرافية بالموارد البشرية والتقنية والمالية والبنية التحتية الضرورية للأداء الفعال لمهامهم؛
4. يجب على الدول الأعضاء أن تضمن اختيار كل هيئة إشرافية موظفيها؛
5. يجب ألا تمس المراقبة المالية التي تخضع لها كل سلطة مشرفة وفقاً للقانون الوطني باستقلاليتها. ويجب على الهيئات الإشرافية أن تُخصص لها ميزانيات سنوية من المال العام لتمكينها من أداء عملها أداءً سليماً.

تُعد استقلالية الهيئات الإشرافية أيضاً شرطاً هاماً بموجب قانون مجلس أوروبا. وتشترط الاتفاقية المحدثة 108 على الهيئات الإشرافية أن «تتصرف بالاستقلالية والحياد التامين في أداء مهامها وممارسة صلاحياتها»، دون طلب التعليمات أو قبولها.[505] وعلى هذا النحو، تقر الاتفاقية بأن تلك السلطات لا يمكن لها أن تصون بفعالية حقوق الأفراد وحرياتهم المتعلقة بمعالجة البيانات ما لم تكن تمارس وظائفها باستقلالية تامة. يحدد التقرير التفسيري الملحق بالاتفاقية المحدثة 108 عدداً من العناصر التي تساهم في صون تلك الاستقلالية. وتشمل تلك العناصر إمكانية تعيين الهيئات الإشرافية لموظفيها واعتماد قرارات دون الخضوع للتدخل الخارجي، بالإضافة إلى العوامل المتعلقة بمدة ممارستها لوظائفها والظروف التي يجوز لها فيها أن تتوقف عن ممارسة وظائفها.[506]

## 2.5. الاختصاصات والصلاحيات

**بموجب قانون الاتحاد الأوروبي**، تحدد اللائحة العامة لحماية البيانات اختصاصات الهيئات الإشرافية وهيكلها التنظيمي وتنص على وجوب تمتعها باختصاص وصلاحية أداء المهام المطلوبة منها بموجب اللائحة. تُعد الهيئة الإشرافية الجهة الرئيسية في القانون الوطني التي تضمن الامتثال لقانون حماية البيانات الأوروبي. ولدى الهيئات الإشرافية قائمة شاملة من المهام والصلاحيات التي تتجاوز المراقبة لتشمل الأنشطة الإشرافية الاستباقية والوقائية. لكي تقوم الهيئات الإشرافية بتلك المهام، يجب أن تتمتع بالصلاحيات التحقيقية والتصحيحية والاستشارية المناسبة كما وردت في المادتين 57 و58 من اللائحة العامة لحماية البيانات، مثل: [507]

- إسداء المشورة للمراقبين وأصحاب البيانات بشأن قضايا حماية البيانات؛
- ترخيص البنود العقود القياسية أوقواعد الشركات الملزمة أو الترتيبات الإدارية؛

[503] محكمة العدل التابعة للاتحاد الأوروبي، القضية C-288/12، المفوضية الأوروبية ضد المجر [الغرفة الكبرى]، 08 أبريل 2014، الفقرتان 50 و67.
[504] اللائحة العامة لحماية البيانات، المادة 52.
[505] الاتفاقية المحدثة 108، المادة 15 (5).
[506] التقرير التفسيري الملحق بالاتفاقية 108.
[507] اللائحة العامة لحماية البيانات، المادتان 57 و58. إطلع أيضاً على الاتفاقية 108، البروتوكول الإضافي، المادة 1.

3. التحقيق في عمليات المعالجة والتدخل وفقا لذلك؛
4. طلب تقديم أي معلومات ذات صلة بالإشراف على أنشطة المراقب؛
5. تحذير المراقبين أو توبيخهم والأمر بإرسال الإشعارات المتعلقة بخروقات البيانات إلى أصحاب البيانات؛
6. الأمر بتصحيح البيانات أو حجبها أو محوها أو تدميرها؛
7. فرض حظر مؤقت أو نهائي على المعالجة أو فرض غرامات إدارية؛
8. إحالة القضايا إلى المحكمة.

لكي تمارس الهيئة الإشرافية وظائفها، يجب عليها أن تتوفر على حق الوصول إلى جميع البيانات الشخصية والمعلومات الضرورية للتحقيق، بالإضافة إلى الولوج إلى أي مقر يحتفظ فيه المراقب بالمعلومات ذات الصلة. واستناداً إلى محكمة العدل التابعة للاتحاد الأوروبي، يجب أن تُفسر صلاحيات الهيئة الإشرافية تفسيراً واسعاً لضمان الفعالية التامة لحماية بيانات المعنيين بها في الاتحاد الأوروبي.

مثال: في قضية «شريمز»، كانت محكمة العدل التابعة للاتحاد الأوروبي معنية بالبت فيما إذا كان نقل البيانات الشخصية بموجب اتفاق الملاذ الآمن الأول بين الاتحاد الأوروبي والولايات المتحدة يتوافق مع قانون حماية البيانات الأوروبي في ضوء تسريبات إدوارد سنودن. ورأت محكمة العدل التابعة للاتحاد الأوروبي في تعليلها أن الهيئات الإشرافية الوطنية - التي تتصرف بصفتها مراقبين مستقلين لمعالجة البيانات التي يقوم بها المراقبون - بإمكانها أن تحول دون نقل البيانات إلى بلد ثالث رغم وجود قرار بشأن كفاية الضمانات إذا كانت هناك أدلة معقولة على أن البلد الثالث لم يعد يضمن الحماية الكافية.[508]

يكون لكل هيئة إشرافية الاختصاص لممارسة الصلاحيات التحقيقية وصلاحيات التدخل داخل أراضيها. ومع ذلك، نظراً إلى أن أنشطة المعالجين والمراقبين غالباً ما تكون عابرة للحدود ونظراً إلى أن أصحاب البيانات الموجودين في دول أعضاء متعددة يتأثرون بمعالجة البيانات، يُطرح سؤال يتعلق بتقسيم الاختصاصات بين مختلف الهيئات الإشرافية. وأُتيحت لمحكمة العدل التابعة للاتحاد الأوروبي فرصة تدارس هذه المسألة في قضية «فيليتيمو».

مثال: في قضية «فيليتيمو»،[509] انشغلت محكمة العدل التابعة للاتحاد الأوروبي بمسألة اختصاص الهيئات الإشرافية الوطنية في التعامل مع القضايا التي تتعلق بمنظمات غير مؤسسة ضمن نفوذها الترابي. وكانت «فيليتيمو» شركة مسجلة في سلوفاكيا وتدير موقعاً إلكترونياً لتجارة العقارات الواقعة بدولة المجر. وقدم المعلنون شكوى إلى الهيئة الإشرافية على حماية البيانات المجرية بسبب انتهاك قانون حماية البيانات المجري، وقامت الهيئة بتغريم فيليتيمو. وطعنت الشركة في الغرامة أمام المحاكم الوطنية، وأحيلت القضية إلى محكمة العدل التابعة للاتحاد الأوروبي لتبت فيما إذا كان الأمر التوجيهي الصادر عن الاتحاد الأوروبي والمتعلق بحماية البيانات قد سمح للهيئات الإشرافية في إحدى الدول الأعضاء بتطبيق قانونها الوطني لحماية البيانات على شركة مسجلة في دولة عضو أخرى.

فسرت محكمة العدل التابعة للاتحاد الأوروبي المادة 4 (1) من الأمر التوجيهي المتعلق بحماية البيانات بما يسمح بتطبيق قانون حماية البيانات لإحدى الدول الأعضاء غير الدولة العضو حيث تم تسجيل المراقب، «ما دام ذلك المراقب يمارس، من خلال ترتيبات مستقرة في أراضي تلك الدولة العضو، نشاطاً حقيقياً وفعلياً - مهما قل شأنه - تتم في سياقه المعالجة». ولاحظت محكمة العدل التابعة للاتحاد الأوروبي، استناداً إلى المعلومات التي عُرضت عليها، أن فيليتيمو سعت إلى نشاط حقيقي وفعلي في دولة المجر ، حيث كان للشركة ممثلاً بدولة المجر تم إدراجه في سجل الشركات السلوفاكي بعنوان مجري، بالإضافة إلى حساب بنكي مجري وصندوق الرسائل، وسعت أيضاً إلى أنشطة بدولة المجر كُتبت باللغة المجرية. ودلت هذه المعلومات على وجود المؤسسة وجعلت نشاط فيليتيمو خاضعاً لقانون حماية البيانات المجري ولاختصاص الهيئة المجرية لحماية البيانات. إلا أن محكمة العدل التابعة للاتحاد الأوروبي تركت للمحكمة الوطنية أمر التحقق من المعلومات والبت فيما إذا كانت فيليتيمو تملك مؤسسة في دولة المجر.

[508] محكمة العدل التابعة للاتحاد الأوروبي، القضية C-362/14، ماكسميليان شريمز ضد مفوض حماية البيانات [الغرفة الكبرى]، 06 أكتوبر 2015، الفقرات 36-26 و41-40.
[509] محكمة العدل التابعة للاتحاد الأوروبي، القضية C-230/14، فيليتيمو (شركة محدودة) ضد الهيئة الوطنية لحماية البيانات وحرية المعلومات، 01 أكتوبر 2015.

إذا استنتجت المحكمة التي أحالت القضية أن «فيلتيمو» تملك مؤسسة في دولة المجر، سيكون للهيئة الإشرافية المجرية صلاحية فرض الغرامة عليها. ومع ذلك، إذا قررت المحكمة الوطنية ما يخالف ذلك، أي أن فيلتيمو لا تملك مؤسسة في دولة المجر، يكون القانون الواجب التطبيق تبعاً لذلك هو قانون الدولة العضو (أو الدول الأعضاء) حيث تم تسجيل الشركة. في هذه الحالة، بما أن صلاحيات الهيئات الإشرافية يجب أن تُمارس بما يتوافق مع السيادة الترابية للدول الأعضاء، فإن الهيئة المجرية لا تكون قادرة على فرض العقوبات. بما أن الأمر التوجيهي المتعلق بحماية البيانات يتضمن واجب التعاون بين الهيئات الإشرافية، يمكن للهيئة الهنغارية، مع ذلك، أن تطلب من نظيرتها السلوفاكية دراسة القضية، وإثبات انتهاك القانون السلوفاكي، وفرض العقوبات التي تنص عليها التشريعات السلوفاكية.

باعتماد اللائحة العامة لحماية البيانات، ثمة حالياً قواعد مفصلة سارية المفعول تتعلق باختصاص الهيئات الإشرافية في القضايا العابرة للحدود، حيث أرست اللائحة "آلية نقطة الخدمات الموحدة" وتضمنت مقتضيات تفرض التعاون بين مختلف الهيئات الإشرافية. ومن أجل التعاون الفعال في القضايا العابرة للحدود، تشترط اللائحة العامة لحماية البيانات إرساء هيئة إشرافية رائدة تكون هي الهيئة المشرفة على المؤسسة الرئيسية أو الوحيدة للمراقب أو المعالج.[510] تتكفل الهيئة الإشرافية الرائدة بالقضايا العابرة للحدود، وتُعد هي المحاور الوحيد بالنسبة للمراقب أو المعالج وتنسق التعاون بين غيرها من الهيئات الإشرافية للتوصل إلى توافق. ويشمل التعاون تبادل المعلومات، وتبادل المساعدة في مجال المراقبة والتحقيق واعتماد القرارات الملزمة.[511]

في قانون مجلس أوروبا، تنص المادة 15 من الاتفاقية المحدثة 108 على اختصاصات الهيئات الإشرافية وصلاحياتها. وتطابق تلك الصلاحيات الصلاحيات المخولة للهيئات الإشرافية بموجب قانون الاتحاد الأوروبي، بما في ذلك صلاحيات التحقيق والتدخل، وصلاحيات إصدار القرارات وفرض العقوبات الإدارية المتعلقة بانتهاكات مقتضيات الاتفاقية، وصلاحيات المشاركة في الدعاوى القضائية. وللهيئات الإشرافية المستقلة أيضاً اختصاص التعامل مع الطلبات والشكاوى التي يتقدم بها أصحاب البيانات و زيادة الوعي العام بقانون حماية البيانات وإسداء المشورة إلى صناع القرار الوطنيين فيما يخص أي تدابير تشريعية أوإدارية تنص على معالجة البيانات الشخصية.

## 3.5. التعاون

تحدد اللائحة العامة لحماية البيانات إطاراً عاماً للتعاون بين الهيئات الإشرافية وتتيح قواعد أكثر تحديداً بشأن تعاون الهيئات الإشرافية في أنشطة معالجة البيانات العابرة للحدود.

بموجب اللائحة العامة لحماية البيانات، تتبادل الهيئات الإشرافية المساعدة فيما بينها وتشارك المعلومات ذات الصلة فيما بينها لتنفيذ اللائحة وتطبيقها على نحو متسق.[512] ويشمل ذلك الهيئة الإشرافية المطلوب منها القيام بالمشاورات وعمليات التفتيش والتحقيقات. ويمكن للهيئات الإشرافية أن تنجز عمليات مشتركة، بما في ذلك التحقيقات المشتركة وتدابير التنفيذ المشتركة التي بمقتضاها يُعد موظفو جميع الهيئات الإشرافية معنيين بها.[513]

في الاتحاد الأوروبي، يعمل المراقبون والمعالجون بشكل متزايد على نطاق عبر وطني. هذا الأمر يقتضي تعاوناً وثيقاً بين الهيئات الإشرافية المختصة في الدول الأعضاء لضمان امتثال معالجة البيانات الشخصية لمتطلبات اللائحة العامة لحماية البيانات. وبموجب آلية «نقطة الخدمات الموحدة» (الشباك الوحيد) المنصوص عليها في اللائحة، إذا كان لدى مراقب أو معالج مؤسسات في عدد من الدول الأعضاء، أو إذا كانت لديه مؤسسة واحدة ولكن عمليات المعالجة تؤثر بشكل كبير على أصحاب البيانات في أكثر من دولة عضو، فإن الهيئة الإشرافية للمؤسسة الرئيسية (أو الوحيدة) هي الهيئة الرائدة للأنشطة عبر الوطنية للمراقب أو المعالج. وتتمتع الهيئات الرائدة بصلاحية اتخاذ إجراءات إنفاذ ضد المراقب أو المعالج. وتهدف آلية نقطة الخدمات الموحدة إلى تحسين التنسيق والتطبيق الموحد لقانون حماية البيانات

[510] اللائحة العامة لحماية البيانات، المادة 56 (1).
[511] نفس المرجع السابق، المادة 60.
[512] نفس المرجع السابق، المادة 61 (1)-(3)، والمادة 62 (1).
[513] نفس المرجع السابق، المادة 62 (1).

في الاتحاد الأوروبي في مختلف الدول الأعضاء. كما أنها مفيدة أيضاً للشركات، بحيث إن هذه الأخيرة لا تحتاج سوى إلى التعامل مع الهيئة الرائدة بدلاً من العديد من الهيئات الإشرافية. هذا الأمر يعزز اليقين القانوني للشركات، وقد يعني أيضًا، من الناحية العملية، أن القرارات يتم اتخاذها بشكل أسرع وأن الشركات لا تتعامل مع هيئات إشرافية مختلفة تفرض عليها متطلبات متضاربة.

يستلزم تحديد الهيئة الرائدة التعرف على موقع المؤسسة الرئيسية للشركة في الاتحاد الأوروبي. هذا وتعرف اللائحة العامة لحماية البيانات مصطلح «المؤسسة الرئيسية»، إضافة إلى ذلك، أصدر فريق عمل المادة 29 إرشادات لتحديد الهيئة الإشرافية الرائدة للمراقب أو المعالج، وهي تتضمن معايير تحديد المؤسسة الرئيسية.[514]

ولضمان مستوى عالٍ من حماية البيانات في مختلف أنحاء الاتحاد الأوروبي، لا تعمل الهيئة الإشرافية الرائدة بمفردها، بل يجب أن تتعاون مع الهيئات الإشرافية الأخرى المعنية لاتخاذ قرارات بشأن معالجة البيانات الشخصية من قبل المراقبين والمعالجين، في محاولة للوصول إلى توافق وضمان الاتساق. ويشمل التعاون بين الهيئات الإشرافية ذات الصلة تبادل المعلومات، والمساعدة المتبادلة، وإجراء تحقيقات وأنشطة مراقبة مشتركة.[515] وعند تبادل تقديم المساعدة، يجب على الهيئات الإشرافية التعامل بدقة مع طلبات المعلومات المقدمة من الهيئات الإشرافية الأخرى وممارسة تدابير الإشراف، من قبيل، على سبيل المثال، التراخيص المسبقة والمشاورات مع مراقب البيانات بشأن أنشطة المعالجة أو عمليات التفتيش أو التحقيقات. ويجب تقديم المساعدة للهيئات الإشرافية في الدول الأعضاء الأخرى عند الطلب دون أي تأخير غير مبرر وفي موعد لا يتجاوز شهراً واحداً من تلقي الطلب.[516]

وعندما يكون للمراقب مؤسسات في عدة دول أعضاء، يمكن للهيئات الإشرافية إجراء عمليات مشتركة تشمل التحقيقات وتدابير الإنفاذ التي يشارك فيها موظفو الهيئات الإشرافية للدول الأعضاء الأخرى.[517]

يعد التعاون بين الهيئات الإشرافية المختلفة أحد المتطلبات الهامة في قانون مجلس أوروبا كذلك. وتنص الاتفاقية 108 المحدثة على أن الهيئات الإشرافية يجب أن تتعاون مع بعضها بالقدر اللازم لأداء مهامها.[518] وينبغي أن يتم ذلك، على سبيل المثال، من خلال تزويد كل طرف الآخر بأي معلومات ذات صلة ومفيدة وتنسيق التحقيقات والقيام بأعمال مشتركة.[519]

## 4.5. مجلس حماية البيانات الأوروبي

لقد سبق وأن تم وصف أهمية الهيئات الإشرافية المستقلة والاختصاصات الرئيسية التي تتمتع بها بموجب قانون حماية البيانات الأوروبي في هذا الفصل. ويعد مجلس حماية البيانات الأوروبي جهة فاعلة أخرى مهمة فيما يخص ضمان تطبيق قواعد حماية البيانات بشكل فعال ومتسق في مختلف أنحاء الاتحاد الأوروبي.

أنشأت اللائحة العامة لحماية البيانات مجلس حماية البيانات الأوروبي كهيئة في الاتحاد الأوروبي تتمتع بشخصية اعتبارية.[520] وقد جاء خلفاً للفريق عمل المادة 29، [521] والذي أنشأه الأمر التوجيهي الخاص بحماية البيانات لتقديم المشورة للمفوضية بشأن أي تدابير خاصة بالاتحاد الأوروبي تؤثر على حقوق الأفراد فيما يتعلق بمعالجة البيانات الشخصية والخصوصية، وتعزيز التطبيق الموحد للأمر التوجيهي، وتزويد المفوضية بآراء الخبراء بشأن المسائل المتعلقة بحماية البيانات. وقد كان فريق عمل المادة 29 يتألف من ممثلين عن الهيئات الإشرافية للدول الأعضاء في الاتحاد الأوروبي، إلى جانب ممثلين عن المفوضية والمشرف الأوروبي على حماية البيانات.

[514] فريق عمل المادة 29 (2016)، «إرشادات لتحديد الهيئة الإشرافية الرائدة لمراقب أو معالج»، WP 244، بروكسيل، 13 ديسمبر 2016، تمت مراجعتها في 5 أبريل 2017.
[515] اللائحة العامة لحماية البيانات، المادة 60 (1)-(3).
[516] نفس المرجع السابق، المادة 61 (1) و(2).
[517] نفس المرجع السابق، المادة 62 (1).
[518] الاتفاقية 108 المحدثة، المادتان 16 و17.
[519] نفس المرجع السابق، المادة 17.
[520] اللائحة العامة لحماية البيانات، المادة 68.
[521] بموجب الأمر التوجيهي رقم EC/95/46، كان واجباً على فريق عمل المادة 29 تقديم المشورة للمفوضية بشأن أي تدابير خاصة بالاتحاد الأوروبي تؤثر على حقوق الأفراد فيما يتعلق بمعالجة البيانات الشخصية والخصوصية، وتعزيز التطبيق الموحد للأمر التوجيهي، وتزويد المفوضية بآراء الخبراء بشأن المسائل المتعلقة بحماية البيانات. وقد كان فريق عمل المادة 29 يتألف من ممثلين عن الهيئات الإشرافية للدول الأعضاء في الاتحاد الأوروبي، إلى جانب ممثلين عن المفوضية والمشرف الأوروبي على حماية البيانات.

بآراء الخبراء بشأن المسائل المتعلقة بحماية البيانات. وقد كان فريق عمل المادة 29 يتألف من ممثلين عن الهيئات الإشرافية للدول الأعضاء في الاتحاد الأوروبي، إلى جانب ممثلين عن المفوضية والمشرف الأوروبي على حماية البيانات.

وعلى غرار فريق عمل المادة 29، يتألف مجلس حماية البيانات الأوروبي من رؤساء الهيئات الإشرافية لكل دولة عضو والمشرف الأوروبي على حماية البيانات أو ممثليهم.[522] ويتمتع المشرف الأوروبي على حماية البيانات بحقوق تصويت مساوية، ما عدا في الحالات المتعلقة بتسوية النزاعات، حيث يجوز له التصويت فقط على القرارات المتعلقة بالمبادئ والقواعد المطبقة على مؤسسات الاتحاد الأوروبي والتي تتوافق من حيث الجوهر مع تلك الخاصة باللائحة العامة لحماية البيانات. ويحق للمفوضية المشاركة في أنشطة مجلس حماية البيانات الأوروبي واجتماعاته، ولكنها لا تتمتع بحقوق التصويت.[523] هذا وينتخب المجلس رئيسه (يُعهد إليه بتمثيله) ونائبين للرئيس من بين أعضائه بالأغلبية النسبية لمدة خمس سنوات. علاوة على ذلك، يوجد لدى المجلس أيضا أمانة تحت تصرفه، يوفرها المشرف الأوروبي على حماية البيانات، بحيث يحصل المجلس على الدعم التحليلي والإداري واللوجستي.[524]

وتُستعرض مهام مجلس حماية البيانات الأوروبي بالتفصيل في المواد 64 و65 و70 من اللائحة العامة لحماية البيانات، وتشمل واجبات شاملة يمكن تقسيمها إلى ثلاثة أنشطة رئيسية:

- **الاتساق**: يمكن لمجلس حماية البيانات الأوروبي إصدار قرارات ملزمة قانوناً في ثلاث حالات: عندما تتقدم هيئة إشرافية باعتراض معلل وذي صلة موضوعية بحالات تهم نقاط الخدمات الموحدة، وعندما تكون هناك آراء متضاربة حول أيٍّ من الهيئات الإشرافية هي الهيئة «الرائدة"، وأخيراً، عندما لا تطلب الهيئة الإشرافية المختصة رأي مجلس حماية البيانات الأوروبي أو لا تتبعه.[525] وتتمثل المسؤولية الرئيسية لمجلس حماية البيانات الأوروبي في ضمان تطبيق اللائحة العامة لحماية البيانات بشكل متسق في مختلف أنحاء الاتحاد الأوروبي، وهي تلعب دوراً رئيسياً في آلية الاتساق، كما هو موضح في الجزء 5.5.

- **المشورة**: تشمل مهام مجلس حماية البيانات الأوروبي تقديم المشورة للمفوضية بشأن أي مسألة تتعلق بحماية البيانات الشخصية في الاتحاد، مثل تعديلات اللائحة العامة لحماية البيانات، أو مراجعات تشريعات الاتحاد الأوروبي التي تهم معالجة البيانات ويمكن أن تتعارض مع قواعد حماية البيانات في الاتحاد الأوروبي، أو إصدار المفوضية قرارات حول مدى كفاية الضمانات المرتبطة بحماية البيانات (قرارات الكفاية اختصاراً) والتي تتيح نقل البيانات الشخصية إلى بلد ثالث أو منظمة دولية.

- **الإرشاد**: يصدر المجلس أيضاً الإرشادات والتوصيات والممارسات الفضلى لتشجيع التطبيق المتسق للائحة، ويدعم التعاون وتبادل المعرفة بين الهيئات الإشرافية. إضافة إلى ذلك، يجب أن يشجع المجلس جمعيات المراقبين أو المعالجين على وضع مدونات السلوك، وإحداث آليات شهادات التصديق وأختام حماية البيانات.

يجوز الطعن في قرارات مجلس حماية البيانات الأوروبي أمام محكمة العدل التابعة للاتحاد الأوروبي.

## 5.5. آلية الاتساق الخاصة باللائحة العامة لحماية البيانات

تحدد اللائحة العامة لحماية البيانات آلية اتساق لضمان تطبيق اللوائح بشكل متسق في مختلف الدول الأعضاء، تتعاون بموجبها الهيئات الإشرافية مع بعضها البعض، وعند الاقتضاء، مع المفوضية. ويتم استخدام آلية الاتساق في حالتين: تتعلق الأولى بآراء مجلس حماية البيانات الأوروبي في الحالات التي تعتزم فيها هيئة إشرافية مختصة اعتماد تدابير معينة، مثل قائمة عمليات المعالجة التي تتطلب تقييم أثر حماية البيانات (DPIA)، أو تحديد البنود التعاقدية القياسية؛ أمَّا الحالة الثانية فتتعلق بقرارات مجلس حماية البيانات الأوروبي الملزمة للهيئات الإشرافية في الحالات التي تهم نقاط الخدمات الموحدة وحين لا تتبع هيئة إشرافية رأي مجلس حماية البيانات الأوروبي أو لا تطلبه.

[522] اللائحة العامة لحماية البيانات، المادة 68 (3).
[523] نفس المرجع السابق، المادة 68 (4) و(5).
[524] نفس المرجع السابق، المادتان 73 و75.
[525] نفس المرجع السابق، المادة 65.

# 6
# حقـــوق أصحـــاب البيانـــات وإنفاذهـــا

| الاتحاد الأوروبي | المسائل المتناولة | مجلس أوروبا |
|---|---|---|
| **الحق في الإخبار** | | |
| اللائحة العامة لحماية البيانات، المادة 12<br><br>محكمة العدل التابعة للاتحاد الأوروبي، C-473/12، قضية «المعهد المهني للوكلاء العقاريين (IPI) ضد إنغلبرت»، 2013<br>محكمة العدل التابعة للاتحاد الأوروبي، C-201/14، قضية «سمارانديا بارا وآخرون ضد الصندوق الوطني للتأمين الصحي وآخرون»، 2015 | شفافية المعلومات | الاتفاقية 108 المحدثة، المادة 8 |
| اللائحة العامة لحماية البيانات، المادة 13 (1) و(2) والمادة 14 (1) و(2) | محتوى المعلومات | الاتفاقية 108 المحدثة، المادة 8 (1) |
| اللائحة العامة لحماية البيانات، المادة 13 (1) والمادة 14 (3) | وقت تقديم المعلومات | الاتفاقية 108 المحدثة، المادة 9 (1) (ب) |
| اللائحة العامة لحماية البيانات، المادة 12 (1) و(5) و(7) | وسائل تقديم المعلومات | الاتفاقية 108 المحدثة، المادة 9 (1) (ب) |
| اللائحة العامة لحماية البيانات، المادة 13 (2) (د) والمادة 14 (2) (ه)، والمواد 77 و78 و79 | الحق في التقدم بشكاية | الاتفاقية 108 المحدثة، المادة 9 (1) (و) |

| | | |
|---|---|---|
| **الحق في الوصول إلى البيانات** | | |
| اللائحة العامة لحماية البيانات، المادة 15 (1)<br>محكمة العدل التابعة للاتحاد الأوروبي، رقم C-553/07، قضية «مجلس العمدة وضباط القانون في روتردام ضد م. إ. إ. رايكيبور»، 2009<br>محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-141/12 وC-372/12، قضية «ي. س. ضد وزارة الهجرة والإدماج واللجوء» وقضية «وزارة الهجرة والإدماج واللجوء ضد م. و س.»، 2014<br>محكمة العدل التابعة للاتحاد الأوروبي، C-434/16، قضية «بيتر نوفاك ضد المفوض المعني بحماية البيانات»، 2017 | حق صاحب البيانات في الوصول إلى بياناته | الاتفاقية 108 المحدثة، المادة 9 (1) (ب)<br>المحكمة الأوروبية لحقوق الإنسان، قضية «ليندر ضد السويد»، رقم 9248/81، 1987 |
| **الحق في التصحيح** | | |
| اللائحة العامة لحماية البيانات، المادة 16 | تصحيح البيانات الشخصية الخاطئة | الاتفاقية 108 المحدثة، المادة 9 (1) (ه)<br>المحكمة الأوروبية لحقوق الإنسان، قضية «جماليتين تشانلي ضد تركيا»، رقم 22427/04، 2008<br>المحكمة الأوروبية لحقوق الإنسان، قضية «تشيوبوتارو ضد مولدوفا»، رقم 27138/04، 2010 |
| **الحق في المحو** | | |
| اللائحة العامة لحماية البيانات، المادة 17 (1) | محو البيانات الشخصية | الاتفاقية 108 المحدثة، المادة 9 (1) (ه)<br>المحكمة الأوروبية لحقوق الإنسان، قضية «سيفيرستيت وايبرغ وآخرون ضد السويد»، رقم 62332/00، 2006 |
| محكمة العدل التابعة للاتحاد الأوروبي، C-131/12، قضية «'غوغل إسبانيا' وشركة 'غوغل' ضد الوكالة الإسبانية لحماية البيانات وماريو كوستيخا غونزاليس» [الغرفة الكبرى]، 2014<br>قضية غرفة التجارة والصناعة والحرف اليدوية والزراعة في ليتشي ضد سالفاتوري ماني،2017 | الحق في النسيان | |
| **الحق في تقييد المعالجة** | | |
| اللائحة العامة لحماية البيانات، المادة 18 (1) | الحق في تقييد استخدام البيانات الشخصية | |
| اللائحة العامة لحماية البيانات، المادة 19 | الالتزام الخاص بالإشعار | |
| **الحق في نقل البيانات** | | |
| اللائحة العامة لحماية البيانات، المادة 20 | الحق في نقل البيانات | |

| | | |
|---|---|---|
| **الحق في الاعتراض** | | |
| اللائحة العامة لحماية البيانات، المادة 21 (1)<br>محكمة العدل التابعة للاتحاد الأوروبي، C-398/15، قضية غرفة التجارة والصناعة والحرف اليدوية والزراعة في ليتشي ضد سالفاتوري ماني،2017 | الحق في الاعتراض بسبب الوضع الخاص لصاحب البيانات | التوصية المتعلقة بالتنميط، المادة 3.5<br>الاتفاقية 108 المحدثة، المادة 9 (1) (د) |
| اللائحة العامة لحماية البيانات، المادة 21 (2) | الحق في الاعتراض على استخدام البيانات لأغراض تسويقية | التوصية المتعلقة بالتسويق المباشر، المادة 1.4 |
| اللائحة العامة لحماية البيانات، المادة 21 (5) | الحق في الاعتراض بوسائل آلية | |
| **الحقوق المتعلقة باتخاذ القرارات الآلية والتنميط** | | |
| اللائحة العامة لحماية البيانات، المادة 22 | الحقوق المتعلقة باتخاذ القرارات الآلية والتنميط | الاتفاقية 108 المحدثة، المادة 9 (1) (أ) |
| اللائحة العامة لحماية البيانات، المادة 21 | الحق في الاعتراض على اتخاذ القرارات آلياً | |
| اللائحة العامة لحماية البيانات، المادة 13 (2) (و) | الحق في تفسير معقول | الاتفاقية 108 المحدثة، المادة 9 (1) (ج) |
| **سبل الانتصاف والمسؤولية والعقوبات والتعويضات** | | |
| الميثاق، المادة 47<br>محكمة العدل التابعة للاتحاد الأوروبي، C-362/14، قضية «ماكسيميليان شريمز ضد المفوض المعني بحماية البيانات» [الغرفة الكبرى]، 2015<br>اللائحة العامة لحماية البيانات، المواد من 77 إلى 84 | فيما يخص انتهاكات قانون حماية البيانات الوطني | الاتفاقية الأوروبية لحقوق الإنسان، المادة 13 (فقط بالنسبة للدول الأعضاء في مجلس أوروبا)<br>الاتفاقية 108 المحدثة، المواد 9 (1) (و) و12 و15 و16 إلى 21<br>المحكمة الأوروبية لحقوق الإنسان، قضية «ك. أ. ضد فنلندا»، رقم 02/2872، 2008<br>المحكمة الأوروبية لحقوق الإنسان، قضية «بيريوك ضد ليتوانيا»، رقم 03/23373، 2008 |
| لائحة حماية البيانات الخاصة بمؤسسات الاتحاد الأوروبي، المادتان 34 و49<br>محكمة العدل التابعة للاتحاد الأوروبي، C-28/08 P، قضية «المفوضية الأوروبية ضد شركة 'بافاريان لاغر' المحدودة» [الغرفة الكبرى]، 2010 | فيما يخص انتهاكات قانون الاتحاد الأوروبي من قبل مؤسسات وهيئات الاتحاد | |

تعتمد فعالية القواعد القانونية بشكل عام، وحقوق أصحاب البيانات بشكل خاص، إلى حد كبير على وجود آليات مناسبة لإنفاذها. ففي العصر الرقمي، أصبحت معالجة البيانات أمراً شائعاً، كما تتزايد صعوبة فهمها بالنسبة للأفراد. وللتخفيف من اختلالات القوة بين أصحاب البيانات والمراقبين، تم منح الأفراد حقوقاً معينة لممارسة سيطرة أكبر على معالجة معلوماتهم الشخصية. وهكذا، فإن المادة 8 (2) من ميثاق الاتحاد الأوروبي للحقوق الأساسية، وهي وثيقة تشكل قانون الاتحاد الأوروبي الأساسي ولها قيمة أساسية في النظام القانوني للاتحاد الأوروبي، تنص على حق الفرد في الوصول إلى بياناته والحق في تصحيحها. في المقابل، أنشأ قانون الاتحاد الأوروبي الثانوي - لا سيما اللائحة العامة لحماية البيانات - إطاراً قانونياً متماسكاً يسهم في تمكين أصحاب البيانات من خلال تزويدهم بحقوق تتعلق بمراقبي البيانات. وإلى جانب حقي الوصول والتصحيح، تقر اللائحة العامة لحماية البيانات بسلسلة من الحقوق الأخرى، مثل الحق في المحو («الحق في النسيان»)، والحق في الاعتراض على معالجة البيانات أو تقييدها، والحقوق المتعلقة باتخاذ القرارات الآلية والتنميط. كما تمت إضافة ضمانات مماثلة إلى الاتفاقية 108 المحدثة لتمكين أصحاب البيانات من ممارسة سيطرة فعالة على بياناتهم. وتستعرض المادة 9 الحقوق التي ينبغي أن يكون الأفراد قادرين على ممارستها فيما يتعلق بمعالجة بياناتهم الشخصية. هذا ويجب على الأطراف المتعاقدة التأكد من أن هذه الحقوق متاحة لكل صاحب بيانات ضمن ولايتها القضائية، وأن تكون مصحوبة بوسائل قانونية وعملية فعالة لتمكين أصحاب البيانات من ممارستها.

علاوةً على منح الحقوق للأفراد، من المهم أيضاً إرساء آليات تمكن أصحاب البيانات من الطعن في انتهاكات حقوقهم، وتحميل المراقبين مسؤولية هذه الانتهاكات والمطالبة بالتعويض. ويقتضي الحق في الانتصاف الفعال، كما هو مكفول بموجب الاتفاقية الأوروبية لحقوق الإنسان والميثاق، توفير سبل الانتصاف القضائية لكل شخص.

## 1.6. حقوق أصحاب البيانات

### النقاط الرئيسية

- يحق لكل صاحب بيانات الحصول على معلومات حول معالجة أي مراقب لبياناته الشخصية، مع مراعاة استثناءات محدودة.
- يتمتع أصحاب البيانات بالحقوق التالية:
  - الوصول إلى البيانات الخاصة بهم والحصول على معلومات معينة حول المعالجة؛
  - تصحيح بياناتهم من طرف المراقب الذي يقوم بمعالجتها في حال كانت خاطئة؛
  - طلب محو بياناتهم من المراقب، حسب الاقتضاء، إذا كان هذا الأخير يعالج بياناتهم بشكل غير قانوني؛
  - الحق في تقييد المعالجة مؤقتاً؛
  - نقل بياناتهم إلى مراقب آخر في ظروف معينة.
- علاوة على ذلك، يحق لأصحاب البيانات الاعتراض على المعالجة بناء على ما يلي:
  - أسباب متعلقة بوضعهم الخاص؛
  - استخدام بياناتهم لأغراض التسويق المباشر.
- يحق لأصحاب البيانات ألا يخضعوا لقرارات تستند فقط إلى المعالجة الآلية، بما في ذلك التنميط، التي تكون لها آثار قانونية أو تؤثر بشكل كبير عليهم. يحق لأصحاب البيانات كذلك:
  - الحصول على تدخل بشري من جانب المراقب؛
  - التعبير عن وجهة نظرهم والطعن في قرار يستند إلى المعالجة الآلية.

## 1.1.6. الحق في الإخبار

وفقًا **لقانون مجلس أوروبا وقانون الاتحاد الأوروبي**، فإن مراقبي عمليات المعالجة ملزمون بإخبار صاحب البيانات عند جمع البيانات الشخصية بشأن المعالجة المزمع إجراؤها. ولا يعتمد هذا الالتزام على طلب من صاحب البيانات، بل يجب على المراقب أن يمتثل بشكل استباقي للالتزام، بغض النظر عما إذا كان صاحب البيانات يبدي اهتماماً بالمعلومات أم لا.

وفي قانون مجلس أوروبا، وفقاً للمادة 8 من الاتفاقية 108 المحدثة، يجب أن تحرص الأطراف المتعاقدة على أن يقوم المراقبون بإطلاع أصحاب البيانات على هويتهم ومكان إقامتهم المعتاد، والأساس القانوني للمعالجة والغرض منها، وفئات البيانات الشخصية التي تتم معالجتها، ومتلقي بياناتهم الشخصية (إن وجدوا) وكيف يمكنهم ممارسة حقوقهم بموجب المادة 9، والتي تتضمن حقوق الوصول والتصحيح والانتصاف القانوني. كما يجب إطلاع أصحاب البيانات على أي معلومات إضافية تعتبر ضرورية لضمان معالجة البيانات الشخصية بشكل منصف وشفاف. ويوضح التقرير التفسيري للاتفاقية 108 المحدثة أن المعلومات المقدمة لأصحاب البيانات «ينبغي أن تكون متاحة بسهولة وسهلة القراءة ومفهومة ومكيفة مع أصحاب البيانات ذوي الصلة»[526]

أما في قانون الاتحاد الأوروبي، يقتضي مبدأ الشفافية أن تكون أي معالجة للبيانات الشخصية شفافة بشكل عام بالنسبة للأفراد. ويحق للأفراد معرفة أي البيانات الشخصية يتم جمعها أو استخدامها أو معالجتها وكيف يتم ذلك، كما أن من حقهم الاطلاع على المخاطر والضمانات والحقوق المكفولة لهم فيما يتعلق بالمعالجة.[527] وهكذا، فإن المادة 12 من اللائحة العامة لحماية البيانات تحدد التزاماً شاملاً واسع النطاق للمراقبين فيما يخص تقديم معلومات شفافة و/أو تبيين كيفية ممارسة أصحاب البيانات لحقوقهم.[528] ويجب أن تكون المعلومات موجزة وشفافة ومفهومة ويسهل الوصول إليها، كما يجب أن تستخدم لغة واضحة وبسيطة. هذا ويجب تقديمها كتابياً، بما يشمل استخدام الوسائل الإلكترونية عند الاقتضاء، ويمكن تقديمها شفهياً بناءً على طلب صاحب البيانات وفي حال تم إثبات هويته بما لا يدع مجالاً للشك. كما يجب تقديم المعلومات دون تأخير أو تكلفة مبالغ فيهما.[529]

وتتناول المادتان 13 و14 من اللائحة العامة لحماية البيانات حق أصحاب البيانات في أن يتم إخبارهم، سواء في الحالات التي يتم فيها جمع البيانات الشخصية منهم مباشرةً، أو في الحالات التي لم يتم فيها الحصول على البيانات منهم.

وقد تم توضيح نطاق الحق في الإخبار والقيود المفروضة عليه بموجب قانون الاتحاد الأوروبي في السوابق القضائية لمحكمة العدل التابعة للاتحاد الأوروبي.

مثال: في قضية «المعهد المهني للوكلاء العقاريين (IPI) ضد إنغلبرت»،[530] طُلب من محكمة العدل التابعة للاتحاد الأوروبي تفسير المادة 13 (1) من الأمر التوجيهي رقم 46/95. وقد أعطت هذه المادة للدول الأعضاء حرية الاختيار فيما إذا كانت ستعتمد تدابير تشريعية لتقييد نطاق حق صاحب البيانات في أن يتم إخباره عند الضرورة لحماية حقوق وحريات الآخرين ومنع الجرائم أو انتهاكات الأخلاقيات في المهن المنظمة والتحقيق فيها، من بين أمور أخرى. هذا ويعتبر المعهد المهني للوكلاء العقاريين هيئة مهنية خاصة بهؤلاء في بلجيكا تتولى مسؤولية ضمان الامتثال للممارسة السليمة لمهنة الوكيل العقاري. وقد طلب المعهد من محكمة وطنية أن تقضي بأن المدعى عليهم قد انتهكوا القواعد المهنية وأن تأمرهم بالتوقف عن ممارسة مختلف أنشطة الوكالات العقارية. وقد استند الإجراء إلى أدلة قدمها محققون خواص استخدمهم المعهد.

[526] التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 68.
[527] اللائحة العامة لحماية البيانات، الحيثية 39.
[528] نفس المرجع السابق، المادتان 13 و14؛ الاتفاقية 108 المحدثة، المادة 8 (1) (ب).
[529] اللائحة العامة لحماية البيانات، المادة 12 (5)؛ الاتفاقية 108 المحدثة، المادة 9 (1) (ب).
[530] محكمة العدل التابعة للاتحاد الأوروبي، C-473/12، قضية « المعهد المهني للوكلاء العقاريين (IPI) ضد جوفري إنغلبرت وآخرون»، 7 نوفمبر 2013.

وقد كانت لدى المحكمة الوطنية شكوك حول قيمة أدلة المحققين، بالنظر إلى إمكانية الحصول عليها دون احترام متطلبات حماية البيانات في التشريع البلجيكي، ولا سيما الالتزام بإخبار أصحاب البيانات بمعالجة بياناتهم الشخصية قبل جمع تلك المعلومة. وقد أشارت محكمة العدل التابعة للاتحاد الأوروبي إلى أن المادة 13 (1) تنص على أنه «يجوز» للدول الأعضاء أن تنص في قانونها الوطني على استثناءات من الالتزام بإخبار أصحاب البيانات بمعالجة بياناتهم، ولكنها ليست ملزمة بذلك. وبما أن المادة 13 (1) تتضمن منع الجرائم الجنائية أو انتهاكات الأخلاقيات والتحقيق فيها وكشفها ومتابعة مرتكبيها كأسباب يمكن للدول الأعضاء من خلالها تقييد حقوق الأفراد، فإن نشاط هيئة مثل المعهد المهني للوكلاء العقاريين والمحققين الخاصين الذين يعملون نيابة عنه يمكن أن يستند إلى هذا الحكم. ومع ذلك، إذا لم تقدم دولة عضو مثل هذا الاستثناء، فيجب إخبار أصحاب البيانات.

مثال: في قضية «سمارانداً بارا وآخرون ضد الصندوق الوطني للتأمين الصحي وآخرون»،[531] أوضحت محكمة العدل التابعة للاتحاد الأوروبي ما إذا كان قانون الاتحاد الأوروبي يمنع هيئة إدارية عامة وطنية من نقل البيانات الشخصية إلى هيئة إدارية عامة أخرى للمعالجة فيما بعد، دون إبلاغ أصحاب البيانات بنقلها ومعالجتها. في هذه القضية، لم تبلغ الوكالة الوطنية لإدارة الضرائب المدعين بعزمها نقل بياناتهم إلى الصندوق الوطني للتأمين الصحي قبل أن تقوم بنقلها.

واعتبرت محكمة العدل التابعة للاتحاد الأوروبي أن شرط إخبار صاحب البيانات بمعالجة بياناته الشخصية بموجب قانون الاتحاد الأوروبي «هو أكثر أهمية لأنه يؤثر على ممارسة أصحاب البيانات لحقهم في الوصول إلى البيانات التي تتم معالجتها والحق في تصحيحها [...] وحقهم في الاعتراض على معالجة تلك البيانات». ويتطلب مبدأ المعالجة المنصفة إخبار أصحاب البيانات بنقل بياناتهم إلى هيئة عامة أخرى لتخضع للمزيد من المعالجة من طرف هذه الأخيرة. ووفقًا للمادة 13 (1) من الأمر التوجيهي رقم 46/95، يجوز للدول الأعضاء تقييد الحق في الإخبار إذا كان ذلك ضرورياً لحماية مصلحة اقتصادية مهمة للدولة، بما في ذلك المسائل الضريبية. لكن يجب فرض هذه القيود من خلال تدابير تشريعية. ونظراً لأنه لم يتم تحديد لا البيانات التي يتم نقلها ولا الترتيبات التفصيلية لنقل البيانات في إجراء تشريعي، وإنما فقط في بروتوكول بين الهيئتين العامتين، فإنه لم يتم استيفاء شروط الاستثناء بموجب قانون الاتحاد الأوروبي. وبالتالي كان ينبغي إخبار المدعين مسبقًا بنقل بياناتهم إلى الصندوق الوطني للتأمين الصحي وبمعالجة هذه الهيئة للبيانات فيما بعد.

**مضمون المعلومات**

بموجب المادة 8 (1) من الاتفاقية 108 المحدثة، يلتزم المراقب بتقديم أي معلومات تضمن معالجة منصفة وشفافة للبيانات الشخصية إلى صاحب البيانات، بما في ذلك:

- هوية المراقب ومكان إقامته المعتاد أو مؤسسته؛
- الأساس القانوني للمعالجة المزمع إجراؤها وأغراضها؛
- فئات البيانات الشخصية المعالجة؛
- المتلقون أو فئات المتلقين للبيانات الشخصية، إن وجدوا؛
- الطرق التي يمكن لأصحاب البيانات من خلالها ممارسة حقوقهم.

وبموجب اللائحة العامة لحماية البيانات، عندما يتم جمع البيانات الشخصية من صاحب البيانات، فإن المراقب ملزم بتقديم المعلومات التالية إلى صاحب البيانات في وقت حصوله على البيانات الشخصية:[532]

- هوية المراقب والمعلومات اللازمة للاتصال به، بما في ذلك التفاصيل الخاصة بالمسؤول عن حماية البيانات، إن وجدت؛
- الغرض والأساس القانوني للمعالجة، أي العقد أو الالتزام القانوني؛
- المصلحة الشرعية لمراقب البيانات، إذا كانت توفر الأساس للمعالجة؛
- المتلقون وفئات المتلقين المحتملين للبيانات الشخصية؛
- ما إذا كان سيتم نقل البيانات إلى بلد ثالث أو منظمة دولية، وما إذا كان ذلك يعتمد على قرار الكفاية المرتبطة بحماية البيانات أو يعتمد على ضمانات مناسبة؛

[531] محكمة العدل التابعة للاتحاد الأوروبي، C-201/14، قضية «سمارانداً بارا وآخرون ضد الصندوق الوطني للتأمين الصحي وآخرون»، 1 أكتوبر 2015.
[532] اللائحة العامة لحماية البيانات، المادة 13 (1).

- الفترة التي سيتم فيها تخزين البيانات الشخصية. وفي حال كان تحديد هذه الفترة غير ممكن، إبراز المعايير المعتمدة لتحديد فترة تخزين البيانات؛
- حقوق أصحاب البيانات فيما يتعلق بالمعالجة، من قبيل حقوق الوصول والتصحيح والمحو وتقييد المعالجة أو الاعتراض عليها؛
- ما إذا كانت إتاحة البيانات الشخصية مطلوبة بموجب القانون أو العقد، وما إذا كان صاحب البيانات ملزماً بإتاحة بياناته الشخصية، وكذلك العواقب في حال عدم إتاحة البيانات الشخصية؛
- اتخاذ القرار آلياً، بما في ذلك التنميط؛
- الحق في التقدم بشكاية إلى هيئة إشرافية؛
- وجود حق سحب الموافقة.

في حالات اتخاذ القرار آلياً، بما في ذلك التنميط، يجب أن يتلقى أصحاب البيانات معلومات مفيدة حول المنطق الذي ينطوي عليه التنميط وأهميته والانعكاسات المتوقع مواجهتها جراء المعالجة.

وفي الحالات التي لا يتم فيها الحصول على البيانات الشخصية من صاحب البيانات مباشرة، يجب على مراقب البيانات إشعار الفرد بمصدر البيانات الشخصية. وعلى أي حال، يجب على المراقب، من بين أمور أخرى، إخبار أصحاب البيانات بوجود عملية اتخاذ القرار آلياً، بما يشمل التنميط.[533] وأخيراً، إذا كان المراقب يعتزم معالجة البيانات الشخصية لغرض آخر غير الذي تم إبلاغه لصاحب البيانات، فإن مبادئ حصر الغرض والشفافية تقتضي أن يقوم بتزويد صاحب البيانات بمعلومات حول هذا الغرض الجديد. ويجب على المراقبين تقديم المعلومات قبل أي معالجة إضافية. بتعبير آخر، في الحالات التي يكون فيها صاحب البيانات قد أعطى موافقته على معالجة البيانات الشخصية، يجب أن يحصل المراقب على موافقة جديدة من صاحب البيانات إذا تغير غرض معالجة البيانات أو إذا تمت إضافة أغراض أخرى.

**وقت تقديم المعلومات**

تميز اللائحة العامة لحماية البيانات بين سيناريوهين اثنين ونقطتين زمنيتين يجب على مراقب البيانات تقديم المعلومات فيهما إلى صاحب البيانات:

- عندما يتم الحصول على البيانات الشخصية مباشرة من صاحب البيانات، يجب على المراقب إشعار صاحب البيانات بجميع المعلومات والحقوق ذات الصلة الخاصة به بموجب اللائحة العامة لحماية البيانات في وقت الحصول على البيانات.[534]
إذا كان المراقب يعتزم إخضاع البيانات الشخصية لمزيد من المعالجة لغرض مختلف، فيجب عليه تقديم جميع المعلومات ذات الصلة قبل إجراء المعالجة.
- في حال عدم الحصول على البيانات الشخصية من صاحب البيانات مباشرةً، يكون المراقب ملزماً بتقديم المعلومات المتعلقة بالمعالجة إلى صاحب البيانات «في غضون فترة معقولة بعد الحصول على البيانات الشخصية لا تقل عن شهر واحد»، أو قبل الكشف عن البيانات لطرف ثالث.

ينص التقرير التفسيري للاتفاقية 108 المحدثة على أنه إذا كان إخبار أصحاب البيانات غير ممكن عند بدء المعالجة، فيمكن أن يتم في مرحلة لاحقة، مثلاً عندما يكون المراقب على اتصال بصاحب البيانات لأي سبب من الأسباب.[536]

**مختلف طرق تقديم المعلومات**

بموجب كل من قانون مجلس أوروبا وقانون الاتحاد الأوروبي، يجب أن تكون المعلومات التي يتعين على المراقب تقديمها لأصحاب البيانات موجزة وشفافة ومفهومة ويسهل الوصول إليها. ويجب تقديمها كتابيا أو بوسائل أخرى بما في ذلك الوسائل الإلكترونية، باستخدام لغة واضحة وبسيطة وسهلة الفهم. وعند تقديم المعلومات، يمكن للمراقب استخدام الأيقونات الموحدة لتقديم المعلومات بطريقة تسهل

[533] اللائحة العامة لحماية البيانات، المادتان 13 (2) و14 (2) (و).
[534] نفس المرجع السابق، المادة 13 (1) و(2)، النص التمهيدي حيث تشير اللائحة العامة لحماية البيانات إلى المعلومات المتعلقة بالالتزام بالتطبيق في «وقت الحصول على البيانات الشخصية».
[535] نفس المرجع السابق، المادتان 13 (3) و14 (3)؛ انظر أيضاً الإشارة إلى فترات زمنية معقولة وبدون تأخير مبالغ فيه في الاتفاقية 108 المحدثة، المادة 8 (1) (ب).
[536] التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 70.

رؤيتها وفهمها.[537] على سبيل المثال، يمكن استخدام أيقونة تمثل قفلًا للإشارة إلى أن البيانات يتم جمعها و/أو تشفيرها بصورة آمنة. هذا و يمكن لأصحاب البيانات أن يطلبوا الحصول على المعلومات بصورة شفهية. ويجب أن تكون المعلومات مجانية، ما لم تكن طلبات صاحب البيانات بلا أساس بشكل واضح أو مبالغ فيها (أي متكررة).[538] ويعد الوصول السهل إلى المعلومات أمراً بالغ الأهمية بالنسبة لقدرة صاحب البيانات على ممارسة حقوقه المنصوص عليها بموجب قانون حماية البيانات في الاتحاد الأوروبي.

يقتضي مبدأ المعالجة المنصفة أن يسهل على أصحاب البيانات فهم المعلومات. ويجب استخدام اللغة المناسبة للمخاطبين. كما يجب أن يتماشى مستوى ونوع اللغة المستخدمة مع ما الجمهور المستهدف، مثلا، ما إذا كان من البالغين أو الأطفال، وما إذا كان من عامة الناس أو من الخبراء الأكاديميين. هذا ويتناول رأي فريق عمل المادة 29 حول زيادة تنسيق أحكام الإخبار مسألة كيفية موازنة هذا الجانب من المعلومات المفهومة، وهذا يعزز فكرة ما يسمى بالإشعارات ذات الطبقات المتعددة،[539] والتي تسمح لصاحب البيانات بتحديد درجة التفصيل التي يفضلها. ومع ذلك، فإن طريقة تقديم المعلومات هذه لا تعفي المراقب من التزامه بموجب المادة 13 والمادة 14 من اللائحة العامة لحماية البيانات، إذ يظل ملزماً بتقديم جميع المعلومات إلى صاحب البيانات.

وتتمثل إحدى أكثر الطرق فعالية لتقديم المعلومات في وضع بنود إخبار مناسبة على الصفحة الرئيسية للمراقب، مثل سياسة خصوصية الموقع الإلكتروني. ومع ذلك، جزء كبير من الناس لا يستخدمون الإنترنت، وهو ما يجب أن تأخذه سياسة الإخبار الخاصة بالشركة أو الهيئة العامة بعين الاعتبار.

قد يبدو إشعار الخصوصية بشأن معالجة البيانات الشخصية على صفحة إلكترونية على النحو التالي:

**من نحن؟**

«مراقب البيانات» هو فندق «بيد أند بريكفست سي أند يو»، الكائن في [العنوان: xxx]، رقم الهاتف: xxx؛ الفاكس: xxx؛ البريد الإلكتروني: info@c&u.com؛ تفاصيل الاتصال بالمسؤول عن حماية البيانات: [xxx].

يشكل إشعار الإخبار الخاص بالبيانات الشخصية جزءاً من الشروط والأحكام التي تؤطر خدماتنا الفندقية.

**ما هي البيانات التي نجمعها منك؟**

نجمع منك البيانات الشخصية التالية: اسمك وعنوانك البريدي ورقم هاتفك وعنوان بريدك الإلكتروني ومعلومات الإقامة ورقم بطاقة الائتمان والخصم وعناوين بروتوكول الإنترنت أو أسماء المجالات الخاصة بأجهزة الكمبيوتر التي استخدمتها للدخول إلى موقعنا.

**لماذا نجمع بياناتك؟**

إننا نقوم بمعالجة بياناتك بناء على موافقتك ولأغراض إجراء الحجوزات، ولإبرام وتنفيذ العقود المتعلقة بالخدمات التي نقدمها لك، وللامتثال للمتطلبات التي يفرضها القانون، من قبيل قانون الرسوم المحلية، والذي يقتضي منا جمع البيانات الشخصية لتمكين دفع ضريبة المدينة عن الإقامة.

**كيف نعالج بياناتك؟**

سيتم الاحتفاظ ببياناتك الشخصية لمدة ثلاثة أشهر. لا تخضع بياناتك لإجراءات القرارات الآلية.

يتبع فندق «بيد أند بريكفست سي أند يو» إجراءات أمنية صارمة لضمان عدم إتلاف معلوماتك الشخصية أو ضياعها أو الكشف عنها لطرف ثالث دون إذنك ولمنع الوصول غير المصرح به. ويتم الاحتفاظ بأجهزة الكمبيوتر التي تخزن المعلومات في بيئة آمنة مع تقييد الوصول إليها ماديا، كما أننا نستخدم جدران حماية آمنة وإجراءات أخرى لتقييد الوصول الإلكتروني. وفي حال كان يجب نقل البيانات إلى طرف ثالث، فإننا نطلب من هذا الأخير اتخاذ تدابير مماثلة لحماية بياناتك الشخصية.

[537] ستعمل المفوضية الأوروبية على تعزيز المعلومات التي ستقدمها الأيقونات والإجراءات الخاصة بتوفير الأيقونات الموحدة عن طريق أعمال مفوضة؛ انظر اللائحة العامة لحماية البيانات، المادة 12 (8).

[538] اللائحة العامة لحماية البيانات، المادة 12 (1) و(5) و(7) والاتفاقية 108 المحدثة، المادة 9 (1) (ب).

[539] فريق عمل المادة 29 (2004)، الرأي 2004/10 حول زيادة تنسيق أحكام الإخبار، 100 WP، بروكسيل، 25 نوفمبر 2004.

إن كافة المعلومات التي نجمعها أو نسجلها مقتصرة على مكاتبنا، وحدهم الأشخاص الذين يحتاجون إلى المعلومات لأداء واجباتهم بموجب هذا العقد يُمنحون حق الوصول إلى البيانات الشخصية. عند الحاجة إلى معلومات لتحديد هويتك، سنطلب ذلك صراحة منك. وقد نطلب منك التعاون مع تحرياتنا الأمنية قبل الكشف عن المعلومات لك. هذا ويمكنك تحديث المعلومات الشخصية التي تقدمها لنا في أي وقت من خلال التواصل معنا مباشرة.

**ما هي حقوقك؟**

لديك الحق في الوصول إلى بياناتك، أو الحصول على نسخة من بياناتك، أو طلب محوها أو تصحيحها، أو طلب نقل بياناتك إلى مراقب آخر.

يمكنك التواصل معنا على info@c&u.com بخصوص طلباتك. يجب أن نجيب على طلبك في غضون شهر واحد، ولكن إذا كان طلبك شديد التعقيد أو تلقينا الكثير من الطلبات الأخرى، فسنبلغك بإمكانية تمديد هذه الفترة لشهرين آخرين.

**الوصول إلى بياناتك الشخصية**

لديك الحق في الوصول إلى بياناتك، وعند الطلب، في معرفة الأسباب الكامنة وراء معالجة البيانات، وطلب محوها أو تصحيحها، إلى جانب الحق في عدم الخضوع لقرار آلي بحت دون أخذ آرائك بعين الاعتبار. يمكنك التواصل معنا على info@c&u.com بخصوص طلباتك. لديك أيضاً الحق في الاعتراض على المعالجة وسحب موافقتك والتقدم بشكاية لدى الهيئة الإشرافية الوطنية إذا اعتبرت أن معالجة البيانات هذه تنتهك القانون، والمطالبة بالتعويض عن الضرر الذي حدث نتيجة للمعالجة غير المشروعة.

**الحق في التقدم بشكاية**

تقتضي اللائحة العامة لحماية البيانات من المراقب إخبار أصحاب البيانات بآليات الإنفاذ بموجب القانون الوطني وقانون الاتحاد الأوروبي في حالات خرق البيانات الشخصية. ويجب على المراقب إخبار أصحاب البيانات بحقهم في التقدم بشكاية تخص خرق البيانات الشخصية لدى هيئة إشرافية، وإذا لزم الأمر، لدى محكمة وطنية.[540] وينص قانون مجلس أوروبا أيضاً على حق أصحاب البيانات في أن يتم إخبارهم بوسائل ممارسة حقوقهم، بما في ذلك الحق في الانتصاف المنصوص عليه في المادة 9 (1) (و).

**إعفاءات من الالتزام بالإخبار**

تقدم اللائحة العامة لحماية البيانات استثناءً للالتزام بالإخبار. فبموجب المادة 13 (4) والمادة 14 (5) من اللائحة العامة لحماية البيانات، لا ينطبق الالتزام بإخبار صاحب البيانات إذا كانت لدى هذا الأخير بالفعل كافة المعلومات ذات الصلة.[541] إضافة إلى ذلك، في حال عدم الحصول على البيانات الشخصية من صاحب البيانات، لن ينطبق الالتزام بالإخبار إذا كان تقديم المعلومات مستحيلًا أو غير متناسب، لا سيما عندما تتم معالجة البيانات الشخصية لأغراض الأرشفة التي تخدم المصلحة العامة، أو لأغراض البحث العلمي أو التاريخي، أو لأغراض إحصائية.[542]

علاوة على ذلك، تتمتع الدول الأعضاء بهامش تقدير بموجب اللائحة العامة لحماية البيانات لحصر الالتزامات والحقوق المقدمة للأفراد بموجب اللائحة إذا كان ذلك تدبيراً ضرورياً ومتناسباً في مجتمع ديمقراطي، مثلاً لحماية الأمن القومي والعام، أو الدفاع، أو حماية التحقيقات والإجراءات القضائية، أو حماية المصالح الاقتصادية والمالية، إلى جانب المصالح الخاصة الأكثر أهمية من مصالح حماية البيانات.[543]

يجب أن تكون الاستثناءات أو القيود ضرورية في مجتمع ديمقراطي ومتناسبة مع الهدف المنشود. وفي حالات استثنائية للغاية، مثلاً بسبب التوصيات الطبية، قد تتطلب حماية صاحب البيانات تقييد الشفافية؛ ويتعلق هذا الأمر بشكل خاص بتقييد حق الوصول المكفول لكل صاحب بيانات.[544] ولكن كحد أدنى من الحماية، يجب أن يحترم القانون الوطني جوهر الحقوق والحريات الأساسية المحمية بموجب قانون الاتحاد الأوروبي،[545] وهذا يقتضي أن يتضمن القانون الوطني أحكاماً محددة توضح الغرض من المعالجة، وفئات البيانات الشخصية المعنية، والضمانات والمتطلبات الإجرائية الأخرى.[546]

[540] اللائحة العامة لحماية البيانات، المادة 13 (2) (د) والمادة 14 (2) (ه)؛ الاتفاقية 108 المحدثة، المادة 8 (1) (و).
[541] نفس المرجع السابق، المادة 13 (4) والمادة 14 (5) (أ).
[542] نفس المرجع السابق، المادة 14 (5) من (ب) إلى (ه).
[543] اللائحة العامة لحماية البيانات، المادة 23 (1).
[544] اللائحة العامة لحماية البيانات، المادة 15.

عندما يتم جمع البيانات لأغراض البحث العلمي أو التاريخي، أو لأغراض إحصائية، أو لأغراض الأرشفة من أجل المصلحة العامة، يمكن أن ينص قانون الاتحاد أو قوانين الدول الأعضاء على استثناءات من الالتزام بالإخبار في حال كان محتملاً أن يجعل هذا الالتزام تحقيق الأغراض المحددة مستحيلاً أو يعيقه بشكل كبير.[547]

هذا وتوجد قيود مماثلة في قانون مجلس أوروبا، حيث يمكن أن تخضع الحقوق الممنوحة لأصحاب البيانات بموجب المادة 9 من الاتفاقية 108 المحدثة لقيود بموجب المادة 11 من الاتفاقية ذاتها، وذلك ضمن إطار شروط صارمة. علاوة على ذلك، وفقًا للمادة 8 (2) من الاتفاقية 108 المحدثة، فإن الالتزام بشفافية المعالجة المفروض على المراقبين لا ينطبق عندما يتوفر صاحب البيانات بالفعل على المعلومات.

**حق الفرد في الوصول إلى بياناته الخاصة**

يقر **قانون مجلس أوروبا** صراحة بالحق في وصول الفرد إلى بياناته الخاصة في المادة 9 من الاتفاقية 108 المحدثة. وتنص هذه الأخيرة على أن لكل فرد الحق في الحصول، عند الطلب، على معلومات حول معالجة البيانات الشخصية المتعلقة به، والتي يتم تقديمها بصورة مفهومة. وإلى جانب مقتضيات الاتفاقية 108 المحدثة، تقر السوابق القضائية للمحكمة الأوروبية لحقوق الإنسان بالحق في الوصول إلى البيانات. وقد اعتبرت المحكمة الأوروبية لحقوق الإنسان مراراً وتكراراً أن للأفراد الحق في الوصول إلى المعلومات المتعلقة ببياناتهم الشخصية، وأن هذا الحق ينشأ من الحاجة إلى احترام الحياة الخاصة.[548] ومع ذلك، فإن الحق في الوصول إلى البيانات الشخصية المخزنة من قبل المؤسسات العامة أو الخاصة قد يكون محدوداً في ظروف معينة.[549]

يقر قانون **الاتحاد الأوروبي** صراحة بالحق في وصول الفرد إلى بياناته الخاصة في المادة 15 من اللائحة العامة لحماية البيانات، كما يعتبره عنصراً من عناصر الحق الأساسي في حماية البيانات الشخصية في المادة 8 (2) من ميثاق الحقوق الأساسية للاتحاد الأوروبي.[550] ويُعد حق الفرد في الوصول إلى بياناته الشخصية عنصراً رئيسياً في قانون حماية البيانات الأوروبي.[551]

تنص اللائحة العامة لحماية البيانات على أن لكل صاحب بيانات الحق في الوصول إلى بياناته الشخصية وإلى معلومات معينة حول المعالجة، والتي يجب على المراقبين توفيرها. ويحق لكل صاحب بيانات، على وجه الخصوص، الحصول على تأكيد (من المراقب) بخصوص ما إذا كانت البيانات المتعلقة به تخضع للمعالجة أم لا، وعلى معلومات حول ما يلي، على أقل تقدير:

- أغراض المعالجة؛
- فئات البيانات المعنية؛
- المتلقون أو فئات المتلقين الذين يتم الكشف عن البيانات لهم؛
- الفترة التي من المقرر تخزين البيانات فيها، أو في حال لم يكن ذلك ممكنًا، المعايير المعتمدة لتحديد هذه الفترة؛
- وجود حقوق تصحيح البيانات الشخصية أو محوها أو تقييد معالجة البيانات الشخصية؛
- الحق في التقدم بشكاية لدى الهيئة الإشرافية.
- أي معلومات متاحة حول مصدر البيانات التي تخضع للمعالجة في حال لم يتم جمع البيانات من صاحبها؛
- في حالات القرارات الآلية، المنطق المعتمد في أي معالجة آلية للبيانات.

يجب على مراقب البيانات تزويد صاحب البيانات بنسخة من البيانات الشخصية التي تتم معالجتها. ويجب أن تكون المعلومات المقدمة إلى صاحب البيانات واضحة، أي أنه يجب على المراقب التأكد من أن صاحب البيانات يمكنه فهم هذه المعلومات. على سبيل المثال، لا

---

[545] اللائحة العامة لحماية البيانات، المادة 23 (1).

[546] نفس المرجع السابق، المادة 23 (2).

[547] نفس المرجع السابق، المادة 89 (2) و(3).

[548] المحكمة الأوروبية لحقوق الإنسان، قضية «غاسكين ضد المملكة المتحدة»، رقم 10454/83، 7 يوليو 1989؛ المحكمة الأوروبية لحقوق الإنسان، قضية «أوديفر ضد فرنسا» [الغرفة الكبرى]، رقم 42326/98، 13 فبراير 2003؛ المحكمة الأوروبية لحقوق الإنسان، قضية «ك. ه. وآخرون ضد سلوفاكيا»، رقم 32881/04، 28 أبريل 2009؛ المحكمة الأوروبية لحقوق الإنسان، قضية «غوديلي ضد إيطاليا»، رقم 33783/09، 25 سبتمبر 2012.

[549] المحكمة الأوروبية لحقوق الإنسان، قضية «ليندر ضد السويد»، رقم 9248/81، 26 مارس 1987.

[550] انظر أيضاً محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-141/12 وC-372/12، قضية «ي. س. ضد وزارة الهجرة والاندماج واللجوء» وقضية «وزارة الهجرة والاندماج واللجوء ضد م. و س.»، 17 يوليو 2014؛ محكمة العدل التابعة للاتحاد الأوروبي، رقم C-615/13 P، قضية «كلاينت أورث/ وشبكة عمل مبيدات الآفات في أوروبا ضد الهيئة الأوروبية للسلامة الغذائية»، المفوضية الأوروبية، 16 يوليو 2015.

[551] محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-141/12 وC-372/12، قضية «ي. س. ضد وزارة الهجرة والاندماج واللجوء» وقضية «وزارة الهجرة والاندماج واللجوء ضد م. و س.»، 17 يوليو 2014.

يكفي إدراج الاختصارات التقنية أو المصطلحات المشفرة أو التسميات المختزلة في الرد على طلب الوصول، ما لم يتم توضيح معنى هذه المصطلحات. عندما يتم اتخاذ القرار آلياً، بما في ذلك التنميط، فإن المنطق العام المعتمد في اتخاذ القرار آلياً سوف يحتاج إلى تفسير، بما في ذلك المعايير التي تم أخذها بعين الاعتبار عند تقييم صاحب البيانات. وتجدر الإشارة إلى وجود متطلبات مماثلة في **قانون مجلس أوروبا**.[553]

مثال: سيساعد الوصول إلى البيانات الشخصية صاحب البيانات على تحديد ما إذا كانت البيانات صحيحة أم لا. لذلك، من الضروري إخبار صاحب البيانات، بطريقة مفهومة، بالبيانات الشخصية التي تتم معالجتها وأيضاً بالفئات التي تتم معالجة هذه البيانات الشخصية ضمنها، مثل الاسم وعنوان بروتوكول الإنترنت وإحداثيات الموقع الجغرافي ورقم بطاقة الائتمان وغيرها.

عندما لا يتم الحصول على البيانات من صاحبها، ينبغي أن يتضمن الرد على طلب الوصول إلى البيانات معلومات حول مصدرها، ما دامت هذه المعلومات متوفرة. ويجب فهم هذا الحكم في سياق الإنصاف والشفافية والمساءلة. ولا يجوز للمراقب إتلاف المعلومات المتعلقة بمصدر البيانات من أجل إعفائه من الكشف عنها، ما لم يكن الحذف قد حدث على الرغم من تلقي طلب الوصول إلى البيانات، كما أنه لا يزال ملزماً بالامتثال لمتطلبات «المساءلة» العامة الخاصة به.

وكما جاء في السوابق القضائية لمحكمة العدل التابعة للاتحاد الأوروبي، لا يجوز أن يكون الحق في الوصول إلى البيانات الشخصية مقيداً بحدود زمنية غير مبررة. كما يجب إعطاء أصحاب البيانات فرصة معقولة للحصول على معلومات متعلقة بعمليات المعالجة التي حدثت في الماضي.

مثال: في قضية «رايكيبور»،[554] طُلب من محكمة العدل التابعة للاتحاد الأوروبي تحديد ما إذا كان ممكنا أن يقتصر حق الفرد في الوصول إلى معلومات حول متلقي أو فئات متلقي البيانات الشخصية ومحتوى البيانات على عام واحد قبل طلب الوصول إلى البيانات. ولتحديد ما إذا كان تشريع الاتحاد الأوروبي يجيز مثل هذا الحد الزمني، قررت محكمة العدل التابعة للاتحاد الأوروبي تفسير المادة 12 في ضوء أغراض الأمر التوجيهي. وقد بدأت المحكمة بالتأكيد على أن حق الوصول ضروري لتمكين صاحب البيانات من ممارسة الحق المتمثل في قيام المراقب بتصحيح بياناته أو محوها أو حجبها، أو إشعار الأطراف الثالثة التي تم الكشف عن البيانات لها بهذا التصحيح أو المحو أو الحجب. كما أن الحق الفعلي في الوصول إلى البيانات ضروري أيضاً لتمكين أصحاب البيانات من ممارسة حقهم في الاعتراض على معالجة بياناتهم الشخصية أو حقهم في التقدم بشكاية والمطالبة بتعويضات عن الضرر.[555]
ولضمان التأثير العملي للحقوق الممنوحة لأصحاب البيانات، رأت المحكمة أن «هذا الحق يجب بالضرورة أن يكون ذا صلة بالماضي. وإذا لم يكن كذلك، فلن يكون صاحب البيانات في وضع يمكّنه من ممارسة حقه في تصحيح أو محو أو حجب البيانات التي يُفترض أنها مخالفة للقانون أو خاطئة أو رفع دعوى قضائية والحصول على تعويض عن الضرر الذي لحق به».

## 2.1.6. الحق في التصحيح

بموجب **قانون الاتحاد الأوروبي وقانون مجلس أوروبا**، يحق لأصحاب البيانات تصحيح بياناتهم الشخصية. وتعد صحة البيانات الشخصية ضرورية لضمان مستوى عالٍ من حماية البيانات بالنسبة لأصحابها.[556]

[552] اللائحة العامة لحماية البيانات، المادة 15 (1)
[553] انظر الاتفاقية 108 المحدثة، المادة 8 (1) (ج).
[554] محكمة العدل التابعة للاتحاد الأوروبي، رقم C-553/07، قضية «مجلس العمدة وضباط القانون في روتردام ضد م. إ. إ. رايكيبور»، 7 مايو 2009.
[555] اللائحة العامة لحماية البيانات، المواد 15 (1) (ج) و(و) و16 و17 (2) و21، والفصل الثامن.
[556] نفس المرجع السابق، المادة 16 والحيثية 65؛ الاتفاقية 108 المحدثة، المادة 9 (1) (ه).

مثال: في قضية «تشيوبوتارو ضد مولدوفا»،[557] لم يتمكن المدعي من تغيير تسجيل أصله العرقي في السجلات الرسمية من مولدوفي إلى روماني بسبب عدم قدرته على إثبات طلبه. وقد اعتبرت المحكمة الأوروبية لحقوق الإنسان أنه من المقبول أن تطلب الدول أدلة موضوعية عند تسجيل الهوية العرقية للفرد. وعندما يستند هذا الطلب إلى أسس ذاتية بحتة وغير مدعمة بأدلة، يمكن للسلطات أن تقابله بالرفض. غير أن طلب المدعي لم يستند فقط على تصوره الذاتي لأصله العرقي؛ حيث كان قادراً على توفير روابط مع المجموعة العرقية الرومانية يمكن التحقق منها بشكل موضوعي مثل اللغة والاسم والتعاطف وغيرها. ومع ذلك، بموجب القانون المحلي، طُلب من المدعي تقديم دليل على أن والديه كانا ينتميان إلى المجموعة العرقية الرومانية. وبالنظر إلى الحقائق التاريخية لمولدوفا، فقد وضع هذا المطلب حاجزًا لا يمكن تجاوزه أمام تسجيل هوية عرقية غير تلك التي سجلتها السلطات السوفياتية بخصوص والديه. ومن خلال حرمان المدعي من دراسة طلبه في ضوء أدلة يمكن التحقق منها موضوعياً، لم تمتثل الدولة لالتزامها الإيجابي بضمان الاحترام الفعلي للحياة الخاصة للمدعي. وخلصت المحكمة إلى أنه كان هناك انتهاك للمادة 8 من الاتفاقية الأوروبية لحقوق الإنسان.

في بعض الحالات، يكفي أن يطلب صاحب البيانات تصحيح شيء من قبيل تهجئة الاسم أو تغيير العنوان أو رقم الهاتف. ووفقًا **لقانون الاتحاد الأوروبي وقانون مجلس أوروبا**، يجب تصحيح البيانات الشخصية الخاطئة دون تأخير غير مبرر أو مبالغ فيه.[558] ومع ذلك، إذا كانت هذه الطلبات مرتبطة بمسائل مهمة من الناحية القانونية، مثل الهوية القانونية لصاحب البيانات، أو مكان الإقامة الصحيح لغرض تسليم المستندات القانونية، قد لا تكون طلبات التصحيح كافية وقد يحق للمراقب أن يطلب دليلاً على الخطأ المزعوم. ولا يجب أن يضع مثل هذا الطلب عبئاً إثباتياً غير معقول على صاحب البيانات، بحيث يمنعه من تصحيح بياناته. وقد اكتشفت المحكمة الأوروبية لحقوق الإنسان انتهاكات للمادة 8 من الاتفاقية الأوروبية لحقوق الإنسان في عدة حالات لم يتمكن فيها المدعي من الطعن في صحة المعلومات المحفوظة في السجلات السرية.[559]

مثال: في قضية «جماليتين تشانلي ضد تركيا»،[560] اكتشفت المحكمة الأوروبية لحقوق الإنسان وجود انتهاك للمادة 8 من الاتفاقية الأوروبية لحقوق الإنسان في تقرير تضمن معلومات غير صحيحة قُدم من قبل الشرطة خلال الإجراءات الجنائية.

وكان المدعي قد تورط مرتين في إجراءات جنائية بسبب عضويته المزعومة في منظمات غير قانونية ولكن لم تتم إدانته. وعندما تم القبض على المدعي مجدداً واتّهم بارتكاب جريمة جنائية أخرى، قدمت الشرطة إلى المحكمة الجنائية تقريراً بعنوان «استمارة معلومات بشأن جرائم إضافية»، قيل فيها أن مقدم الطلب عضو في منظمتين غير قانونيتين. ولم ينجح طلب المدعي الرامي إلى تعديل التقرير وسجلات الشرطة في تحقيق مسعاه. وقد رأت المحكمة الأوروبية لحقوق الإنسان أن المعلومات الواردة في تقرير الشرطة تندرج في نطاق المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان، حيث إن المعلومات العامة المجمعة بشكل منهجي والمخزنة في الملفات التي تحتفظ بها السلطات يمكن أن تندرج ضمن معنى «الحياة الخاصة». علاوة على ذلك، فإن صياغة تقرير الشرطة كانت خاطئة، كما أن تقديمه إلى المحكمة الجنائية لم يتم وفقاً للقانون المحلي. وبالتالي، خلصت المحكمة إلى وجود انتهاك للمادة 8.

خلال القضايا أو الإجراءات المدنية التي تتم أمام أنظار سلطة عامة لتقرير ما إذا كانت البيانات صحيحة أم لا، يمكن لصاحب البيانات أن يطلب مُدخلة أو ملاحظة لوضعها في ملف البيانات الخاص به تفيد بأنه يطعن في صحة البيانات وأن القرار الرسمي معلق.[561] خلال هذه الفترة، لا يجب على مراقب البيانات تقديم البيانات على أنها صحيحة أو غير قابلة للتعديل، لا سيما لأطراف ثالثة.

## 3.1.6 الحق في المحو («الحق في النسيان»)

يُعد منح أصحاب البيانات الحق في محو بياناتهم أمراً مهماً جداً بالنسبة للتطبيق الفعلي لمبادئ حماية البيانات، ولا سيما مبدأ تقليل البيانات إلى الحد الأدنى (يجب أن تقتصر البيانات الشخصية على ما هو ضروري للأغراض التي تتم من أجلها معالجة هذه البيانات). وبالتالي، فإن حق المحو موجود في الصكوك القانونية لكل من مجلس أوروبا والاتحاد الأوروبي.[562]

[557] المحكمة الأوروبية لحقوق الإنسان، قضية «تشيوبوتارو ضد مولدوفا»، رقم 27138/04، 27 أبريل 2010، الفقرات 51 و59.
[558] اللائحة العامة لحماية البيانات، المادة 16؛ الاتفاقية 108 المحدثة، المادة 9 (1).
[559] المحكمة الأوروبية لحقوق الإنسان، قضية «روتارو ضد رومانيا» [الغرفة الكبرى]، رقم 28341/95، 4 مايو 2000.
[560] المحكمة الأوروبية لحقوق الإنسان، قضية «جماليتين تشانلي ضد تركيا»، رقم 22427/04، 18 نوفمبر 2008، الفقرات 33 و42-43؛ المحكمة الأوروبية لحقوق الإنسان، قضية «داليا ضد فرنسا»، رقم 964/07، 2 فبراير 2010.
[561] اللائحة العامة لحماية البيانات، المادة 18 والحيثية 67.
[562] نفس المرجع السابق، المادة 17.

مثال: في قضية «سيفيرستيت وايبرغ وآخرون ضد السويد»،[563] كان المدعون ينتمون إلى أحزاب سياسية ليبرالية وشيوعية معينة، واشتبهوا في قيام الشرطة بإدراج معلومات متعلقة بهم في سجلاتها الأمنية، مما دفعهم إلى طلب محوها. وقد أعربت المحكمة الأوروبية لحقوق الإنسان عن ارتياحها لأن تخزين البيانات المتنازع بشأنها كان له أساس قانوني وهدف شرعي. ومع ذلك، فيما يتعلق ببعض المدعين، رأت المحكمة الأوروبية لحقوق الإنسان أن استمرار الاحتفاظ بالبيانات كان تدخلاً غير متناسب في حياتهم الخاصة. فعلى سبيل المثال، في حالة أحد المدعين، احتفظت السلطات بمعلومات تزعم بأنه في عام 1969، دعا إلى المقاومة العنيفة للشرطة أثناء المظاهرات. وقد اعتبرت المحكمة الأوروبية لحقوق الإنسان أن هذه المعلومات لا يمكن أن يكون لها أي مصلحة أمنية وطنية ذات صلة موضوعية، لا سيما بالنظر إلى طبيعتها التاريخية. وقد خلصت المحكمة إلى وجود انتهاك للمادة 8 من الاتفاقية الأوروبية لحقوق الإنسان فيما يتعلق بأربعة من المدعين الخمسة، لأنه نظراً للمدة الزمنية الطويلة التي انقضت منذ الأفعال المزعومة للمدعين، فقد انتفت ضرورة مواصلة تخزين بياناتهم.

مثال: في قضية «برونيه ضد فرنسا»،[564] اعترض المدعي على تخزين معلوماته الشخصية في قاعدة بيانات تابعة للشرطة كانت تحتوي على معلومات عن أشخاص مدانين ومتهمين وضحايا. وعلى الرغم من إيقاف الإجراءات الجنائية ضد المدعي، ظهرت تفاصيله في قاعدة البيانات. وقد رأت المحكمة الأوروبية لحقوق الإنسان أنه تم انتهاك المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان. وقد اعتبرت المحكمة في استنتاجها أنه، من الناحية العملية، لم تكن أمام المدعي إمكانية لحذف بياناته الشخصية من قاعدة البيانات. كما نظرت المحكمة الأوروبية لحقوق الإنسان في طبيعة المعلومات المدرجة في قاعدة البيانات واعتبرت أنها تتعارض مع خصوصية المدعي، لأنها تتضمن تفاصيل عن هويته وشخصيته. علاوة على ذلك، اعتبرت المحكمة أن فترة الاحتفاظ بالسجلات الشخصية في قاعدة البيانات، والتي بلغت 20 عاماً، كانت طويلة للغاية، لا سيما أنه لم يسبق لأي محكمة أن أدانت المدعي.

وتقر الاتفاقية 108 المحدثة صراحةً بأن لكل فرد الحق في محو البيانات غير الدقيقة أو الخاطئة أو المعالجة بشكل غير مشروع.[565]

وفي قانون الاتحاد الأوروبي، تُفعّل المادة 17 من اللائحة العامة لحماية البيانات طلبات أصحاب البيانات بمحو البيانات أو حذفها. وينطبق الحق في محو البيانات الشخصية للفرد دون تأخير غير مبرر في الحالات التالية:

- لم تعد البيانات الشخصية ضرورية فيما يتعلق بالأغراض التي تم جمعها أو معالجتها من أجلها؛
- قيام صاحب البيانات بسحب الموافقة التي تستند إليها المعالجة وعدم وجود أي أساس قانوني آخر للمعالجة؛
- اعتراض صاحب البيانات على المعالجة وعدم وجود أسباب شرعية مهيمنة للمعالجة؛
- معالجة البيانات الشخصية بصورة غير مشروعة؛
- ضرورة محو البيانات الشخصية للامتثال لالتزام قانوني في قانون الاتحاد أو قانون الدولة العضو الذي يخضع له المراقب؛
- جمع البيانات الشخصية فيما يتعلق بعرض خدمات مجتمع المعلومات للأطفال وفقاً للمادة 8 من اللائحة العامة لحماية البيانات.[566]

يقع عبء إثبات شرعية معالجة البيانات على المراقبين، لأنهم مسؤولون عن مشروعية المعالجة.[567] ووفقاً لمبدأ المساءلة، يجب أن يكون المراقب قادراً في أي وقت على إثبات وجود أساس قانوني سليم لمعالجة البيانات، وإلا وجب إيقاف المعالجة.[568] وتحدد اللائحة العامة لحماية البيانات استثناءات خاصة بالحق في النسيان، بما في ذلك الحالات التي تكون فيها معالجة البيانات الشخصية ضرورية من أجل ما يلي:

- ممارسة الحق في حرية التعبير والإخبار؛
- الامتثال لالتزام قانوني يتطلب المعالجة بموجب قانون الاتحاد أو قانون الدولة العضو الذي يخضع له المراقب، أو أداء مهمة يتم تنفيذها للمصلحة العامة أو ممارسة الصلاحيات الرسمية المخولة للمراقب؛
- دواعي المصلحة العامة في مجال الصحة العامة؛
- أغراض الأرشفة للمصلحة العامة أو أغراض البحث العلمي أو التاريخي أو لأغراض إحصائية.
- إقامة الدعوات القانونية أو ممارستها أو الدفاع عنها.[569]

وقد أكدت محكمة العدل التابعة للاتحاد الأوروبي على أهمية الحق في المحو لضمان مستوى عالٍ من حماية البيانات.

[563] المحكمة الأوروبية لحقوق الإنسان، قضية «سيفيرستيت وايبرغ وآخرون ضد السويد»، رقم 62332/00، 6 يونيو 2006، الفقرتان 89 و90؛ انظر أيضاً، على سبيل المثال، المحكمة الأوروبية لحقوق الإنسان، قضية «م. ك. ضد فرنسا»، رقم 19522/09، 18 أبريل 2013.

[564] المحكمة الأوروبية لحقوق الإنسان، قضية «برونيه ضد فرنسا»، رقم 21010/10، 18 سبتمبر 2014.

[565] الاتفاقية 108 المحدثة، المادة 9 (1) (ه).

[566] اللائحة العامة لحماية البيانات، المادة 17 (1).

[567] نفس المرجع السابق.

[568] نفس المرجع السابق، المادة 5 (2).

[569] نفس المرجع السابق، المادة 17 (3).

مثال: في قضية «غوغل إسبانيا»،[570] كانت محكمة العدل التابعة للاتحاد الأوروبي مهتمة بما إذا كانت شركة «غوغل» ملزمة بحذف المعلومات القديمة المتعلقة بالصعوبات المالية للمدعي من نتائج قائمة البحث الخاصة بها. ومن بين الأمور التي اعترضت عليها «غوغل»، تحميلها المسؤولية، بحجة أنها توفر فقط رابطًا تشعبياً للصفحة الإلكترونية الخاصة بالجهة الناشرة التي تستضيف المعلومات، وهي في هذه الحالة عبارة عن صحيفة نشرت تقارير عن إفلاس المدعي.[571]

واعتبرت «غوغل» أن طلب حذف معلومات قديمة من صفحة إلكترونية يجب أن يقدم لمضيف هذه الصفحة وليس لـ«غوغل»، والتي يقتصر دورها على توفير رابط إلى الصفحة الأصلية. وقد خلصت محكمة العدل التابعة للاتحاد الأوروبي إلى أن محرك بحث «غوغل»، عندما يبحث في الشبكة عن المعلومات والصفحات، وعندما يقوم بترتيب المحتوى لتقديم نتائج البحث، يصبح مسؤولاً عن معالجة البيانات التي تترتب عنها مسؤوليات والتزامات بموجب قانون الاتحاد الأوروبي.

وقد أوضحت محكمة العدل التابعة للاتحاد الأوروبي أن محركات البحث على الإنترنت ونتائج البحث التي تقدم بيانات شخصية من شأنها تكوين ملف مفصل عن شخص معين.[572] حيث تنشر محركات البحث المعلومات الواردة في قائمة النتائج في كل مكان. وفي ضوء الخطورة المحتملة لهذا التدخل، فإنه لا يمكن تبريره فقط بالمصلحة الاقتصادية التي يتحصل عليها مشغل محرك البحث من هذه المعالجة. لذلك، يتعين السعي لتحقيق توازن عادل لا سيما بين المصلحة الشرعية لمستخدمي الإنترنت في الوصول إلى المعلومات والحقوق الأساسية لصاحب البيانات بمقتضى المادتين 7 و8 من ميثاق الحقوق الأساسية للاتحاد الأوروبي. وفي مجتمع أصبح يطغى عليه الطابع الرقمي بصورة متزايدة، يعد المطلب المتمثل في صحة البيانات الشخصية وعدم تجاوزها لما هو ضروري (أي بالنسبة للمعلومات المتاحة لعموم الجمهور) أساسياً لضمان مستوى عال من حماية البيانات للأفراد. «وفي سياق هذه المعالجة، يتعين على المراقب، في إطار مسؤولياته وصلاحياته وقدراته، ضمان استجابة المعالجة لمتطلبات» قانون الاتحاد الأوروبي، لكي يكون للضمانات القانونية المعمول بها تأثير كامل.[573] وهذا يعني أن الحق في محو البيانات الشخصية عند تقادم المعالجة أو عندما لا تكون ضرورية يشمل أيضا مراقب البيانات الذي ينسخ المعلومات.[574]

وبخصوص ما إذا كان مطلوباً من «غوغل» إزالة الروابط المتعلقة بالمدعي أم لا، رأت محكمة العدل التابعة للاتحاد الأوروبي أنه في ظل ظروف معينة، يحق للأفراد طلب محو البيانات الشخصية. ويمكن الاحتجاج بهذا الحق عندما تكون المعلومات المتعلقة بالفرد خاطئة أو غير ملائمة أو غير ذات صلة أو مبالغ فيها لأغراض معالجة البيانات. وأقرت المحكمة أن هذا الحق ليس مطلقاً حيث يجب أن يكون متوازناً مع الحقوق والمصالح الأخرى، ولا سيما مصلحة عامة الناس في الوصول إلى معلومات معينة. ويجب تقييم كل طلب محو على أساس كل حالة على حدة لتحقيق التوازن بين الحقوق الأساسية لحماية البيانات الشخصية والحياة الخاصة لصاحب البيانات من جهة، والمصالح الشرعية لجميع مستخدمي الإنترنت، بما في ذلك الناشرين، من جهة أخرى. وقد قدمت المحكمة إرشادات حول العوامل التي يجب مراعاتها أثناء عملية الموازنة هذه. كما تعتبر طبيعة المعلومات المعنية عاملاً مهماً للغاية. فإذا كانت المعلومات تتعلق بالحياة الخاصة للفرد، ولا توجد مصلحة عامة في إتاحتها، فإن حماية البيانات والخصوصية ستبطل حق عامة الناس في الوصول إلى هذه المعلومات. وعلى العكس من ذلك، إذا تبين أن صاحب البيانات شخصية عامة، أو أن المعلومات ذات طبيعة تبرر إتاحتها لعامة الناس، فإن مصلحة الجمهور الراجحة بالوصول إلى المعلومات قد تبرر التدخل في الحقين الأساسيين لصاحب البيانات المتمثلين في حماية البيانات والخصوصية.

بعد إصدار الحكم، اعتمد فريق عمل المادة 29 مبادئ توجيهية لتنفيذ حكم محكمة العدل التابعة للاتحاد الأوروبي.[575] وتشمل المبادئ التوجيهية قائمة بالمعايير المشتركة التي يتعين على الهيئات الإشرافية اعتمادها للتعامل مع الشكايات المتعلقة بطلبات الأفراد بخصوص

[570] محكمة العدل التابعة للاتحاد الأوروبي، C-131/12، قضية «غوغل إسبانيا' وشركة 'غوغل' ضد الوكالة الإسبانية لحماية البيانات وماريو كوستيجا غونزاليس» [الغرفة الكبرى]،13 مايو 2014، الفقرات من 55 إلى 58.

[571] اعترضت «غوغل» أيضاً على تطبيق قواعد حماية البيانات في الاتحاد الأوروبي نظراً لأن الشركة تأسست في الولايات المتحدة وأن معالجة البيانات الشخصية المعنية في القضية تمت أيضاً في الولايات المتحدة. وكانت الحجة الثانية لعدم قابلية تطبيق قانون حماية البيانات في الاتحاد الأوروبي تتعلق بالادعاء بأن محركات البحث لا يمكن النظر إليها ك«مراقبين» فيما يتعلق بالبيانات المعروضة في نتائجها حيث ليس لديها معرفة بالبيانات ولا تمارس أي مراقبة عليها. لكن محكمة العدل التابعة للاتحاد الأوروبي رفضت كلتا الحجتين، معتبرة أن الأمر التوجيهي رقم EC/95/46 كان قابلاً للتطبيق في هذه الحالة. وواصلت فحص نطاق الحقوق المكفولة، ولا سيما الحق في محو البيانات الشخصية.

[572] نفس المرجع السابق، الفقرات 36 و38 و80-81 و97.

[573] نفس المرجع السابق، الفقرات من 81 إلى 83.

[574] محكمة العدل التابعة للاتحاد الأوروبي، رقم C-131/12، قضية «غوغل إسبانيا وشركة غوغل ضد الوكالة الإسبانية لحماية البيانات وماريو غونزاليس» [الغرفة الكبرى]، 13 مايو 2014، الفقرة 88. انظر أيضاً فريق عمل المادة 29 (2014)، المبادئ التوجيهية حول تنفيذ حكم محكمة العدل التابعة للاتحاد الأوروبي بخصوص قضية «غوغل إسبانيا وشركة غوغل ضد الوكالة الإسبانية لحماية البيانات وماريو غونزاليس»، WP 255 ،C-131/12، بروكسيل، 26 نوفمبر 2014 وتوصية لجنة الوزراء 2012(3) الموجهة للدول الأعضاء بشأن حماية حقوق الإنسان فيما يتعلق بمحركات البحث، 4 أبريل 2012.

[575] فريق عمل المادة 29، المبادئ التوجيهية حول تنفيذ حكم محكمة العدل التابعة للاتحاد الأوروبي الخاص بقضية «غوغل إسبانيا وشركة غوغل ضد الوكالة الإسبانية لحماية البيانات وماريو غونزاليس» WP 255 ،C-131/12، بروكسيل، 26 نوفمبر 2014.

محو البيانات، مع شرح ما ينطوي عليه الحق في المحو وتوجيه هذه الهيئات فيما يتعلق بعملية موازنة الحقوق. وتشدد المبادئ التوجيهية على أن التقييمات يجب أن تتم على أساس كل حالة على حدة. وبما أن حق المرء في أن ينسى ليس مطلقاً، فإن نتيجة الطلب قد تختلف باختلاف الحالة. وقد تجلى هذا الأمر بوضوح في السوابق القضائية لمحكمة العدل التابعة للاتحاد الأوروبي عقب قضية «غوغل».

في قضية «غرفة التجارة في ليتشي ضد ماني»،[576] كان على محكمة العدل التابعة للاتحاد الأوروبي النظر فيما إذا كان لشخص ما الحق في محو بياناته الشخصية المنشورة في سجل عام للشركات بعد تصفية شركته. حيث طلب السيد ماني من غرفة التجارة في ليتشي حذف بياناته الشخصية من ذلك السجل، بعد أن تبين له أن من الممكن لعملاء محتملين أن يطلعوا على السجل ويجدوا أنه كان سابقاً مديراً لشركة أعلنت إفلاسها قبل أزيد من عقد من الزمن. واعتقد المدعي أن هذه المعلومات ستأثر سلباً على العملاء المحتملين.

وفي إطار الموازنة بين حق السيد ماني في حماية بياناته الشخصية ومصلحة عامة الناس في الوصول إلى المعلومات، نظرت محكمة العدل التابعة للاتحاد الأوروبي أولاً في الغرض من السجل العام. وأشارت إلى أن القانون ينص على الإفصاح، خاصة الأمر التوجيهي للاتحاد الأوروبي الذي يهدف إلى جعل معلومات الشركات متاحة بسهولة أكثر لأطراف ثالثة. وبالتالي، ينبغي أن يكون بإمكان هؤلاء الوصول والتمكن من الاطلاع على الوثائق الأساسية وغيرها من المعلومات الخاصة بالشركة، «ولا سيما تفاصيل الأشخاص المصرح لهم بإلزام الشركة». وقد كان الغرض من الإفصاح أيضاً ضمان اليقين القانوني في ظل المعاملات التجارية المكثفة بين الدول الأعضاء، من خلال الحرص على وصول أطراف ثالثة إلى جميع المعلومات ذات الصلة بالشركات في جميع أنحاء الاتحاد الأوروبي.

كما أشارت المحكمة إلى أنه حتى بعد مرور الوقت، وحتى بعد حل الشركة، غالباً ما تظل الحقوق والالتزامات القانونية المتعلقة بها قائمة. وقد تكون النزاعات المتعلقة بحل الشركة طويلة الأمد، وقد تثار أسئلة تتعلق بشركة ما ومديريها والقائمين على تصفيتها لسنوات عديدة بعد تصفية الشركة. وقد رأت المحكمة أنه، في ضوء مجموعة السيناريوهات المحتملة والاختلافات في فترات التقادم الخاصة بكل دولة عضو، «يبدو من المستحيل في الوقت الحالي تحديد مهلة زمنية واحدة، تبدأ من يوم حل الشركة ويتم في نهايتها القول بأن إدراج مثل هذه البيانات في السجل والإفصاح عنها لم يعودا ضروريين». ونظراً للهدف الشرعي من الإفصاح والصعوبات في تحديد فترة يمكن في نهايتها حذف البيانات الشخصية من السجل دون الإضرار بمصالح الأطراف الثالثة، تبين للمحكمة أن قواعد حماية البيانات في الاتحاد الأوروبي لا تضمن حق محو البيانات الشخصية للأشخاص الذين يوجدون في وضع السيد ماني.

عندما يخرج المراقب البيانات الشخصية للعلن ويُطلب منه حذفها، يكون مراقب البيانات ملزماً ويجب أن يتخذ خطوات «معقولة» لإبلاغ المراقبين الآخرين الذين يعالجون نفس البيانات بطلب صاحب البيانات المتعلق بمحوها. ويجب أن تأخذ أنشطة المراقب بعين الاعتبار التكنولوجيا المتاحة وتكلفة التنفيذ.[577]

## 4.1.6. الحق في تقييد المعالجة

تمكن المادة 18 من اللائحة العامة لحماية البيانات أصحاب البيانات من منع المراقب مؤقتاً من معالجة بياناتهم الشخصية. وقد يطلب أصحاب البيانات من المراقب تقييد عملية المعالجة عندما:

- يتم الطعن في صحة البيانات الشخصية؛
- تكون المعالجة غير مشروعة ويطالب صاحب البيانات بتقييد استخدام البيانات الشخصية بدلاً من محوها؛
- يجب الاحتفاظ بالبيانات من أجل رفع دعوى قضائية أو الدفاع عنها؛
- هناك قرار معلق بأن المصالح الشرعية لمراقب البيانات تطغى على مصالح صاحب البيانات.[578]

[576] محكمة العدل التابعة للاتحاد الأوروبي، رقم C-398/15، قضية «غرفة التجارة والصناعة والحرف اليدوية والزراعة في ليتشي ضد سالفاتوري ماني»، 9 مارس 2017.
[577] للائحة العامة لحماية البيانات، المادة 17 (2) والحيثية 66.
[578] نفس المرجع السابق، المادة 18 (1).

قد تشمل الطرق التي يمكن فيها للمراقب تقييد معالجة البيانات الشخصية نقلَ البيانات المختارة مؤقتاً إلى نظام معالجة آخر، وعدم إتاحة البيانات للمستخدمين أو إزالة البيانات الشخصية على أساس مؤقت.[579] ويتعين على المراقب إشعار صاحب البيانات قبل رفع التقييد عن المعالجة.[580]

**الالتزام بالإشعار فيما يتعلق بتصحيح أو محو البيانات الشخصية أو تقييد المعالجة**

يجب على المراقب إبلاغ كل متلق يكشف له عن البيانات الشخصية بأي تصحيح أو محو للبيانات الشخصية أو أي تقييد للمعالجة، طالما أن هذا الأمر ليس مستحيلاً أو غير متناسب.[581] وإذا طلب صاحب البيانات معلومات عن المتلقين، يجب على المراقب تزويده بها.[582]

## 5.1.6. الحق في نقل البيانات

بمقتضى اللائحة العامة لحماية البيانات، لأصحاب البيانات الحق في نقل البيانات في الحالات التي تتم فيها معالجة البيانات الشخصية التي قدموها للمراقب بوسائل آلية بناء على موافقتهم، أو في الحالات التي تكون فيها معالجة البيانات الشخصية ضرورية لتفعيل عقد ما وتتم بوسائل آلية. وهذا يعني أن الحق في نقل البيانات لا ينطبق في الحالات التي تكون فيها معالجة البيانات الشخصية مبنية على أساس قانوني مغاير للموافقة أو العقد.[583]

إذا كان الحق في نقل البيانات قابلا للتطبيق، فإنه يحق لأصحاب البيانات أن تُنقل بياناتهم الشخصية مباشرة من مراقب إلى آخر إذا كان ذلك ممكناً من الناحية التقنية.[584] ومن أجل تسهيل ذلك، يتعين على المراقب تطوير صيغ قابلة للتشغيل البيني تتيح إمكانية نقل البيانات لفائدة أصحاب البيانات.[585] وتنص اللائحة العامة لحماية البيانات على أن هذه الصيغ يجب أن تكون مُهيكلة وشائعة الاستعمال وقابلة للقراءة الآلية لتسهيل التشغيل البيني.[586] ويمكن تعريف قابلية التشغيل البيني بالمعنى الواسع بقدرة النظم المعلوماتية على تبادل البيانات وتمكين مشاركة المعلومات.[587] وفي الوقت الذي يكون فيه الغرض من الصيغ المستخدمة هو تحقيق التشغيل البيني، فإن اللائحة العامة لحماية البيانات لا تفرض توصيات معينة بشأن الصيغة المحددة التي سيتم توفيرها؛ إذ قد تختلف الصيغ باختلاف القطاعات.[588]

وفقاً للمبادئ التوجيهية لفريق عمل المادة 29، «يدعم [الحق في نقل البيانات] اختيار المستخدم وسيطرته وتمكينه»، بهدف منح أصحاب البيانات السيطرة على بياناتهم الشخصية.[589] وتوضح المبادئ التوجيهية العناصر الرئيسية لإمكانية نقل البيانات، والتي تشمل:

- حق أصحاب البيانات في تلقي بياناتهم الشخصية التي تتم معالجتها من قبل المراقب في صيغة مُهيكلة وشائعة الاستخدام وقابلة للقراءة آلياً وقابلة للتشغيل البيني؛
- الحق في نقل البيانات الشخصية من مراقب بيانات إلى آخر دون عائق إذا كان ذلك ممكناً من الناحية التقنية؛
- نظام مراقبة البيانات - حين يستجيب المراقب لطلب نقل البيانات، فإنه يتبع تعليمات صاحب البيانات، ما يعني أنه ليس مسؤولاً عن امتثال الجهة المتلقية لقانون حماية البيانات، نظراً لأن صاحب البيانات هو من يقرر من ستنقل إليه البيانات؛
- لا تمس ممارسة الحق في نقل البيانات بأي حق آخر كما هو الحال بالنسبة لأي حق آخر وارد في اللائحة العامة لحماية البيانات.

الحق في الاعتراض

---

[583] نفس المرجع السابق، الحيثية 68 والمادة 20 (1).

[584] نفس المرجع السابق، المادة 20 (2).

[585] نفس المرجع السابق، الحيثية 68 والمادة 20 (1).

[586] نفس المرجع السابق، الحيثية 68.

[587] المفوضية الأوروبية، بلاغ حول نظم معلوماتية أقوى وأذكى من أجل الحدود والأمن، بلاغ (2016) رقم 205 النهائي، 2 أبريل 2016.

[588] فريق عمل المادة 29 (2016)، المبادئ التوجيهية بشأن الحق في نقل البيانات، WP 242، 13 ديسمبر 2016 والتي تمت مراجعتها في 5 أبريل 2017، ص. 13.

[589] نفس المرجع السابق.

[590] انظر أيضاً المحكمة الأوروبية لحقوق الإنسان، قضية «م. س. ضد السويد»، رقم 20837/92، 27 أغسطس 1997 (حيث تم إرسال بيانات طبية دون موافقة أو إمكانية الاعتراض)؛ المحكمة الأوروبية لحقوق الإنسان، قضية «لينجر ضد السويد»، رقم 9248/81، 26 مارس 1987؛ المحكمة الأوروبية لحقوق الإنسان، قضية «موزلي ضد المملكة المتحدة»، رقم 48009/08، 10 مايو 2011.

[591] اللائحة العامة لحماية البيانات، الحيثية 69؛ المادة 6 (1) (ه) و(و).

[592] الاتفاقية 108 المحدثة، المادة 9 (1) (د)؛ التوصية بشأن التنميط، المادة 5 (3).

## 6.1.6. الحق في الاعتراض

يمكن لأصحاب البيانات الاحتجاج بالحق في الاعتراض على معالجة البيانات الشخصية لأسباب تتعلق بوضعهم الخاص ومعالجة البيانات لأغراض التسويق المباشر. ويمكن ممارسة الحق في الاعتراض بوسائل آلية.

**الحق في الاعتراض لأسباب تتعلق بالأوضاع الخاصة لأصحاب البيانات**

لا يملك أصحاب البيانات حقاً عاماً في الاعتراض على معالجة بياناتهم.[590] وتمكن المادة 21 (1) من اللائحة العامة لحماية البيانات صاحب البيانات من الاعتراض لأسباب تتعلق بوضعه الخاص عندما يكون الأساس القانوني هو أداء المراقب لمهمة تصب في المصلحة العامة، أو حين تكون المعالجة مبنية على المصالح الشرعية للمراقب.[591] كما ينطبق الحق في الاعتراض على أنشطة التنميط. وقد تم الإقرار بحق مماثل في الاتفاقية 108 المحدثة.[592]

ويهدف الحق في الاعتراض لأسباب تتعلق بالوضع الخاص لصاحب البيانات إلى خلق التوازن السليم بين حقوق حماية البيانات الخاصة بصاحب البيانات والحقوق الشرعية للآخرين فيما يخص معالجة بياناته. غير أن محكمة العدل التابعة للاتحاد الأوروبي قد أوضحت أن حقوق صاحب البيانات تطغى «كقاعدة عامة» على المصالح الاقتصادية لمراقب البيانات اعتماداً على «طبيعة المعلومات المعنية ومدى حساسيتها بالنسبة للحياة الخاصة لصاحب البيانات ومصلحة الجمهور في الحصول عليها».[593] وبموجب اللائحة العامة لحماية البيانات، يقع عبء الإثبات على عاتق المراقبين، الذين يجب أن يأتوا بأسباب مقنعة لمواصلة المعالجة.[594] وبالمثل، يوضح التقرير التفسيري للاتفاقية 108 المحدثة أن الأسس المشروعة لمعالجة البيانات (التي قد تلغي حق أصحاب البيانات في الاعتراض) يجب أن يتم توضيحها على أساس كل حالة على حدة.[595]

مثال: في قضية «ماني»،[596] رأت محكمة العدل التابعة للاتحاد الأوروبي أنه بسبب الغرض الشرعي للإفصاح على البيانات الشخصية في سجل الشركات، لا سيما ضرورة حماية مصالح الأطراف الأخرى وضمان اليقين القانوني، فإنه في الأساس، لم يكن للسيد ماني الحق في محو بياناته الشخصية من سجل الشركات. غير أنها تقر بوجود الحق في الاعتراض على المعالجة من خلال إشارتها إلى أنه «لا يمكن استبعاد [...] احتمال وجود أوضاع خاصة تبرر فيها بشكل استثنائي الأسباب المهيمنة والشرعية المتعلقة بوضع الشخص المعني محدودية الوصول إلى البيانات الشخصية المدخلة في السجل، عند انقضاء فترة طويلة بما فيه الكفاية [...] لأطراف ثالثة يمكنهم إثبات مصلحة محددة في اطلاعهم [على هذه البيانات]».

اعتبرت محكمة العدل التابعة للاتحاد الأوروبي أن من مسؤولية المحاكم الوطنية تقييم كل قضية، مع مراعاة جميع الظروف ذات الصلة للفرد وما إذا كانت هناك أسباب شرعية ومهيمنة يمكن أن تبرر بشكل استثنائي وصول أطراف أخرى إلى البيانات الشخصية الواردة في سجلات الشركات بطريقة محدودة. بيد أنها أوضحت أنه في قضية السيد ماني، فمجرد تأثير الإفصاح عن بياناته الشخصية في السجل كما هو مزعوم على عملائه، لا يمكن اعتباره سبباً شرعياً ومهيمناً، كما أن للعملاء المحتملين للسيد ماني مصلحة شرعية في الوصول إلى المعلومات المتعلقة بإفلاس شركته القديمة.

يتجلى تأثير الاعتراض الناجح في أن المراقب قد يتوقف عن معالجة البيانات المعنية. ومع ذلك، تظل عمليات المعالجة التي تخضع لها بيانات صاحب البيانات قبل الاعتراض شرعية.

---

[593] محكمة العدل التابعة للاتحاد الأوروبي، C-131/12، قضية «غوغل إسبانيا وشركة غوغل ضد الوكالة الاسبانية لحماية البيانات، وماريو كوستيخا غونزاليس [الغرفة الكبرى]، 13 مايو 2014، الفقرة 81.

[594] انظر أيضا الاتفاقية 108 المحدثة، تشير المادة 98 (1) (د) إلى أن صاحب البيانات يمكن أن يعترض على معالجة بياناته «ما لم يثبت المراقب أسباب مشروعة للمعالجة تتجاوز مصالحه أو حقوقه وحرياته الأساسية.»

[595] التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 78.

[596] محكمة العدل التابعة للاتحاد الأوروبي، C-398/15، قضية «غرفة التجارة والصناعة والحرف اليدوية والزراعة في ليتشي ضد سالفاتوري ماني»، 9 مارس 2017، الفقرتان 47 و60.

**حق الاعتراض على معالجة البيانات لأغراض التسويق المباشر**

تنص المادة 21 (2) من اللائحة العامة لحماية البيانات على حق خاص في الاعتراض على استعمال البيانات الشخصية لأغراض التسويق المباشر، ما يوضح بشكل أكبر المادة 13 من الأمر التوجيهي الخاص بالخصوصية الإلكترونية. وقد تمت الإشارة إلى هذا الحق في الاتفاقية 108 المحدثة، وكذلك توصية مجلس أوروبا بشأن التسويق المباشر.[597] أما التقرير التفسيري للاتفاقية 108 المحدثة فيوضح أن الاعتراضات على معالجة البيانات لأغراض التسويق المباشر ينبغي أن تؤدي إلى محو أو حذف غير مشروطين للبيانات الشخصية المعنية.[598]

يحق لصاحب البيانات الاعتراض على استخدام بياناته الشخصية لأغراض التسويق المباشرة في أي وقت وبدون مقابل. ويجب إبلاغ أصحاب البيانات بهذا الحق بطريقة واضحة وبشكل منفصل عن أي معلومات أخرى.

**الحق في الاعتراض بواسطة وسائل آلية**

عند استخدام المعلومات الشخصية ومعالجتها لأغراض خدمات مجتمع المعلومات، يجوز لصاحب البيانات ممارسة حقه في الاعتراض على معالجة بياناته الشخصية بواسطة وسائل آلية.

ويقصد بخدمات مجتمع المعلومات أي خدمة تقدم بمقابل وعن بعد بوسائل إلكترونية وبطلب شخصي من متلقي الخدمة.[599]

يجب أن يكون لدى مراقبي البيانات الذين يقدمون خدمات مجتمع المعلومات ترتيبات وإجراءات تقنية مناسبة لضمان إمكانية ممارسة الحق في الاعتراض بالوسائل الآلية بشكل فعال،[600] على سبيل المثال، قد يتضمن ذلك حظر ملفات تعريف الارتباط («كوكيز») على صفحات الويب أو إيقاف تشغيل تتبع تصفح الإنترنت.

**الحق في الاعتراض في إطار أغراض البحث العلمي أو التاريخي أو لأغراض إحصائية**

بموجب قانون الاتحاد الأوروبي، يتعين تفسير البحث العلمي بمعنى واسع، بما في ذلك على سبيل المثال، التطوير والبيان التكنولوجيين، والبحوث الأساسية، والبحوث التطبيقية، والبحوث الممولة من القطاع الخاص.[601] وتشمل الأبحاث التاريخية أيضا البحث لأغراض خاصة بالأنساب، مع مراعاة أن اللائحة لا ينبغي أن تنطبق على الأشخاص المتوفين.[602] ويقصد بالأغراض الإحصائية أي عملية لجمع ومعالجة البيانات الشخصية اللازمة للاستبيانات الإحصائية أو للخروج بنتائج إحصائية،[603] وهنا أيضاً يكون الوضع الخاص لصاحب البيانات الأساس القانوني فيما يتعلق بالحق في الاعتراض على معالجة البيانات الشخصية لأغراض البحث.[604] ويبقى الاستثناء الوحيد هو ضرورة المعالجة لأداء مهمة يتم تنفيذها لأسباب تتعلق بالمصلحة العامة. ومع ذلك، لا ينطبق الحق في المحو عندما تكون المعالجة ضرورية (لأسباب تتعلق بالمصلحة العامة أو بدونها) لأغراض البحث العلمي أو التاريخي أو لأغراض إحصائية.[605]

وتوازن اللائحة العامة لحماية البيانات بين متطلبات البحث العلمي والإحصائي والتاريخي وحقوق أصحاب البيانات من خلال وضع ضمانات واستثناءات محددة في المادة 89. وبالتالي، قد يقدم قانون الاتحاد أو الدول الأعضاء استثناءات فيما يتعلق بالحق في الاعتراض بالقدر الذي يمكن أن يؤدي هذا الحق إلى جعل تحقيق أغراض البحث مستحيلاً أو يضر بها بشكل خطير، وفي حال كانت هذه الاستثناءات ضرورية لتحقيق

[598] التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 79.
[599] الأمر التوجيهي رقم EC/98/34 كما تم تعديله من خلال الأمر التوجيهي رقم EC/98/48 الذي يحدد إجراء خاصاً بتقديم المعلومات في مجال المعايير واللوائح التقنية، المادة 1 (2).
[600] اللائحة العامة لحماية البيانات، المادة 21 (5).
[601] نفس المرجع السابق، الحيثية 159.
[602] نفس المرجع السابق، الحيثية 160.
[603] نفس المرجع السابق، الحيثية 162.
[604] نفس المرجع السابق، المادة 21 (6).
[605] نفس المرجع السابق، المادة 17 (3) (د).

تلك الأغراض.

بموجب **قانون مجلس أوروبا**، تنص المادة 9 (2) من الاتفاقية 108 المحدثة على أن القيود المفروضة على حقوق أصحاب البيانات، بما في ذلك الحق في الاعتراض، قد ينص عليها القانون فيما يتعلق بمعالجة البيانات لأغراض الأرشفة التي تصب في المصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو لأغراض إحصائية عندما لا يكون هناك خطر واضح يهدد بانتهاك الحقوق والحريات الأساسية لأصحاب البيانات.

ومع ذلك، فإن التقرير التفسيري (الفقرة 41) يقر أيضاً بأنه يجب أن تتاح لأصحاب البيانات الفرصة لإعطاء موافقتهم فقط على مجالات معينة من البحث أو أجزاء من المشاريع البحثية في حدود القدر الذي يسمح به الغرض المقصود، وللاعتراض في حال إدراكهم أن المعالجة تطاولت على حقوقهم وحرياتهم بدون أساس شرعي.

وبعبارة أخرى، فإن مثل هذه المعالجة تعتبر بالتالي متوافقة شريطة وجود ضمانات أخرى وأن العمليات، من حيث المبدأ، تستبعد أي استخدام للمعلومات التي تم الحصول عليها لاتخاذ قرارات أو تدابير تتعلق بفرد معين.

## 7.1.6. اتخاذ القرار الفردي آلياً، بما يشمل التنميط

يقصد بالقرارات الآلية القرارات التي تُتخذ باستخدام البيانات الشخصية التي تتم معالجتها فقط بالوسائل الآلية دون أي تدخل بشري. وبمقتضى **قانون الاتحاد الأوروبي**، يجب ألا يخضع أصحاب البيانات لقرارات آلية تترتب عنها آثار قانونية أو تأثيرات مهمة مماثلة. وإذا كان من المحتمل أن يكون لمثل هذه القرارات تأثير كبير على حياة الأفراد من حيث صلتها، على سبيل المثال، بالجدارة الائتمانية أو التوظيف الإلكتروني أو الأداء في العمل أو تحليل السلوك أو الموثوقية، فإن توفير حماية خاصة يعد ضروريا لتجنب العواقب السلبية. ويشمل اتخاذ القرار آليا التنميط، والذي يشمل أي شكل من أشكال التقييم الآلي «للجوانب الشخصية المتعلقة بشخص طبيعي، ولا سيما لتحليل الجوانب المتعلقة بأداء صاحب البيانات في العمل أو وضعه الاقتصادي أو صحته أو تفضيلاته الشخصية أو اهتماماته، أو موثوقيته أو سلوكه أو موقعه أو تحركاته أو التنبؤ بها».[606]

مثال: لإجراء تقييم سريع للجدارة الائتمانية للعميل المستقبلي، تقوم وكالات المراجع الائتمانية بجمع بيانات معينة، مثل كيفية حفاظ العميل على حساباته الائتمانية والخاصة بالخدمات/المرافق وتفاصيل عناوينه السابقة بالإضافة إلى المعلومات المستمدة من المصادر العامة، مثل السجل الانتخابي أو السجلات العامة (بما في ذلك أحكام المحاكم) أو البيانات الخاصة بالإفلاس والإعسار. ويتم إدخال هذه البيانات الشخصية لاحقاً في خوارزمية التنقيط، والتي تحسب القيمة الإجمالية التي تمثل الجدارة الائتمانية للعميل المحتمل.

ووفقاً لفريق عمل المادة 29، فإن الحق في عدم الخضوع لقرارات تستند فقط إلى المعالجة الآلية التي قد يكون لها آثار قانونية على صاحب البيانات أو تؤثر عليه بشكل كبير، يعادل حظراً عاماً، ولا يستدعي من صاحب البيانات السعي بشكل استباقي للاعتراض على مثل هذا القرار.[607]

ومع ذلك، فإنه وفقاً للائحة العامة لحماية البيانات، قد يكون اتخاذ القرارات الآلية ذات الآثار القانونية أو التي تؤثر بشكل كبير على الأفراد أمراً مقبولاً إذا كان ذلك ضرورياً لإبرام عقد أو تنفيذه بين مراقب البيانات وصاحب البيانات، أو إذا قدم صاحب البيانات موافقة صريحة بذلك. بالإضافة إلى ذلك، يُقبل اتخاذ القرار الآلي إذا كان مصرحاً به بموجب القانون وإذا كانت حقوق صاحب البيانات وحرياته ومصالحه المشروعة محمية بشكل مناسب.[608]

هذا وتنص اللائحة العامة لحماية البيانات أيضاً على أنه من بين التزامات المراقب فيما يتعلق بالمعلومات التي يتم تقديمها عند جمع

[606] نفس المرجع السابق، الحيثية 71، المادة 4 (4) والمادة 22. (يُذكر أن مفردة «التنميط» مستعملة هنا بمعنى «التصنيف» ترجمةً عن مصطلح profiling بالإنجليزية وprofilage بالفرنسية).
[607] فريق عمل المادة 29، المبادئ التوجيهية الخاصة بإتخاذ القرارات الفردية الآلية والتنميط لأغراض اللائحة رقم 2016/679، 3 WP 251، أكتوبر 2017، ص. 15.
[608] اللائحة العامة لحماية البيانات، المادة 22 (2).

البيانات الشخصية، وجوب إخبار أصحاب بالبيانات بوجود عملية اتخاذ قرار آلي، بما يشمل التنميط. ولا يتم المساس بالحق في الوصول إلى البيانات الشخصية التي يعالجها المراقب.[610] ويجب ألا تشير المعلومات إلى إجراء التنميط فحسب، بل يجب أن تضم أيضاً معلومات مفيدة حول المنطق المتضمن في التنميط والانعكاسات المنتظرة على الأفراد جراء المعالجة.[611] على سبيل المثال، فإن شركة التأمين الصحي التي تستخدم خاصية اتخاذ القرارات آلياً في التطبيقات الذكية ينبغي منها تزويد أصحاب البيانات بمعلومات عامة حول كيفية عمل الخوارزمية والعوامل التي تستخدمها الخوارزمية لاحتساب أقساط التأمين الخاصة بهم. وبالمثل، عند ممارسة «حق الوصول» (أي حق الولوج)، يمكن لأصحاب البيانات طلب معلومات من المراقب بشأن وجود عملية اتخاذ قرار آلي والمعلومات المفيدة حول المنطق المتضمن.[612]

تهدف المعلومات المقدمة لأصحاب البيانات إلى توفير الشفافية وتمكينهم من تقديم موافقة مستنيرة،عند الاقتضاء، أو طلب تدخل بشري. ويتعين على مراقب البيانات تنفيذ التدابير المناسبة لصون حقوق صاحب البيانات وحرياته ومصالحه الشرعية، وهذا يشمل على الأقل الحق في التدخل البشري من جانب المراقب وإمكانية تعبير صاحب البيانات عن وجهة نظره والطعن في قرار ما اعتمد على المعالجة الآلية لبياناتهم الشخصية.[613]

ولقد قدم الفريق عمل المادة 29 مزيداً من الإرشادات حول استخدام القرار الآلي بموجب اللائحة العامة لحماية البيانات.[614]

بمقتضى قانون مجلس أوروبا، يحق للأفراد عدم الخضوع لقرار سيؤثر عليهم بشكل كبير ويستند فقط إلى المعالجة الآلية دون أخذ وجهات نظرهم بعين الاعتبار.[615] إن شرط مراعاة آراء صاحب البيانات عندما تستند القرارات إلى المعالجة الآلية فقط يعني أن لديهم الحق في الطعن في مثل هذه القرارات، ويجب أن يكونوا قادرين على الطعن في أي بيانات شخصية خاطئة يستخدمها المراقبون، والاحتجاج على ما إذا كان التنميط الذي خضعوا له ذا صلة موضوعية.[616] ومع ذلك، لا يمكن للفرد ممارسة هذا الحق إذا كان القرار الآلي منصوصاً عليه بموجب قانون يخضع له المراقب ويضع أيضاً تدابير مناسبة لصون حقوق صاحب البيانات وحرياته ومصالحه الشرعية. إضافة إلى ذلك، يحق لأصحاب البيانات، عند الطلب، معرفة المنطق وراء معالجة البيانات التي تم تنفيذها.[617] ويعطي التقرير التفسيري للاتفاقية 108 المحدثة مثال التصنيف الائتماني، حيث يجب أن يكون للأفراد الحق في معرفة قرار التصنيف (التنقيط) الإيجابي أو السلبي إلى جانب المنطق الذي تقوم عليه معالجة بياناتهم الشخصية، والذي أدى إلى مثل هذا القرار. «إن فهم هذه العناصر يساهم في الممارسة الفعالة للضمانات الأساسية الأخرى مثل الحق في الاعتراض والحق في تقديم شكاية إلى هيئة مختصة.»[618]

تحدد التوصية بشأن التنميط، وإن لم تكن ملزمة قانوناً، شروط جمع البيانات الشخصية ومعالجتها في سياق التنميط.[619] وتتضمن مقتضيات بشأن ضرورة ضمان أن تكون المعالجة في سياق التنميط عادلة ومشروعة ومتناسبة وتُجرى لأغراض محددة وشرعية. كما تتضمن مقتضيات بشأن المعلومات التي يجب أن يوفرها المراقبون لأصحاب البيانات. هذا وقد أشارت التوصية أيضاً إلى مبدأ جودة البيانات، الذي يقتضي من المراقبين اتخاذ تدابير لتصحيح عوامل عدم دقة البيانات، للحد من المخاطر أو الأخطاء التي قد تترتب على التنميط، وإلى تقييم جودة البيانات والخوارزميات المستخدمة بشكل دوري.

---

[609] نفس المرجع السابق، المادة 12.

[610] نفس المرجع السابق، المادة 15.

[611] نفس المرجع السابق، المادة 13 (2) (و).

[612] نفس المرجع السابق، المادة 15 (1) (ج).

[613] نفس المرجع السابق، المادة 22 (3).

[614] لفريق عمل المادة 29، المبادئ التوجيهية الخاصة بإتخاذ القرارات الفردية الآلية والتنميط لأغراض اللائحة رقم 2016/679، WP 251، 3 أكتوبر 2017.

[615] الاتفاقية 108 المحدثة، المادة 9 (1) (أ).

[616] التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 75.

[617] الاتفاقية 108 المحدثة، المادة 9 (1) (ج).

[618] التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 77.

[619] مجلس أوروبا، توصية لجنة أوروبا (2010)13 الموجهة للدول الأعضاء بشأن حماية الأفراد بخصوص المعالجة الآلية للبيانات الشخصية في سياق التنميط، المادة 5 (5).

## 2.6. سبل الانتصاف والمسؤولية والعقوبات والتعويضات

### النقاط الرئيسية

- وفقاً للاتفاقية 108 المحدثة، يجب أن يحدد القانون الوطني الخاص بالأطراف المتعاقدة سبل الانتصاف والعقوبات المناسبة ضد انتهاكات الحق في حماية البيانات.
- في الاتحاد الأوروبي، توفر اللائحة العامة لحماية البيانات سبل الانتصاف لأصحاب البيانات في الحالات التي تنتهك فيها حقوقهم، فضلاً عن العقوبات المفروضة على المراقبين والمعالجين الذين لا يلتزمون بمقتضيات اللائحة. كما ينص على الحق في التعويض والمسؤولية.
- يحق لأصحاب البيانات تقديم شكاية إلى هيئة إشرافية بشأن الانتهاكات المزعومة للائحة، كما يحق لهم الحصول على سبل انتصاف قضائية فعالة وعلى التعويض.
- في إطار ممارسة حقهم في الحصول على سبل انتصاف فعالة، يمكن لمنظمات غير هادفة للربح تعمل في مجال حماية البيانات تمثيل الأفراد.
- يتحمل المراقب أو المعالج مسؤولية أي ضرر مادي أو غير مادي ينتج عن الانتهاك.
- للهيئة الإشرافية صلاحية فرض غرامات إدارية على الانتهاكات التي تطال اللائحة حيث قد تصل قيمة هذه الغرامات إلى 20 مليون يورو (20.000.000€) أو في حال تعلق الأمر بمؤسسة، فتصل الغرامة إلى 4% من حجم أعمالها الإجمالي العالمي - أو أيهما كان أعلى.

7. يجوز لأصحاب البيانات رفع الانتهاكات التي طالت قانون حماية البيانات إلى المحكمة الأوروبية لحقوق الإنسان، كحل أخير وتحت شروط معينة.

- يحق لأي شخص طبيعي أو اعتباري تقديم شكاية ضد أي قرارات صادرة عن مجلس حماية البيانات الأوروبي لدى محكمة العدل التابعة للاتحاد الأوروبي وفقاً للشروط المنصوص عليها في المعاهدات.

لا يكفي اعتماد الصكوك القانونية لضمان حماية البيانات الشخصية داخل أوروبا. فلجعل قواعد حماية البيانات الأوروبية فعالة، من الضروري إحداث آليات تمكن الأفراد من مواجهة انتهاكات حقوقهم والمطالبة بتعويض عن أي ضرر يتعرضون له. ومن المهم أيضاً أن تتمتع الهيئات الإشرافية بصلاحية فرض عقوبات فعالة ورادعة ومتناسبة مع الانتهاك ذي الصلة.

يمكن للشخص الذي تكون حقوقه على المحك ممارسة الحقوق المنصوص عليها في قانون حماية البيانات؛ وسيكون هذا الشخص هو صاحب البيانات. ومع ذلك، يجوز لأشخاص آخرين -يستوفون المتطلبات اللازمة بموجب القانون الوطني - تمثيل أصحاب البيانات في ممارسة حقوقهم. وينص عدد من التشريعات الوطنية على وجوب تمثيل الأطفال والأشخاص ذوي الإعاقة الذهنية من قبل أولياء أمورهم.[620] وبموجب قانون حماية البيانات في الاتحاد الأوروبي، يجوز لجمعية - يكون هدفها القانوني هو تعزيز حقوق حماية البيانات - تمثيل أصحاب البيانات أمام هيئة إشرافية أو محكمة.[621]

### 1.2.6. الحق في التقدم بشكاية لدى هيئة إشرافية

بموجب **قانوني مجلس أوروبا والاتحاد الأوروبي**، يحق للأفراد التقدم بالطلبات والشكايات لدى الهيئة الإشرافية المختصة إذا رأوا أن معالجة بياناتهم الشخصية لا تتم وفقاً للقانون.

---

[615] الاتفاقية 108 المحدثة، المادة 9 (1) (أ).
[616] التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 75.
[617] الاتفاقية 108 المحدثة، المادة 9 (1) (ج).
[618] التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 77.
[619] مجلس أوروبا، توصية لجنة أوروبا (2010)13 الموجهة للدول الأعضاء بشأن حماية الأفراد بخصوص المعالجة الآلية للبيانات الشخصية في سياق التنميط، المادة 5 (5).
[620] وكالة الاتحاد الأوروبي للحقوق الأساسية (2015)، دليل بشأن القانون الأوروبي المتعلق بحقوق الطفل، لوكسمبورغ، إصدارات المكتب؛ وكالة الاتحاد الأوروبي للحقوق الأساسية (2013)، الأهلية القانونية للأشخاص ذوي الإعاقة الذهنية والأشخاص الذين يعانون من مشاكل عقلية، لوكسمبورغ، إصدارات المكتب.
[621] اللائحة العامة لحماية البيانات، المادة 80.

معالجة بياناتهم الشخصية لا تتم وفقاً للقانون.

وتقر الاتفاقية 108 المحدثة بحق أصحاب البيانات في الاستفادة من مساعدة هيئة إشرافية لممارسة حقوقهم بموجب الاتفاقية، بغض النظر عن جنسيتهم أو إقامتهم.[622] ولا يجوز رفض طلب المساعدة إلا في ظروف استثنائية، وينبغي ألا يتحمل أصحاب البيانات التكاليف والرسوم المتعلقة بالمساعدة.[623]

يمكن العثور على مقتضيات مماثلة في النظام القانوني للاتحاد الأوروبي. حيث تقتضي اللائحة العامة لحماية البيانات من الهيئات الإشرافية اعتماد تدابير لتسهيل التقدم بالشكايات، مثل وضع نموذج إلكتروني لهذا الغرض.[624] ويمكن لصاحب البيانات رفع الشكاية للهيئة الإشرافية في الدولة العضو حيث يوجد محل إقامته المعتاد أو مكان عمله أو مكان الانتهاك المزعوم.[625] يجب التحقيق في الشكايات، ويجب على الهيئة الإشرافية إبلاغ الشخص المعني بنتيجة الإجراءات الخاصة بالادعاء.[626]

يمكن لفت انتباه المشرف الأوروبي على حماية البيانات إلى الانتهاكات التي قد ترتكبها مؤسسات أو هيئات الاتحاد الأوروبي.[627] وفي حالة عدم وجود رد من المشرف الأوروبي على حماية البيانات في غضون ستة أشهر، سيتم اعتبار الشكاية مرفوضة. ويمكن تقديم الطعون ضد قرارات المشرف الأوروبي على حماية البيانات أمام محكمة العدل التابعة للاتحاد الأوروبي في إطار اللائحة (الجماعة الأوروبية) رقم 45/2001 التي تفرض التزاماً بالامتثال لقواعد حماية البيانات على مؤسسات وهيئات الاتحاد الأوروبي.

يجب أن تكون هناك إمكانية للاستئناف أمام المحاكم ضد قرارات الهيئة الإشرافية الوطنية. وينطبق هذا الأمر على صاحب البيانات وكذلك على المراقبين والمعالجين الذين كانوا أطرافاً في الإجراءات المرفوعة أمام هيئة إشرافية.

مثال: في سبتمبر 2017، فرضت هيئة حماية البيانات الإسبانية غرامة على «فيسبوك» لانتهاكه العديد من لوائح حماية البيانات. وقد أدانت الهيئة الإشرافية الشبكة الاجتماعية لجمعها للبيانات الشخصية وتخزينها ومعالجتها، بما في ذلك الفئات الخاصة من البيانات الشخصية، لأغراض دعائية ودون الحصول على موافقة صاحب البيانات. واستند القرار إلى تحقيق تم بمبادرة خاصة من الهيئة الإشرافية.

## 2.2.6. الحق في الحصول على سبل انتصاف قضائية فعالة

بالإضافة إلى الحق في رفع الشكايات للهيئة الإشرافية، يجب أن يكون للأفراد الحق في الحصول على سبل انتصاف قضائية فعالة ورفع قضيتهم أمام المحكمة. إن الحق في الانتصاف القانوني مكرس بشكل تام في التقاليد القانونية الأوروبية، ومعترف به كحق أساسي، بموجب المادة 47 من ميثاق الحقوق الأساسية للاتحاد الأوروبي والمادة 13 من الاتفاقية الأوروبية لحقوق الإنسان.[628]

**بمقتضى قانون الاتحاد الأوروبي**، تتجلى أهمية تزويد أصحاب البيانات بسبل الانتصاف القانونية الفعالة في حالة حدوث انتهاك لحقوقهم في كل من مقتضيات اللائحة العامة لحماية البيانات- التي تنص على الحق في الحصول على سبل انتصاف قضائية فعالة ضد الهيئات الإشرافية والمراقبين والمعالجين- والسوابق القضائية لمحكمة العدل التابعة للاتحاد الأوروبي.

[622] الاتفاقية 108 المحدثة، المادة 18.

[623] نفس المرجع السابق، المادتان 17-16.

[624] اللائحة العامة لحماية البيانات، المادة 57 (2).

[625] نفس المرجع السابق، المادة 77 (1).

[626] نفس المرجع السابق، المادة 77 (2).

[627] لائحة (الجماعة الأوروبية) رقم 45/2001 الصادرة عن البرلمان الأوروبي والمجلس المؤرخة في 18 ديسمبر 2000 بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية من قبل مؤسسات وهيئات الجماعة وبشأن حرية حركة هذه البيانات، الجريدة الرسمية L 8 2001 إ.

[628] انظر على سبيل المثال المحكمة الأوروبية لحقوق الإنسان، قضية «كارابيولو ضد تركيا»، رقم 30083/10، 7 يونيو 2016؛ المحكمة الأوروبية لحقوق الإنسان، قضية «مصطفى سيزجين تانريكولو ضد تركيا»، رقم 27473/06، 18 يوليو 2017.

مثال: في قضية «شريمز»،[629] قضت محكمة العدل التابعة للاتحاد الأوروبي ببطلان قرار «الملاذ الآمن» المتعلق بمدى كفاية الضمانات المرتبطة بحماية البيانات. فقد سمح هذا القرار بنقل الدولي للبيانات من الاتحاد الأوروبي إلى منظمات في الولايات المتحدة أشهدت على نفسها في إطار نظام الملاذ الآمن. وقد اعتبرت محكمة العدل التابعة للاتحاد الأوروبي أن نظام الملاذ الآمن يتضمن العديد من أوجه القصور، مما يضر بحقوق مواطني الاتحاد الأوروبي الأساسية في حماية الخصوصية وحماية البيانات الشخصية والحق في الحصول على سبل انتصاف قانونية فعالة.

فيما يتعلق بانتهاك حقوق الخصوصية وحماية البيانات، سلطت محكمة العدل التابعة للاتحاد الأوروبي الضوء على أن تشريعات الولايات المتحدة تسمح لبعض السلطات العامة بالوصول إلى البيانات الشخصية المنقولة من الدول الأعضاء إلى الولايات المتحدة ومعالجتها بطريقة لا تتوافق مع أغراض النقل الأصلية وبشكل يتجاوز ما كان ضرورياً ومتناسباً مع حماية الأمن القومي. وفيما يتعلق بالحق في الانتصاف الفعال، أشارت المحكمة إلى أن أصحاب البيانات ليس لديهم وسائل إدارية أو قضائية للانتصاف للتمكن من الوصول إلى البيانات المتعلقة بهم وتصحيحها أو محوها، حسب ما تقتضيه الحالة. وخلصت محكمة العدل إلى أن التشريعات التي لا تنص على أي إمكانية لنهج سبل الانتصاف القانونية للوصول إلى بياناتهم الشخصية أو تصحيحها أو محوها «لا تحترم جوهر الحق الأساسي في الحماية القضائية الفعالة، على النحو المنصوص عليه في المادة 47 من الميثاق». وشددت على أن وجود سبل انتصاف قضائية بما يضمن الامتثال للقواعد القانونية أمر متأصل في سيادة القانون.

يجوز للأفراد أو المراقبين أو المعالجين الذين يسعون إلى الطعن في قرار ملزم قانوناً صادر عن هيئة إشرافية رفع دعوى أمام المحكمة.[360] ويجب تفسير مصطلح «القرار» على نطاق واسع، بحيث يشمل ممارسة الهيئات الإشرافية لسلطات التحقيق والمعاقبة والترخيص، وكذلك قرارات رد أو رفض شكاية ما. ومع ذلك، لا يمكن للتدابير غير الملزمة قانوناً، مثل الآراء أو المشورة التي تقدمها الهيئة الإشرافية، أن تشكل موضوع إجراء أمام المحكمة.[631] حيث يجب رفع الدعوى القضائية أمام محاكم الدولة العضو التي أُحدثت فيها الهيئة الإشرافية ذات الصلة.[632]

وفي الحالات التي ينتهك فيها المراقب أو المعالج حقوق صاحب البيانات، يحق لأصحاب البيانات رفع شكاية أمام المحكمة.[633] وبالنسبة للإجراءات التي تم رفعها ضد المراقب أو المعالج، من المهم على وجه الخصوص أن يُقدم للأفراد الخيارفيم يتعلقبمكان اتخاذ الإجراء. ويجوز لهم أن يختاروا القيام بذلك إما في الدولة العضو التي يتوفر فيها المراقب أو المعالج على مؤسسة، أو الدولة العضو التي يوجد بها محل الإقامة الاعتيادي لصاحب البيانات المعني.[634] ويسهل الاحتمال الثاني بشكل كبير على الأفراد ممارسة حقوقهم، لأنه يمكنهم من رفع دعاوى في الدولة التي يقيمون فيها وداخل ولاية قضائية مألوفة. وقد يؤدي حصر مكان الإجراءات ضد المراقبين والمعالجين في الدولة العضو التي يمتلكون فيها مؤسسة إلى ثني أصحاب البيانات المقيمين في الدول الأعضاء الأخرى عن رفع دعوى قضائية، حيث قد ينجم عن ذلك تكاليف سفر وتكاليف إضافية، وقد تكون الإجراءات قيد التنفيذ بلغة أخرى وفي ولاية قضائية أجنبية. إلا أنه يوجد استثناء وحيد يتعلق بالحالات التي يكون فيها المراقب أو المعالج عبارة عن هيئات عامة وتتم المعالجة في إطار ممارسة سلطاتها العامة. في هذه الحالة، تكون محاكم الدولة حيث توجد الهيئة العامة ذات الصلة هي وحدها ذات الاختصاص فيما يتعلق باستقبال الدعوى.[635]

ورغم أنه في معظم الحالات يتم البت في القضايا المتعلقة بقواعد حماية البيانات في محاكم الدول الأعضاء، إلا أنه قد يتم عرض بعض القضايا أمام محكمة العدل التابعة للاتحاد الأوروبي. وينطبق الاحتمال الأول في الحالة التي يسعى فيها صاحب البيانات أو المراقب أو المعالج أو الهيئة الإشرافية إلى اتخاذ إجراء لإلغاء قرار المجلس حماية البيانات الأوروبي . ومع ذلك، يخضع الإجراء لمقتضيات المادة 263 من المعاهدة المنظمة لعمل الاتحاد الأوروبي، مما يعني أنه من أجل أن يكون الإجراء مقبولاً، يجب على هؤلاء الأفراد والجهات إثبات أن قرار مجلس الإدارة يخصهم بشكل مباشر وفردي.

---

[629] محكمة العدل التابعة للاتحاد الأوروبي، رقم C-362/14، قضية «ماكسيميليان شريمز ضد مفوض حماية البيانات» [الغرفة الكبرى]، 6 أكتوبر 2015.
[630] اللائحة العامة لحماية البيانات، المادة 78.
[631] نفس المرجع السابق، الحيثية 143.
[632] نفس المرجع السابق، المادة 78 (3).
[633] نفس المرجع السابق، المادة 79.
[634] نفس المرجع السابق، المادة 79 (2).
[635] نفس المرجع السابق.

ويتعلق السيناريو الثاني بحالات قيام مؤسسات أو هيئات الاتحاد الأوروبي بمعالجة البيانات الشخصية بشكل غير مشروع. ففي الحالات التي تنتهك فيها مؤسسات الاتحاد الأوروبي قانون حماية البيانات، يمكن لأصحاب البيانات رفع دعوى مباشرة أمام المحكمة العامة للاتحاد الأوروبي (وهي جزء من محكمة العدل التابعة للاتحاد الأوروبي). وتعد المحكمة العامة، في المقام الأول، مسؤولة عن الشكايات المتعلقة بانتهاك مؤسسات الاتحاد الأوروبي لقانون الاتحاد. وبالتالي، يمكن التقدم بالشكايات ضد المشرف الأوروبي على حماية البيانات - باعتباره مؤسسة من مؤسسات الاتحاد الأوروبي - لدى المحكمة العامة أيضاً.[636]

مثال: في قضية شركة «بافاريان لاغر»،[637] طلبت الشركة من المفوضية الأوروبية السماح بالوصول إلى المحضر الكامل للاجتماع الذي عقدته المفوضية والذي يُزعم أنه يتعلق بمسائل قانونية ذات صلة بالشركة. وقد رفضت اللجنة طلب الشركة بالوصول إليه على أساس تجاوز هذا الأمر مصالح حماية البيانات.[638] وعليه، قدمت شركة «بافاريان لاغر»، بموجب المادة 32 من لائحة حماية البيانات الخاصة بمؤسسات الاتحاد الأوروبي، شكاية أمام المحكمة الابتدائية (سابقاً قبل المحكمة العامة) بخصوص هذا القرار. وفي قرارها بخصوص (القضية T 194/04)، «شركة بافاريان لاغر المحدودة ضد لجنة المجتمعات الأوروبية»، ألغت المحكمة الابتدائية قرار المفوضية المتعلق برفض طلب الوصول، فيما استأنفت المفوضية الأوروبية هذا القرار أمام محكمة العدل التابعة للاتحاد الأوروبي.

وقد أصدرت محكمة العدل التابعة للاتحاد الأوروبي حكماً (في الغرفة الكبرى) يقضي بإلغاء حكم المحكمة الابتدائية وتأكيد رفض المفوضية الأوروبية لطلب الوصول إلى محضر الاجتماع الكامل، من أجل حماية البيانات الشخصية للأشخاص الموجودين في الاجتماع. واعتبرت محكمة العدل اللجنة محقة في رفضها الافصاح عن تلك المعلومات، بالنظر إلى أن المشاركين لم يعطوا موافقتهم على الكشف عن بياناتهم الشخصية. بالإضافة إلى ذلك، لم تثبت شركة «بافاريان لاغر» الضرورة من الوصول إلى تلك المعلومات.

وأخيراً، يجوز لأصحاب البيانات أو الهيئات الإشرافية أو المراقبين أو المعالجين، في سياق الدعاوى المحلية، أن يلتمسوا من المحكمة الوطنية أن تطلب توضيحاً من محكمة العدل التابعة للاتحاد الأوروبي بشأن تفسير وصلاحية أعمال مؤسسات أو هيئات أو مكاتب أو وكالات الاتحاد الأوروبي. وتُعرف هذه التوضيحات بالأحكام الأولية. ولا يعتبر هذا حلاً مباشراً لمقدم الشكاية، ولكنه يمكّن المحاكم الوطنية من ضمان تطبيق التفسير الصحيح لقانون الاتحاد الأوروبي. ومن خلال آلية الأحكام الأولية هذه، وصلت القضايا المؤثرة -مثل قضايا «ديجيتال رايتس آيرلاند» و«حكومة ولاية كيرنتن وآخرين»[639] و«شريمز»[640] - التي أثرت بشكل كبير على تطوير قانون حماية البيانات في الاتحاد الأوروبي إلى محكمة العدل التابعة للاتحاد الأوروبي.

مثال: لقد تم ضم قضيتي «شركة 'ديجيتال رايتس آيرلاند' المحدودة و'حكومة كيرنتن وآخرين'» المضمومتان التي قامت المحكمة العليا الأيرلندية والمحكمة الدستورية النمساوية برفعهما وتخصان امتثال الأمر التوجيهي رقم EC/2006/24 (الأمر التوجيهي الخاص بالاحتفاظ بالبيانات) لقانون الاتحاد الأوروبي لحماية البيانات. وقد قدمت المحكمة الدستورية النمساوية أسئلة لمحكمة العدل التابعة للاتحاد الأوروبي بشأن صلاحية المواد من 3 إلى 9 من الأمر التوجيهي رقم EC/2006/24 في ضوء المواد 7 و9 و11 من ميثاق الحقوق الأساسية للاتحاد الأوروبي. وشملت هذه التساؤلات ما إذا كانت بعض مقتضيات القانون الاتحادي النمساوي الخاص بالاتصالات المعتمد للأمر التوجيهي الخاص بالاحتفاظ بالبيانات غير متوافقة مع جوانب من الأمر التوجيهي الخاص بحماية البيانات السابق ولائحة حماية البيانات الخاصة بمؤسسات الاتحاد الأوروبي.

[636] اللائحة (الجماعة الأوروبية) رقم 45/2001، المادة 32 (3).

[637] محكمة العدل التابعة للاتحاد الأوروبي، C-28/08 P، قضية «المفوضية الأوروبية ضد شركة 'الجعة البافارية' المحدودة» [الغرفة الكبرى]، 2010.

[638] من أجل تحليل للحجة، انظر المشرف الأوروبي على حماية البيانات (2011)، وصول العامة للوثائق التي تتضمن بيانات شخصية بعد حكم شركة «الجمة البافارية»، بروكسل، المشرف الأوروبي على لحماية البيانات.

[639] محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-293/12 و C-594/12، قضية «شركة 'ديجيتال رايتس آيرلاند' المحدودة ضد وزير الاتصالات والموارد البحرية والطبيعية وآخرين» و«حكومة كيرنتن وآخرين» [الغرفة الكبرى]، 8 أبريل 2014.

[640] محكمة العدل التابعة للاتحاد الأوروبي، رقم C-362/14، قضية «ماكسيميليان شريمز ضد مفوض حماية البيانات» [الغرفة الكبرى]، 6 أكتوبر 2015.

وفي قضية «حكومة كيرنتن وآخرين»، رأى السيد سيتلينغر - أحد المدعين في الدعوى المقامة أمام المحكمة الدستورية - أنه استعمل الهاتف والانترنت والبريد الإلكتروني لأغراض تتعلق بالعمل وبحياته الخاصة. وبالتالي، فإن المعلومات التي أرسلها والتي تلقاها قد مرت عبر شبكات الاتصالات العامة. وبموجب قانون الاتصالات النمساوية لسنة 2003، كان مقدم خدمات الاتصالات الخاصة به ملزماً قانوناً بجمع وتخزين البيانات المتعلقة باستعماله للشبكة. واعتقد السيد سيتلينغر أن جمع وتخزين بياناته الشخصية غير ضروريين للأغراض التقنية الخاصة بإرسال وتلقي المعلومات عبر الشبكات. وبالفعل لم يكن جمع وتخزين البيانات ضرورياً لأغراض الفوترة. وأشار السيد سيتلينغر إلى أنه لم يمنح موافقته لاستعمال بياناته الشخصية بهذه الطريقة، والتي كانت تجمع وتخزن فقط بسبب قانون الاتصالات النمساوية لسنة 2003.

لذلك، رفع السيد سيتلينغر دعوى أمام المحكمة الدستورية النمساوية، حيث ادعى أن الالتزامات القانونية الخاصة بمقدم خدمات الاتصالات قد انتهكت حقوقه الأساسية بموجب المادة 8 من ميثاق الحقوق الأساسية للاتحاد الأوروبي. ونظراً لأن التشريع النمساوي قد نفذ قانون الاتحاد الأوروبي (الأمر التوجيهي الخاص بالاحتفاظ بالبيانات آنذاك)، أحالت المحكمة الدستورية النمساوية الأمر إلى محكمة العدل التابعة للاتحاد الأوروبي لتقرير مدى توافق الأمر التوجيهي مع حقوق الخصوصية وحماية البيانات المنصوص عليها في ميثاق الاتحاد الأوروبي للحقوق الأساسية.

أصدرت الغرفة الكبرى لمحكمة العدل التابعة للاتحاد الأوروبي قراراً بخصوص القضية أدى إلى إلغاء الأمر التوجيهي الخاص بالاحتفاظ بالبيانات التابع للاتحاد الأوروبي. وتبين لمحكمة العدل أن الأمر التوجيهي ينطوي على تدخل خطير بشكل خاص في الحقوق الأساسية للخصوصية وحماية البيانات، دون أن يقتصر هذا التدخل على ما هو ضروري للغاية. وقد سعى الأمر التوجيهي إلى تحقيق هدف مشروع، حيث أتاح للسلطات الوطنية فرصاً إضافية للتحقيق في الجرائم الخطيرة ومقاضاة مرتكبيها، وبالتالي كان أداة قيمة بالنسبة للتحقيقات الجنائية. ومع ذلك، لاحظت محكمة العدل التابعة للاتحاد الأوروبي أن القيود المفروضة على الحقوق الأساسية يجب أن تنطبق فقط إذا كانت ضرورية للغاية ويجب أن تكون مصحوبة بقواعد واضحة ودقيقة فيما يتعلق بنطاقها، إلى جانب وضع ضمانات لصون حقوق الأفراد. وفقاً لمحكمة العدل التابعة للاتحاد الأوروبي، فشل الأمر التوجيهي في استيفاء معيار الضرورة. فلم يضع أولاً قواعد واضحة ودقيقة تحد من مدى التدخل. فبدلاً من اشتراط وجود علاقة بين البيانات المحتفظ بها والجرائم الخطيرة، ينطبق الأمر التوجيهي على جميع البيانات الوصفية لجميع مستخدمي كافة وسائل الاتصال الإلكترونية. وبالتالي، فقد شكل عملياً تدخلاً في حقوق الخصوصية وحماية البيانات لجميع سكان الاتحاد الأوروبي، والذي يمكن اعتباره غير متناسب. ولم يتضمن شروطاً للحد من الأشخاص المصرح لهم بالوصول إلى البيانات الشخصية، ولم يكن هذا الوصول خاضعاً لشروط إجرائية مثل شرط الحصول على موافقة سلطة إدارية أو محكمة قبل الوصول إليها. وأخيراً، لم يحدد الأمر التوجيهي ضمانات واضحة لحماية البيانات المحتفظ بها. لذلك، فشلت في ضمان الحماية الفعالة للبيانات ضد مخاطر الاستخدام التعسفي وضد أي وصول غير قانوني إلى البيانات واستخدامها.[642]

من حيث المبدأ، يجب على محكمة العدل التابعة للاتحاد الأوروبي الإجابة على الأسئلة المحالة لها ولا يمكنها رفض إصدار حكمها الأولي على أساس أن هذا الرد لن يكون ذا صلة ومناسباً من حيث الوقت فيما يتعلق بالقضية الأصلية. ومع ذلك، يمكنها أن ترفض الرد إذا كان السؤال لا يندرج ضمن نطاق اختصاصها.[643] وتصدر محكمة العدل التابعة للاتحاد الأوروبي قراراً فقط بشأن العناصر المكونة للطلب المَحال لها لإصدار حكم أولي، بينما تحتفظ المحكمة الوطنية باختصاصها في الفصل في القضية الأصلية.[644]

**بموجب قانون مجلس أوروبا**، يجب على الأطراف المتعاقدة وضع سبل انتصاف قضائية وغير قضائية متناسبة مع الانتهاكات التي طالت مقتضيات الاتفاقية 108 المحدثة.[645] بالإضافة إلى ذلك، يمكن رفع الادعاءات المتعلقة بانتهاكات حقوق حماية البيانات التي تمس المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان ضد طرف متعاقد في الاتفاقية أمام المحكمة الأوروبية لحقوق الإنسان عند استنفاد جميع سبل

[641] محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-293/12 و C-594/12، قضية «شركة 'ديجيتال رايتس آيرلاند' المحدودة ضد وزير الاتصالات والموارد البحرية والطبيعية وآخرين» و«حكومة كيرنتن وآخرين» [الغرفة الكبرى]، 8 أبريل 2014.

[642] محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-293/12 وC-594/12، قضية «شركة 'ديجيتال رايتس آيرلاند' المحدودة ضد وزير الاتصالات والموارد البحرية والطبيعية وآخرين» و«حكومة كيرنتن وآخرين» [الغرفة الكبرى]، 8 أبريل2014، الفقرة 69.

[643] محكمة العدل التابعة للاتحاد الأوروبي، C-244/80، قضية «باسكوال فوغليا ضد ماريبلا نوفيلو» (رقم 2)، 16 ديسمبر 1981؛ محكمة العدل التابعة للاتحاد الأوروبي، C-467/04، الإجراءات الجنائية ضد «غاسباريني وآخرون»، 28 سبتمبر 2006.

[644] محكمة العدل التابعة للاتحاد الأوروبي، قضية C-438/05 «الاتحاد الدولي لعمال النقل واتحاد البحارة الفنلندي ضد شركة 'فايكينغ لاين'» [الغرفة الكبرى]، 11 ديسمبر 2007، الفقرة 85.

[645] الاتفاقية 108 المحدثة، المادة 12.

الانتصاف المحلية المتاحة. ويجب أن تستوفي أي دفوعات خاصة بانتهاك المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان أمام المحكمة الأوروبية لحقوق الإنسان معايير المقبولية الأخرى (المادتان 34 و35 من الاتفاقية الأوروبية لحقوق الإنسان).[646]

على الرغم من أن الطلبات المقدمة إلى المحكمة الأوروبية لحقوق الإنسان لا يمكن توجيهها إلا ضد الأطراف المتعاقدة، يمكن أن تتطرق بشكل غير مباشر إلى أفعال أو تقصير من الأطراف الخاصة، طالما أن الطرف المتعاقد لم يفِ بالتزاماته الإيجابية بموجب الاتفاقية الأوروبية لحقوق الإنسان ولم يوفر حماية كافية من انتهاك حقوق حماية البيانات في قانونه الوطني.

مثال: في قضية «ك. ي. ضد فنلندا»،[647] اشتكى المدعي- وهو قاصر - من نشر إعلان له ذي طبيعة جنسية على أحد مواقع المواعدة عبر الإنترنت. لم يكشف مزود الخدمة عن هوية الشخص الذي نشر المعلومات بسبب التزامات السرية بموجب القانون الفنلندي. وقد ادعى المدعي أن القانون الفنلندي لا يوفر حماية كافية ضد مثل هذه الأفعال التي يقوم بها شخص عادي يضع بيانات تجريمية خاصة بالمدعي على الإنترنت. ورأت المحكمة الأوروبية لحقوق الإنسان أن الدول لا تُجبر فقط على الامتناع عن التدخل التعسفي في الحياة الخاصة للأفراد، بل قد تخضع أيضا لالتزامات إيجابية تتضمن «اعتماد تدابير تهدف إلى ضمان احترام الحياة الخاصة حتى في مجال العلاقات بين الأفراد فيما بينهم». وفي حالة المدعي، تتطلب حمايته العملية والفعالة اتخاذ خطوات فعالة لتحديد الجاني ومقاضاته. ومع ذلك، لم توفر الدولة مثل هذه الحماية، وخلصت المحكمة إلى أن المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان قد انتهكت.

مثال: في قضية « كوبكه ضد ألمانيا»،[648] تم الاشتباه في قيام المدعية بالسرقة في مكان عملها وتعرضت للمراقبة السرية بالفيديو. وقد خلصت المحكمة الأوروبية لحقوق الإنسان إلى أنه «لا يوجد ما يشير إلى أن السلطات المحلية فشلت في تحقيق توازن عادل، ضمن هامش تقديرها، بين حق المدعية في احترام حياتها الخاصة بموجب المادة 8 ومصلحة صاحب العمل في حماية حقوق الملكية والمصلحة العامة في الإدارة السليمة للعدالة». ولذلك قضت بعدم قبول الطلب.

إذا وجدت المحكمة الأوروبية لحقوق الإنسان أن طرفاً متعاقداً قد انتهك أياً من الحقوق المحمية بموجب الاتفاقية الأوروبية لحقوق الإنسان، فإن هذا الطرف المتعاقد يكون ملزماً بتنفيذ حكم المحكمة الأوروبية لحقوق الإنسان (المادة 46 من الاتفاقية الأوروبية لحقوق الإنسان). أمّا إجراءات التنفيذ فيتعين عليها أولاً أن تضع حداً للانتهاك ثم أن تتدارك، قدر الإمكان، انعكاساته السلبية على المدعي. وقد يتطلب تنفيذ الأحكام أيضاً اتخاذ تدابير عامة لمنع أي انتهاكات مشابهة لتلك التي وجدتها المحكمة، سواء من خلال إدخال تغييرات على التشريع أو من خلال السوابق القضائية أو غيرها من التدابير.

عندما يتبين للمحكمة الأوروبية لحقوق الإنسان وجود انتهاك للاتفاقية الأوروبية لحقوق الإنسان، فإن المادة 41 من الاتفاقية الأوروبية لحقوق الإنسان تجيز لها منح «ترضية عادلة» للمدعي على نفقة الطرف المتعاقد.

**الحق في تفويض هيئة أو منظمة أو جمعية غير ربحية**

تمكّن اللائحة العامة لحماية البيانات الأفراد من التقدم بشكاية لدى هيئة إشرافية أو رفع دعوى قضائية أمام محكمة لتفويض هيئة أو منظمة أو جمعية غير ربحية لتمثيلهم.[649] ويجب أن يكون لهذه الجهات غير الربحية أهداف قانونية في مجال المصلحة العامة وأن تكون نشطة في مجال حماية البيانات. كما يجوز لهما التقدم بشكاية أو ممارسة الحق في الحصول على تعويض قضائي نيابة عن صاحب (أصحاب) البيانات. وتمنح اللائحة الدول الأعضاء الخيار في أن تقرر - وفقاً للقانون الوطني - ما إذا كان بإمكان هيئة ما تقديم شكاية نيابة عن أصحاب البيانات دون تفويض منهم.

[646] الاتفاقية الأوروبية لحقوق الإنسان، المواد من 34-37.
[647] المحكمة الأوروبية لحقوق الإنسان، قضية «ك. ي. ضد فنلندا»، رقم 2872/02، 2 ديسمبر 2008.
[648] المحكمة الأوروبية لحقوق الإنسان، قضية « كوبكه ضد ألمانيا» (القرار)، رقم 420/07، 5 أكتوبر 2010.
[649] اللائحة العامة لحماية البيانات، المادة 80.

يمكّن الحق في التمثيل الأفراد من الاستفادة من الخبرة والقدرة التنظيمية والمالية لهذه الجهات غير الربحية، مما يسهل على الأفراد بشكل كبير ممارسة حقوقهم. وتسمح اللائحة العامة لحماية البيانات لهذه الجهات بتقديم دعاوى جماعية نيابة عن عدد من أصحاب البيانات. هذا الأمر يفيد أيضا أداء نجاعة النظام القضائي، حيث يتم تجميع الدعاوى المتشابهة وفحصها معاً.

## 3.2.6. المسؤولية والحق في التعويض

يجب أن يمكّن الحق في الانتصاف الفعال الأفراد من المطالبة بالتعويض عن أي ضرر لحق بهم نتيجة معالجة بياناتهم الشخصية بطريقة تنتهك التشريع المعمول به. وتم الإقرار صراحةً بمسؤولية المراقبين والمعالجين عن المعالجة غير المشروعة في اللائحة العامة لحماية البيانات،[650] وتمنح اللائحة الأفراد الحق في الحصول على تعويض من المراقب أو المعالج عن الأضرار المادية وغير المادية، في حين تنص حيثياتها على أنه «يجب تفسير مفهوم الضرر على نطاق واسع في ضوء السوابق القضائية لمحكمة العدل بطريقة تعكس بشكل تام أهداف هذه اللائحة».[651] كما تقع المسؤولية على عاتق المراقبين ويمكن أن يخضعوا لمطالبات التعويض إذا لم يفوا بالتزاماتهم بموجب اللائحة. ويتحمل معالجو البيانات الشخصية المسؤولية عن الضرر الناجم عن المعالجة فقط في حال عدم امتثالهم لالتزامات اللوائح الموجهة على وجه التحديد إلى المعالجين، أو عدم التزامهم بالتعليمات القانونية للمراقب أو مخالفتهم لها. وفي حال دفع مراقب أو معالج تعويضا كاملاً، فإن اللائحة العامة لحماية البيانات تنص على أنه بإمكانه المطالبة باستعادة جزء من التعويض يعادل درجة المسؤولية عن الضرر من المراقبين أو المعالجين الأخرين المشاركين في نفس المعالجة.[652] وفي الوقت نفسه، فإن الاستثناءات من المسؤولية صارمة للغاية ورهينة بإثبات أن المراقب أو المعالج ليس مسؤولاً بأي شكل من الأشكال عن الحدث الذي أدى إلى حدوث الضرر.

يجب أن يكون التعويض 'كاملاً وفعلياً' فيما يتعلق بالضرر الناتج. عندما يكون الضرر ناتجاً عن معالجة أجراها العديد من المراقبين أو المعالجين، يجب أن يتحمل كل مراقب أو معالج المسؤولية عن الضرر بالكامل. وتسعى هذه القاعدة إلى ضمان التعويض الفعلي لأصحاب البيانات ونهج منسق للامتثال من قبل المراقبين والمعالجين المشاركين في أنشطة المعالجة.

مثال: إن أصحاب البيانات غير مطالبين برفع دعوى والمطالبة بالتعويض من جميع الجهات المسؤولة عن الضرر، لأن هذا قد يستلزم إجراءات مكلفة وطويلة. ويكفي أن تُرفَع دعوى ضد أحد المراقبين المشتركين، والذي يمكن بعد ذلك تحميله المسؤولة عن الضرر الكامل. في مثل هذه الحالات، يحق للمراقب أو المعالج الذي يدفع التعويض عن الضرر استرداد المبلغ المدفوع لاحقاً من الجهات الأخرى المشاركة في المعالجة والمسؤولة عن الانتهاك، وذلك عن مسؤوليتهم الجزئية عن الضرر. وتتم هذه الإجراءات بين مختلف المعالجين والمراقبين المشتركين بعد أن يتلقى صاحب البيانات التعويض، ولا يكون صاحب البيانات جزءاً منها.

وفي الإطار القانوني لمجلس أوروبا، تتطلب المادة 12 من الاتفاقية 108 المحدثة من الأطراف المتعاقدة وضع سبل انتصاف مناسبة لانتهاكات القانون الوطني المنفّذ لمتطلبات الاتفاقية. ويشير التقرير التفسيري للاتفاقية 108 المحدثة إلى أن سبل الانتصاف يجب أن تشمل إمكانية الطعن القضائي في قرار أو ممارسة ما، بينما يجب أيضاً توفير سبل الانتصاف غير القضائية.[653] وتُترك مسألة تقدير الطرق والقواعد المختلفة المتعلقة بالوصول إلى سبل الانتصاف هذه، إلى جانب الإجراءات الواجب اتباعها، بيد كل طرف متعاقد. كما يجب على الأطراف المتعاقدة والمحاكم الوطنية أن تنظر أيضاً في مقتضيات التعويض المالي للأضرار المادية وغير المادية الناجمة عن المعالجة، فضلاً عن إمكانية تمكين الإجراءات الجماعية.[654]

[650] نفس المرجع السابق، المادة 82.
[651] نفس المرجع السابق، الحيثية 146.
[652] نفس المرجع السابق، المادة 82 (2) و(5).
[653] التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 100.
[654] نفس المرجع السابق.

## 4.2.6. العقوبات

بموجب **قانون مجلس أوروبا**، تنص المادة 12 من الاتفاقية 108 المحدثة على وجوب تحديد كل طرف متعاقد للعقوبات وسبل الانتصاف المناسبة فيما يخص انتهاكات مقتضيات القانون المحلي التي تفعل المبادئ الأساسية لحماية البيانات المنصوص عليها في الاتفاقية 108. ولا تنص الاتفاقية على مجموعة معينة من العقوبات أو تفرضها، وإنما تشير بوضوح إلى أن كل طرف متعاقد لديه السلطة التقديرية لتحديد طبيعة العقوبات القضائية أو غير القضائية، والتي قد تكون جنائية أو إدارية أو مدنية. وينص التقرير التفسيري للاتفاقية 108 المحدثة على أن العقوبات يجب أن تكون فعالة ومتناسبة ورادعة.[655] ويجب على الأطراف المتعاقدة احترام هذا المبدأ عند تحديد طبيعة وشدة العقوبات المتاحة في نظامها القانوني المحلي.

وبموجب **قانون الاتحاد الأوروبي**، تُمكّن المادة 83 من اللائحة العامة لحماية البيانات الهيئات الإشرافية في الدول الأعضاء من فرض غرامات إدارية على انتهاكات اللائحة. كما تنص المادة 83 أيضاً على مستوى الغرامات والظروف التي تأخذها السلطات الوطنية بعين الاعتبار عند اتخاذ قرار بشأن فرض غرامة معينة، فضلاً عن الحد الأقصى الإجمالي لتلك الغرامة. وبذلك، يكون نظام العقوبات موحداً في جميع أنحاء الاتحاد الأوروبي.

تتبع اللائحة العامة لحماية البيانات نهجاً متدرجاً فيما يخص الغرامات. إذ تتمتع الهيئات الإشرافية بصلاحية فرض غرامات إدارية على انتهاكات اللائحة تصل إلى 20 مليون يورو، أو، في حالة المؤسسات، 4% من إجمالي مردودها السنوي في جميع أنحاء العالم - حيث تُطبّق أعلاهما. وتشمل الانتهاكات التي يمكن أن تؤدي إلى هذا المستوى من الغرامات انتهاكات المبادئ الأساسية للمعالجة وشروط الموافقة، وانتهاكات حقوق أصحاب البيانات ومقتضيات اللوائح التي تحكم نقل البيانات الشخصية إلى المتلقين في بلدان ثالثة. أما بالنسبة للانتهاكات الأخرى، فقد تفرض الهيئات الإشرافية غرامات تصل إلى 10 ملايين يورو أو، في حالة المؤسسات، 2% من إجمالي مردوداتها السنوية في جميع أنحاء العالم - حيث تطبّق أعلاهما.

عند تحديد نوع ومستوى الغرامة التي سيتم فرضها، يجب أن تأخذ الهيئات الإشرافية سلسلة من العوامل بعين الاعتبار،[656] على سبيل المثال، يجب أن تراعي على النحو الواجب طبيعة الانتهاك وخطورته ومدته، وفئات البيانات الشخصية المتأثرة، وما إذا كان الانتهاك مقصوداً أم ناتجاً عن إهمال. وفي حال اتخذ المراقب أو المعالج إجراءات للتخفيف من الضرر الذي لحق بأصحاب البيانات، فإنه يجب أيضاً أخذ ذلك بعين الاعتبار. وبالمثل، فإن درجة التعاون مع الهيئة الإشرافية بعد حدوث الانتهاك، والطريقة التي علمت بها الهيئة الإشرافية بالانتهاك (على سبيل المثال، ما إذا كان قد تم الإبلاغ عنه من قبل الجهة المسؤولة عن المعالجة، أو من قبل صاحب البيانات الذي تعرضت حقوقه للانتهاك) تُعد عوامل مهمة أخرى توجه الهيئات الإشرافية في اتخاذ قرارها.[657]

وتتوفر الهيئات الإشرافية، بالإضافة إلى القدرة على فرض الغرامات الإدارية، على مجموعة واسعة من السلطات التصحيحية الأخرى تحت تصرفها. وقد تم تحديد ما يسمى بالسلطات "التصحيحية" للهيئات الإشرافية في المادة 58 من اللائحة العامة لحماية البيانات، وهي تتراوح بين إصدار الأوامر والتحذيرات والتوبيخات في حق المراقبين والمعالجين، وفرض حظر مؤقت أو حتى دائم على أنشطة المعالجة.

وفيما يتعلق بالعقوبات المتعلقة بانتهاكات قانون الاتحاد الأوروبي من قبل مؤسسات أو هيئات الاتحاد، نظراً لنطاق الاختصاص الخاص بلائحة حماية البيانات الخاصة بمؤسسات الاتحاد الأوروبي، يمكن توخي العقوبات في شكل إجراء تأديبي. فوفقاً للمادة 49 من تلك اللائحة، «أي إخفاق في الامتثال للالتزامات بموجب هذه اللائحة، سواء كان عن قصد أو نتيجة إهمال، يجعل أي موظف أو أي مُستخدَم آخر في الجماعات الأوروبية عرضة لإجراءات تأديبية [...]».

[655] نفس المرجع السابق.

[656] اللائحة العامة لحماية البيانات، المادة 83 (2).

[657] فريق عمل المادة 29 (2017)، المبادئ التوجيهية المتعلقة بتطبيق وتحديد الغرامات الإدارية لأغراض اللائحة 2016/679، WP 253، 3 أكتوبر 2017.

# 7

# عمليـات نقـل البيانـات الشخصيـة وتدفقاتهـا على المستـوى الدولـي

| الاتحاد الأوروبي | المسائل المتناولة | مجلس أوروبا |
|---|---|---|
| **عمليات نقل البيانات الشخصية** | | |
| اللائحة العامة لحماية البيانات، المادة 44 | مفهوم | الاتفاقية 108 المحدثة، المادة 14 (1) و(2) |
| **التدفق الحر للبيانات الشخصية** | | |
| اللائحة العامة لحماية البيانات، المادة 1 (3) والحيثية 170 | بين الدول الأعضاء في الاتحاد الأوروبي | |
| | بين الأطراف المتعاقدة في الاتفاقية 108 | الاتفاقية 108 المحدثة، المادة 14 (1) |
| **عمليات نقل البيانات الشخصية إلى دول ثالثة أو منظمات دولية** | | |
| اللائحة العامة لحماية البيانات، المادة 45<br>القضية C-362/14، «ماكسيميليان شريمز ضد مفوض حماية البيانات» [الغرفة الكبرى]، 2015 | قرار المفوضية حول مدى كفاية الضمانات المرتبطة بحماية البيانات / البلدان الثالثة أو المنظمات الدولية التي تتوفر على مستويات مناسبة من الحماية | الاتفاقية 108 المحدثة، المادة 14 (2) |

| | | |
|---|---|---|
| اللائحة العامة لحماية البيانات، المادة 46 (1) و46 (2) | الضمانات المناسبة، بما في ذلك الحقوق القابلة للتنفيذ وسبل الانتصاف القانونية لأصحاب البيانات، المتاحة من خلال البنود التعاقدية المعيارية وقواعد الشركات الملزمة ومدونات قواعد السلوك وآليات شهادات التصديق | الاتفاقية 108 المحدثة، المادة 14 (2) و(3) و(5) و(6) |
| اللائحة العامة لحماية البيانات، المادة 46 (3) | رهناً بترخيص من الهيئة الإشرافية المختصة: البنود التعاقدية والمقتضيات المدرجة في الترتيبات الإدارية بين السلطات العامة | |
| اللائحة العامة لحماية البيانات، المادة 46 (5) | التراخيص الحالية على أساس الأمر التوجيهي رقم 46/95 | |
| اللائحة العامة لحماية البيانات، المادة 47 | قواعد الشركات المُلزِمة | |
| اللائحة العامة لحماية البيانات، المادة 49 | استثناءات الحالات الخاصة | الاتفاقية 108 المحدثة، المادة 14 (4) |
| أمثلة:<br>اتفاق سجلات أسماء الركاب (PNR) بين الاتحاد الأوروبي والولايات المتحدة<br>اتفاق «سويفت» بين الاتحاد الأوروبي والولايات المتحدة | الاتفاقات الدولية | الاتفاقية 108 المحدثة، المادة 14 (3) (أ) |

بموجب قانون الاتحاد الأوروبي، تنص اللائحة العامة لحماية البيانات على التدفق الحر للبيانات داخل الاتحاد الأوروبي. إلا أنها تحتوي على متطلبات محددة تتعلق بنقل البيانات الشخصية إلى دول ثالثة خارج الاتحاد الأوروبي وإلى منظمات دولية. وتقر اللائحة بأهمية عمليات النقل هذه، لا سيما في ضوء التجارة والتعاون الدوليين، ولكنها تعترف أيضاً بالمخاطر المتزايدة المحدقة بالبيانات الشخصية. لذلك، تهدف اللائحة إلى تقديم نفس مستوى الحماية للبيانات الشخصية التي يتم نقلها إلى دول ثالثة مقارنة بتلك التي تتمتع بها داخل الاتحاد الأوروبي.[658] هذا ويقر قانون مجلس أوروبا أيضاً بأهمية تنفيذ قواعد بالنسبة لتدفقات البيانات عبر الحدود، بناءً على التدفق الحر بين الأطراف والمتطلبات المحددة لعمليات النقل إلى الجهات غير الأطراف.

## 1.7. طبيعة عمليات نقل البيانات الشخصية

### النقاط الرئيسية

- يتضمن قانونا الاتحاد الأوروبي ومجلس أوروبا قواعد بشأن نقل البيانات الشخصية إلى المتلقين في دول ثالثة أو إلى المنظمات الدولية.
- يسمح ضمان حماية حقوق صاحب البيانات عند نقل بياناته خارج الاتحاد الأوروبي بأن تبقى الحماية التي يوفرها قانون الاتحاد الأوروبي سارية على البيانات الشخصية التي تنشأ في الاتحاد الأوروبي.

بموجب **قانون مجلس أوروبا**، تُوصف تدفقات البيانات عبر الحدود على أنها عمليات نقل بيانات شخصية إلى متلقين يخضعون لولاية قضائية أجنبية،[659] ولا يُسمح بتدفق البيانات عبر الحدود إلى متلق لا يخضع لولاية طرف متعاقد إلا إذا كان هناك مستوىً مناسب من الحماية.[660]

ينظم **قانون الاتحاد الأوروبي** عمليات نقل «البيانات الشخصية التي تخضع للمعالجة أو المتوخى معالجتها بعد نقلها إلى بلد ثالث أو إلى منظمة دولية [...]»،[661] ولا يُسمح بتدفقات البيانات هذه إلا إذا كانت تمتثل للقواعد المنصوص عليها في الفصل الخامس من اللائحة العامة لحماية البيانات.

يُسمح بتدفقات البيانات الشخصية عبر الحدود إلى متلق يخضع للولاية القضائية لطرف متعاقد أو دولة عضو بموجب قانون مجلس أوروبا أو قانون الاتحاد الأوروبي، على التوالي. ويسمح كلا النظامين القانونيين أيضاً بنقل البيانات إلى دولة ليست طرفاً متعاقداً أو دولة عضو، شريطة استيفاء شروط معينة.

[658] اللائحة العامة لحماية البيانات، الحيثيتان 101 و116.
[659] التقرير التفسيري للاتفاقية 108 المحدثة، الفقرة 102.
[660] الاتفاقية 108 المحدثة، المادة 14 (2).
[661] اللائحة العامة لحماية البيانات، المادة 44.

## 2.7. حرية حركة/تدفق البيانات الشخصية بين الدول الأعضاء أو الأطراف المتعاقدة

### النقاط الرئيسية

- يجب أن يكون تدفق البيانات الشخصية في جميع أنحاء الاتحاد الأوروبي، وكذلك عمليات نقل البيانات الشخصية بين الأطراف المتعاقدة في الاتفاقية 108 المحدثة، خالياً من القيود. ولكن بما أنه ليست كل الأطراف المتعاقدة في الاتفاقية 108 المحدثة دولاً أعضاء في الاتحاد الأوروبي، فإن عمليات النقل من دولة عضو في الاتحاد الأوروبي إلى دولة ثالثة، وإن كانت طرفاً متعاقداً في الاتفاقية 108، غير ممكنة ما لم تستوف الشروط المنصوص عليها في اللائحة العامة لحماية البيانات.

بموجب **قانون مجلس أوروبا**، يجب أن يكون هناك تدفق حر للبيانات الشخصية بين الأطراف المتعاقدة في الاتفاقية 108 المحدثة. غير أنه قد يُحظر النقل إذا كان هناك «خطر حقيقي وجسيم بأن يؤدي النقل إلى طرف آخر إلى التحايل على مقتضيات الاتفاقية» أو إذا كان الطرف مُلزَماً بالقيام بذلك من خلال «قواعد حماية مُنسَّقة تتشاركها الدول المنتمية إلى منظمة دولية إقليمية».[662]

وبموجب **قانون الاتحاد الأوروبي**، تُمنع القيود أو تدابير الحظر على حرية حركة البيانات الشخصية بين الدول الأعضاء في الاتحاد الأوروبي لأسباب تتعلق بحماية الأشخاص الذاتيين فيما يتعلق بمعالجة البيانات الشخصية.[663] وقد تم توسيع منطقة التدفق الحر للبيانات من خلال اتفاق المنطقة الاقتصادية الأوروبية (EEA)،[664] والذي أدخل أيسلندا وليشتنشتاين والنرويج إلى السوق الداخلية.

مثال: إذا قامت مؤسسة فرعية تابعة لمجموعة دولية من الشركات، لها مقر في العديد من الدول الأعضاء من بينها سلوفينيا وفرنسا، بإرسال بيانات شخصية من سلوفينيا إلى فرنسا، يجب ألا يكون تدفق البيانات هذا مقيداً أو محظوراً بموجب القانون الوطني السلوفيني لأسباب مرتبطة بحماية البيانات الشخصية.

غير أنه، إذا أرادت المؤسسة الفرعية السلوفينية ذاتها نقل نفس البيانات الشخصية إلى الشركة الأم في ماليزيا، فيجب على مُصدِّر البيانات السلوفيني مراعاة القواعد الواردة في الفصل الخامس من اللائحة العامة لحماية البيانات. وتهدف هذه المقتضيات إلى حماية البيانات الشخصية لأصحاب البيانات الخاضعين لولاية الاتحاد الأوروبي.

إن تدفقات البيانات الشخصية إلى الدول الأعضاء في المنطقة الاقتصادية الأوروبية للأغراض المتعلقة بمنع الجرائم الجنائية أو التحقيق فيها أو الكشف عنها أو متابعة مرتكبيها أو تنفيذ العقوبات الجنائية تخضع للأمر التوجيهي رقم 680/2016، بموجب قانون الاتحاد الأوروبي.[665] ويضمن هذا أيضاً عدم تقييد أو حظر تبادل البيانات الشخصية من قبل السلطات المختصة داخل الاتحاد لأسباب تتعلق بحماية البيانات. وبموجب قانون مجلس أوروبا، تندرج معالجة جميع البيانات الشخصية (بما يشمل ذلك تدفقها عبر الحدود مع أطراف أخرى في الاتفاقية 108)، دون أي استثناءات بناءً على الأغراض أو مجالات العمل، في نطاق الاتفاقية 108، وذلك على الرغم من أنه يجوز وضع إعفاءات من قبل الأطراف المتعاقدة. إن جميع أعضاء المنطقة الاقتصادية الأوروبية هم أيضاً أطراف في الاتفاقية 108.

---

[662] الاتفاقية 108 المحدثة، المادة 14 (1).

[663] اللائحة العامة لحماية البيانات، المادة 1 (3).

[664] قرار مجلس أوروبا والمفوضية الأوروبية المؤرخ في 13 ديسمبر 1993 بشأن إبرام الاتفاق بشأن المنطقة الاقتصادية الأوروبية بين الجماعات الأوروبية والدول الأعضاء فيها وجمهورية النمسا وجمهورية فنلندا وجمهورية أيسلندا وإمارة ليختنشتاين ومملكة النرويج ومملكة السويد والاتحاد السويسري، الجريدة الرسمية L 1 1994 OJ.

[665] الأمر التوجيهي (الاتحاد الأوروبي) 2016/680 الصادر عن البرلمان الأوروبي والمجلس بتاريخ 27 أبريل 2016 بشأن حماية الأشخاص الذاتيين فيما يتعلق بمعالجة البيانات الشخصية من قبل السلطات المختصة لأغراض منع الجرائم الجنائية أو التحقيق فيها أو الكشف عنها أو متابعة مرتكبيها أو تنفيذ العقوبات الجنائية، وبشأن حرية نقل هذه البيانات، والمُلغي للقرار الإطاري الصادر عن مجلس أوروبا JHA/2008/977، الجريدة الرسمية L119 2016 OJ.

## 3.7. عمليات نقل البيانات الشخصية إلى دول ثالثة/من غير الأطراف أو إلى منظمات دولية

### النقاط الرئيسية

- يسمح كل من **مجلس أوروبا والاتحاد الأوروبي** بنقل البيانات الشخصية إلى دول ثالثة أو منظمات دولية، شريطة استيفاء شروط معينة لحماية البيانات الشخصية.

- **بموجب قانون مجلس أوروبا**، يمكن تحقيق مستوىً مناسب من الحماية بموجب قانون الدولة أو المنظمة الدولية أو من خلال وضع المعايير المناسبة.
- **بموجب قانون الاتحاد الأوروبي**، يمكن نقل البيانات إذا كان البلد الثالث يضمن مستوىً كافٍ من الحماية أو إذا كان مراقب البيانات أو معالجها يوفر الضمانات المناسبة، بما في ذلك حقوق أصحاب البيانات القابلة للتنفيذ وسبل الانتصاف القانونية، من خلال وسائل مثل بنود حماية البيانات المعيارية أو قواعد الشركات المُلزِمة.

- ينص كل من **قانون مجلس أوروبا وقانون الاتحاد الأوروبي** على بنود الاستثناء التي تسمح بنقل البيانات الشخصية في ظروف محددة حتى في حال عدم وجود مستوىً كافٍ من الحماية أو ضمانات مناسبة.

وعلى الرغم من أن كلاً من قانون مجلس أوروبا وقانون الاتحاد الأوروبي يسمح بتدفق البيانات إلى دول ثالثة أو إلى منظمات دولية، فإنهما يضعان شروطاً مختلفة، وتأخذ كل مجموعة من الشروط بعين الاعتبار الهياكل والأغراض المختلفة للمنظمة المعنية.

بموجب **قانون الاتحاد الأوروبي**، توجد مبدئياً طريقتان للسماح بنقل البيانات الشخصية إلى دول ثالثة أو إلى منظمات دولية. إذ يمكن أن يتم نقل البيانات الشخصية على أساس: قرار حول مدى كفاية الضمانات المرتبطة بحماية البيانات صادر عن المفوضية الأوروبية (المشار إليه اختصاراً بـ«قرار كفاية»)؛[666] أو، في حالة عدم وجود هذا القرار، عندما يوفر المراقب أو المعالج الضمانات المناسبة لصاحب البيانات، بما فيها الحقوق القابلة للتنفيذ وسبل الانتصاف القانونية.[667] أما في حال عدم وجود قرار الكفاية أو ضمانات مناسبة، فهناك عدد من الاستثناءات.

ولكن، بموجب **قانون مجلس أوروبا**، لا يُسمح بالنقل الحر للبيانات إلى غير الأطراف في الاتفاقية إلا على أساس:
- قانون تلك الدولة أو المنظمة الدولية، بما في ذلك المعاهدات أو الاتفاقات الدولية السارية والتي تضمن وجود الضمانات المناسبة؛
- الضمانات المعيارية المخصَّصة أو المعتمدة التي توفرها الصكوك المُلزِمة قانوناً والقابلة للتنفيذ التي تم تبنيها وتنفيذها من قبل الأشخاص المشاركين في عملية نقل البيانات ومعالجتها لاحقا.[668]

وعلى غرار قانون الاتحاد الأوروبي، في غياب مستوىً مناسب من حماية البيانات، هناك عدد من الاستثناءات.

### 1.3.7. عمليات نقل البيانات الشخصية على أساس قرار المفوضية حول مدى كفاية الضمانات المرتبطة بحماية البيانات

بموجب **قانون الاتحاد الأوروبي**، فإن التدفق الحر للبيانات الشخصية إلى الدول الثالثة بمستوىً كافٍ من حماية البيانات منصوص عليه في المادة 45 من اللائحة العامة لحماية البيانات. وقد أوضحت محكمة العدل التابعة لاتحاد الأوروبي أن مصطلح «المستوى الكافي من

[666] اللائحة العامة لحماية البيانات، المادة 45.
[667] نفس المرجع السابق، المادة 46
[668] الاتفاقية 108 المحدّثة، المادة 14 (3) (أ) و(ب).
[669] محكمة العدل التابعة للاتحاد الأوروبي، القضية C-362/14، «ماكسيميليان شريمز ضد مفوض حماية البيانات» [الغرفة الكبرى]، 6 أكتوبر 2015، الفقرة 96.

الحماية» يتطلب من الدولة الثالثة ضمان مستوىً من حماية الحقوق والحريات الأساسية التي «تعادل جوهرياً»[669] الضمانات التي يكفلها القانون في الاتحاد الأوروبي. وفي نفس الوقت، قد تختلف الوسائل التي يلجأ إليها البلد الثالث من أجل ضمان هذا المستوى من الحماية عن تلك المستخدمة داخل الاتحاد الأوروبي، إذ لا يتطلب معيار كفاية مستوى الحماية أن تكون قواعد الاتحاد الأوروبي مستنسخة حرفياً.[670]

تقيّم المفوضية الأوروبية مستوى حماية البيانات في الدول الأجنبية من خلال النظر في قانونها الوطني والتزاماتها الدولية السارية. كما يجب أن تؤخذ مشاركة الدولة في الأنظمة متعددة الأطراف أو الإقليمية بعين الاعتبار، لا سيما فيما يتعلق بحماية البيانات الشخصية. وفي حال اعتبرت المفوضية الأوروبية أن الدولة الثالثة أو المنظمة الدولية تضمن مستوىً مناسباً من الحماية، فيمكنها إصدار قرار حول مدى كفاية الضمانات المرتبطة بحماية البيانات، والذي يكون له أثر مُلزِم.[671] ومع ذلك، فقد ذكرت محكمة العدل التابعة للاتحاد الأوروبي أن الهيئات الإشرافية الوطنية تحتفظ بصلاحية النظر في ادعاء شخص فيما يتعلق بحماية بياناته الشخصية التي تم نقلها إلى دولة ثالثة تعتبرها المفوضية على أنها تضمن مستوىً كافياً من الحماية، عندما يجادل هذا الشخص بأن القوانين والممارسات السارية في البلد الثالث لا تضمن مستوىً كافياً من الحماية.[672]

يمكن للمفوضية الأوروبية أيضاً تقييم مدى كفاية مستوى الحماية التي توفرها منطقة معينة داخل بلد ثالث، أو أن تقتصر على قطاعات محددة، كما كان الحال بالنسبة للتشريعات التجارية الخاصة في كندا على سبيل المثال.[673] وهناك أيضاً قرارات بخصوص كفاية مستوى الحماية تتعلق بعمليات النقل بناءً على الاتفاقات المبرمة بين الاتحاد الأوروبي ودول أخرى. وتشير هذه القرارات حصرياً إلى نوع واحد من أنواع نقل البيانات، مثل نقل شركة الطيران لسجلات أسماء الركاب (PNR) إلى سلطات مراقبة الحدود الأجنبية عندما تقوم شركة الطيران برحلة من الاتحاد الأوروبي إلى وجهات خارجية معينة (انظر الجزء 4.3.7).

وتخضع قرارات المفوضية حول مدى كفاية الضمانات المرتبطة بحماية البيانات للمراقبة بشكل مستمر. إذ تراجع المفوضية الأوروبية بانتظام مثل هذه القرارات لتتبع التطورات التي يمكن أن تؤثر على وضعها. وبالتالي، إذا وجدت المفوضية الأوروبية أن الدولة الثالثة أو المنظمة الدولية المعنية لم تعد تستوفي الشروط التي تبرر قرار الكفاية، فيمكنها تعديل هذا القرار أو تعليقه أو إلغائه. كما يجوز للمفوضية أيضاً الدخول في مفاوضات مع الدولة الثالثة أو المنظمة الدولية المعنية لمعالجة المشكلة الكامنة وراء قرارها.

تظل قرارات الكفاية التي اعتمدتها المفوضية الأوروبية على أساس الأمر التوجيهي رقم EC/95/46 سارية المفعول حتى يتم تعديلها أو استبدالها أو إلغاؤها بواسطة قرار من المفوضية يتم اعتماده وفقاً للقواعد الواردة في المادة 45 من اللائحة العامة لحماية البيانات.

حتى الآن، اعترفت المفوضية الأوروبية بكل من أندورا والأرجنتين وكندا (المنظمات التجارية التي تندرج في نطاق «قانون المعلومات الشخصية والوثائق الإلكترونية» (PIPEDA)) وكذا جزر فارو وغيرنزي وجزيرة مان وإسرائيل وجيرزي ونيوزيلندا وسويسرا وأوروغواي على أنها توفر مستوىً كافياً من الحماية. وفيما يتعلق بعمليات نقل البيانات الشخصية إلى الولايات المتحدة، اعتمدت المفوضية الأوروبية قرار كفاية سنة 2000 يسمح بنقل البيانات إلى الشركات التي تقوم بالتصديق الذاتي على حمايتها للبيانات الشخصية المنقولة من الاتحاد الأوروبي والامتثال لما يسمى بـ'مبادئ الملاذ الآمن'.[674] ولكن محكمة العدل التابعة للاتحاد الأوروبي ألغت هذا القرار في عام 2015 وتم اعتماد قرار كفاية جديد في يوليو 2016، والذي سمح للشركات بالانضمام اعتباراً من 1 أغسطس 2016.

---

[670] نفس المرجع السابق، الفقرة 74. انظر أيضاً، المفوضية الأوروبية (2017)، الرسالة الموجهة من المفوضية إلى البرلمان الأوروبي والمجلس «تبادل وحماية البيانات الشخصية في عالم مَعْولم»، الطبعة البهائية 7(2017)COM المؤرخة في 10 يناير 2017 صفحة 6.

[671] للحصول على قائمة محدثة باستمرار للبلدان التي حصلت على استنتاج بكفاية مستوى الحماية، انظر الصفحة الرئيسية للمديرية العامة للعدالة التابعة للمفوضية الأوروبية.

[672] محكمة العدل التابعة للاتحاد الأوروبي، القضية C-362/14، «ماكسيميليان شريمز ضد مفوض حماية البيانات» [الفرقة الكبرى]، 6 أكتوبر 2015، الفقرات 63 و66-65.

[673] المفوضية الأوروبية (2002)، القرار 2/2002/EC الصادر في 20 ديسمبر 2001 وفقاً للأمر التوجيهي EC/95/46 الصادر عن البرلمان الأوروبي والمجلس بشأن الحماية الكافية للبيانات الشخصية التي ينص عليها القانون الكندي لحماية المعلومات الشخصية والوثائق الإلكترونية، الجريدة الرسمية 2 L 2002 0J.

[674] قرار المفوضية الأوروبية EC/2000/520 الصادر في 26 يوليو 2000 وفقاً للأمر التوجيهي EC/95/46 الصادر عن البرلمان الأوروبي والمجلس بشأن مدى كفاية الحماية التي توفرها مبادئ خصوصية «الملاذ الآمن» والأسئلة المتكررة ذات الصلة الصادرة عن وزارة الولايات المتحدة للتجارة، الجريدة الرسمية 215 L 0J. وقد قضت محكمة العدل التابعة للاتحاد الأوروبي ببطلان القرار، الملف C-632/14، «ماكسيميليان شريمز ضد مفوض حماية البيانات» [الفرقة الكبرى].

مثال: في قضية «شريمز»،[675] كان ماكسيميليان شريمز، وهو مواطن نمساوي، مُستخدماً لـ»فيسبوك» لعدة سنوات. وقد تم نقل بعض أو كل البيانات التي قدمها السيد شريمز إلى «فيسبوك» من الشركة الفرعية الأيرلندية التابعة لـ»فيسبوك» إلى خوادم موجودة في الولايات المتحدة، حيث تمت معالجتها هناك. فقدم السيد شريمز شكوى إلى هيئة حماية البيانات الأيرلندية، معتبراً أنه في ضوء الإبلاغ عن المخالفات الأمريكية الذي قام به المبلغ إدوارد سنودن فيما يتعلق بأنشطة المراقبة لأجهزة المخابرات الأمريكية، فإن القانون والممارسات الأمريكية لا توفر حماية كافية للبيانات المنقولة إلى تلك الدولة. ورفضت السلطة الأيرلندية الشكوى، على أساس أن المفوضية الأوروبية قد اعتبرت في قرارها الصادر في 26 يوليو 2000 أنه بموجب مخطط «الملاذ الآمن»، فإن الولايات المتحدة تضمن مستوىً كافياً من الحماية للبيانات الشخصية المنقولة. ثم عُرضت القضية على المحكمة العليا الأيرلندية، والتي أحالتها بدورها إلى محكمة العدل التابعة للاتحاد الأوروبي لإصدار حكم أولي فيها.

قضت محكمة العدل التابعة للاتحاد الأوروبي بأن قرار المفوضية بشأن مدى كفاية الحماية التي يوفرها إطار عمل «الملاذ الآمن» باطل. إذ لاحظت المحكمة أولاً أن القرار قد سمح بتقييد نطاق انطباق مبادئ حماية بيانات الواردة في نص «الملاذ الآمن» على أساس متطلبات الأمن القومي أو المصلحة العامة أو إنفاذ القانون أو على أساس التشريعات الأمريكية المحلية. وبالتالي، مكّن هذا القرار من التدخل في الحقوق الأساسية للأشخاص الذين تم نقل بياناتهم الشخصية أو يمكن نقلها إلى الولايات المتحدة.[676] وأشارت محكمة العدل التابعة للاتحاد الأوروبي كذلك إلى أن القرار لم يتضمن أي نتائج بشأن وجود قواعد في الولايات المتحدة ترمي إلى الحد من مثل هذا التدخل،[677] ولا على وجود أي حماية قانونية فعالة ضد هذا التدخل. وأبرزت محكمة العدل التابعة للاتحاد الأوروبي أن مستوى حماية الحقوق والحريات الأساسية المكفولة داخل الاتحاد الأوروبي يتطلب تشريعاً يتعارض مع المادتين 7 و8 لوضع قواعد واضحة ودقيقة تحدد نطاق وكيفية تطبيق تدبير معين، وتفرض الحد الأدنى من الضمانات والاستثناءات والقيود فيما يتعلق بحماية البيانات الشخصية. [678] ونظراً لأن قرار المفوضية لم ينص على أن الولايات المتحدة تضمن بالفعل مثل هذا المستوى من الحماية بسبب قانونها المحلي أو التزاماتها الدولية، فقد خلصت محكمة العدل التابعة للاتحاد الأوروبي إلى أنها فشلت في استيفاء متطلبات بند النقل ذي الصلة الوارد في الأمر التوجيهي المتعلق بحماية البيانات وبالتالي إلى أن القرار باطل.[679]

وعليه، فإن مستوى الحماية في الولايات المتحدة لم يكن 'معادلاً في الأساس' للحقوق والحريات الأساسية التي يكفلها الاتحاد الأوروبي.[680] كما اعتبرت محكمة العدل التابعة للاتحاد الأوروبي أن مواد مختلفة من ميثاق الاتحاد الأوروبي للحقوق الأساسية قد انتُهكت. أولاً، تم خرق جوهر المادة 7، حيث كان التشريع الأمريكي «يسمح للسلطات العامة بالوصول بشكل عام إلى محتويات الاتصالات الإلكترونية». ثانياً، تم انتهاك جوهر المادة 47 أيضاً، حيث لم يوفر التشريع للأفراد سبل الانتصاف القانونية فيما يتعلق بالوصول إلى البيانات الشخصية أو تصحيحها أو محوها. وأخيراً، بما أن نظام «الملاذ الآمن» قد انتهك المواد المذكورة أعلاه، لم تعد معالجة البيانات الشخصية التي تتم بموجبه مشروعة، مما أدى إلى انتهاك المادة 8.

بعد أن قضت محكمة العدل التابعة للاتحاد الأوروبي ببطلان نظام «الملاذ الآمن»، اتفقت المفوضية الأوروبية والولايات المتحدة على إطار عمل جديد، وهو «درع الخصوصية بين الاتحاد الأوروبي والولايات المتحدة». وفي 12 يوليو 2016، اعتمدت المفوضية قراراً يعلن أن الولايات المتحدة تضمن مستوىً كافياً من الحماية للبيانات الشخصية المنقولة من الاتحاد الأوروبي إلى المنظمات في الولايات المتحدة بموجب «درع الخصوصية».[681]

---

[675] محكمة العدل التابعة للاتحاد الأوروبي، قضية C-632/14، «ماكسيميليان شريمز ضد مفوض حماية البيانات» [الغرفة الكبرى]، 6 أكتوبر 2015.

[676] نفس المرجع السابق، الفقرة 84.

[677] نفس المرجع السابق، الفقرتان 89-88.

[678] نفس المرجع السابق، الفقرتان 92-91.

[679] نفس المرجع السابق، الفقرتان 97-96.

[680] نفس المرجع السابق، الفقرات 74-73 و96.

[681] القرار التنفيذي للمفوضية الأوروبية (الاتحاد الأوروبي) 2016/1250 الصادر في 12 يوليو 2016 وفقاً للأمر التوجيهي رقم EC/95/46 الصادر عن البرلمان الأوروبي والمجلس بشأن كفاية الحماية التي يوفرها «درع الخصوصية بين الاتحاد الأوروبي والولايات المتحدة»، الجريدة الرسمية L 207 OJ. رحب فريق عمل المادة 29 بالتحسينات التي أدخلتها آلية «درع الخصوصية» مقارنة بقرار «الملاذ الآمن» وأثنى على المفوضية وسلطات الولايات المتحدة لأخذها في الاعتبار في النسخة النهائية لوثائق «درع الخصوصية» المخاوف التي أعرب عنها في رأيه WP238 بشأن مشروع قرار كفاية «درع الخصوصية بين الاتحاد الأوروبي والولايات المتحدة». إلا أن فريق العمل سلط الضوء على عدد من الشواغل المتبقية. لمزيد من التفاصيل، انظر فريق عمل المادة 29 المعني بحماية البيانات، الرأي 01/2016 بشأن مشروع قرار كفاية مستوى حماية «درع الخصوصية بين الاتحاد الأوروبي والولايات المتحدة»، المعتمد في 13 أبريل 2016، WP 238/16 EN.

وعلى غرار ترتيب «الملاذ الآمن»، يهدف إطار عمل «درع الخصوصية بين الاتحاد الأوروبي والولايات المتحدة» إلى حماية البيانات الشخصية التي يتم نقلها من الاتحاد الأوروبي إلى الولايات المتحدة لأغراض تجارية.[682] ويمكن للشركات الأمريكية بشكل طوعي أن تصادق ذاتياً على التزامها بقائمة «درع الخصوصية» من خلال الالتزام باستيفاء معايير حماية البيانات الواردة في إطار العمل هذا. كما تراقب السلطات الأمريكية المختصة التزام الشركات المعتمدة بهذه المعايير.

ينص مخطط «درع الخصوصية» على وجه الخصوص على:

- التزامات حماية البيانات المفروضة على الشركات التي تتلقى البيانات الشخصية من الاتحاد الأوروبي؛
- حماية الأفراد وإنصافهم، ولا سيما إنشاء آلية أمانة المظالم، وهي آلية مستقلة عن أجهزة المخابرات الأمريكية وتتعامل مع الشكاوى التي يقدمها الأفراد الذين يعتقدون أن بياناتهم الشخصية قد استُخدِمت بطريقة غير مشروعة من قبل السلطات الأمريكية في مجال الأمن القومي؛
- مراجعة سنوية مُشتركة لتتبع تنفيذ الإطار؛[683] وقد تم إجراء المراجعة الأولى في سبتمبر 2017.[684]

إن لدى حكومة الولايات المتحدة تعهدات وضمانات كتابية مصاحبة لقرار «درع الخصوصية». وهي تنص على القيود والضمانات المتعلقة بوصول حكومة الولايات المتحدة إلى البيانات الشخصية لأغراض إنفاذ القانون والأمن القومي.

## 2.3.7. عمليات نقل البيانات الشخصية الخاضعة للضمانات المناسبة

يقر كل من **قانون الاتحاد الأوروبي وقانون مجلس أوروبا** بالضمانات المناسبة بين المراقب المُصدِّر للبيانات والمتلقي في الدولة الثالثة أو المنظمة الدولية باعتبارها وسيلة ممكنة لضمان مستوىً كافٍ من حماية البيانات بالنسبة للمتلقي.

بموجب **قانون الاتحاد الأوروبي**، يُسمح بنقل البيانات الشخصية إلى دولة ثالثة أو إلى منظمة دولية إذا كان المراقب أو المعالج يوفر الضمانات المناسبة والحقوق القابلة للتنفيذ ، وإذا كانت سبل الانتصاف القانونية الفعالة متاحة لأصحاب البيانات.[685] إن قائمة 'الضمانات المناسبة' المقبولة منصوص عليها حصرياً في قانون حماية البيانات في الاتحاد الأوروبي. ويمكن وضع الضمانات المناسبة من خلال:

- صك مُلزِم قانوناً وقابل للتنفيذ بين السلطات أو الهيئات العامة؛
- قواعد الشركات المُلزِمة؛
- بنود حماية البيانات المعيارية المعتمدة إما من قبل المفوضية الأوروبية أو من قبل هيئة إشرافية؛
- مدونات قواعد السلوك؛
- آليات شهادات التصديق.[686]

تُعتبر البنود التعاقدية المخصصة بين المراقب أو المعالج في الاتحاد الأوروبي ومتلقي البيانات في البلد الثالث وسيلة أخرى لتوفير الضمانات المناسبة. ومع ذلك، تحتاج هذه البنود التعاقدية إلى الحصول على تصريح من الهيئة الإشرافية المختصة أولاً حتى يمكن الاعتماد عليها كأداة لنقل البيانات الشخصية. وبالمثل، يمكن للسلطات العامة الاستفادة من مقتضيات حماية البيانات المدرجة في ترتيباتها الإدارية، شريطة أن تكون الهيئة الإشرافية قد صرحت بذلك.[687]

---

[682] لمزيد من المعلومات، انظر صحيفة وقائع «درع الخصوصية بين الاتحاد الأوروبي والولايات المتحدة».

[683] لمزيد من المعلومات، انظر صفحة الويب الخاصة بالمفوضية الأوروبية عن «درع الخصوصية بين الاتحاد الأوروبي والولايات المتحدة».

[684] المفوضية الأوروبية، تقرير من المفوضية إلى البرلمان الأوروبي والمجلس حول المراجعة السنوية الأولى لسير عمل «درع الخصوصية بين الاتحاد الأوروبي والولايات المتحدة»، النسخة النهائية 18 ،611 (2017) COM أكتوبر 2017. انظر أيضاً، فريق عمل المادة 29، «درع الخصوصية بين الاتحاد الأوروبي والولايات المتحدة» - المراجعة السنوية المشتركة الأولى، المعتمدة في 28 نوفمبر 2017، WP 255/17 EN.

[685] اللائحة العامة لحماية البيانات، المادة 46.

[686] اللائحة العامة لحماية البيانات، المادتان 46 (1) (ج) و(د) و(2) (أ) و(ب) و(هـ) و(و) و47.

[687] نفس المرجع السابق، المادة 46 (3).

بموجب **قانون مجلس أوروبا**، يجوز تدفق البيانات إلى دولة أو منظمة دولية ليست طرفاً في الاتفاقية 108 المحدثة، شريطة أن يتم تأمين مستوىً مناسب من الحماية. ويمكن تحقيق ذلك من خلال:

- قانون الدولة أو المنظمة الدولية؛ أو
- الضمانات المخصصة أو المعيارية المُضمَّنة في وثيقة مُلزِمة قانوناً.[688]

**عمليات نقل البيانات الشخصية الخاضعة لبنود تعاقدية**

يعترف كل من **قانون مجلس أوروبا وقانون الاتحاد الأوروبي** بالبنود التعاقدية بين المراقب المُصدِّر للبيانات والمتلقي في الدولة الثالثة باعتبارها وسيلة ممكنة لضمان مستوىً كافٍ من حماية البيانات بالنسبة للمتلقي.[689]

على مستوى **الاتحاد الأوروبي**، وضعت المفوضية الأوروبية، بمساعدة فريق عمل المادة 29، بنوداً معيارية لحماية البيانات تم اعتمادها رسمياً بقرار من المفوضية كدليل على مستوىً كافٍ لحماية البيانات.[690] ونظراً لأن قرارات المفوضية مُلزِمة في مجملها في الدول الأعضاء، يجب على السلطات الوطنية التي تشرف على عمليات نقل البيانات أن تقر بهذه البنود التعاقدية المعيارية في إجراءاتها.[691] وبالتالي، إذا وافق المراقب المُصدِّر للبيانات والمتلقي في البلد الثالث على هذه البنود ووقَّعا عليها، فمن المفترض أن يوفر ذلك للهيئة الإشرافية دليلاً كافياً على وجود ضمانات كافية.

ومع ذلك، في قضية «شريمز»، رأت محكمة العدل التابعة للاتحاد الأوروبي أن المفوضية الأوروبية ليست لديها الصلاحية لتقييد سلطات الهيئات الإشرافية الوطنية لمراقبة نقل البيانات الشخصية إلى دولة ثالثة والتي كانت موضوع قرار حول مدى كفاية الضمانات المرتبطة بحماية البيانات صادر عن المفوضية.[692] وبالتالي، لا تُمنع الهيئات الإشرافية الوطنية من ممارسة سلطاتها، بما فيها سلطة تعليق أو حظر نقل البيانات الشخصية، عندما يتم النقل بما ينتهك قانون الاتحاد الأوروبي أو قانون حماية البيانات الوطني، كما هو الحال على سبيل المثال عندما لا يحترم مستورد البيانات البنود التعاقدية المعيارية.[693]

لا يمنع وجود بنود حماية البيانات المعيارية في الإطار القانوني للاتحاد الأوروبي المراقبين من صياغة بنود تعاقدية فردية مخصصة أخرى، طالما أن الهيئة الإشرافية قد وافقت على هذه البنود.[694] إلا أنه سيتعين عليهم ضمان نفس المستوى من الحماية كما هو منصوص عليه في البنود المعيارية لحماية البيانات. لدى اعتمادها للبنود المخصصة، تكون الهيئات الإشرافية مطالبةً بتطبيق آلية الاتساق، وذلك لضمان اتباع نهج تنظيمي متسق في جميع أنحاء الاتحاد الأوروبي.[695] وهذا يعني أنه يجب على الهيئة الإشرافية المختصة أن ترسل مشروع قرارها بشأن تلك البنود إلى المجلس الأوروبي لحماية البيانات. ويصدر المجلس الأوروبي لحماية البيانات بعد ذلك رأياً حول هذه المسألة، ويجب على الهيئة الإشرافية أن تأخذ هذا الرأي في الاعتبار الى اقصى حد عند الشروع في اتخاذ قرارها. أما إذا لم تكن تنوي اتباع رأي المجلس الأوروبية لحماية البيانات، فيتم تشغيل آلية تسوية المنازعات داخل المجلس الأوروبية لحماية البيانات، وتتبنى هذه الأخيرة بعد ذلك قراراً مُلزِماً.[696]

إن أهم خصائص البند التعاقدي المعياري هي:

- بند الطرف الثالث المستفيد الذي يمكِّن أصحاب البيانات من ممارسة الحقوق التعاقدية على الرغم من أنهم ليسوا طرفاً في العقد؛
- موافقة متلقي البيانات أو مستوردها على الخضوع لسلطة الهيئة الإشرافية الوطنية و/أو المحاكم الوطنية للمراقب المُصدِّر للبيانات في حالة حدوث منازعة.

---

[688] الاتفاقية 108 المحدثة، المادة 14 (3) (ب).

[688] الاتفاقية 108 المحدثة، المادة 14 (3) (ب).

[689] اللائحة العامة لحماية البيانات، المادة 46 (3)؛ الاتفاقية 108 المحدثة، المادة 14 (3) (ب).

[690] نفس المرجع السابق، المادة 46 (2) (ب) والمادة 46 (5).

[691] نفس المرجع السابق، المادة 46 (2) (ج)؛ المعاهدة المتعلقة بسير عمل الاتحاد الأوروبي، المادة 288.

[692] محكمة العدل التابعة للاتحاد الأوروبي، القضية C-362/14، «ماكسيميليان شريمز ضد مفوض حماية البيانات»[الغرفة الكبرى]، 6 أكتوبر 2015، الفقرات 98-96 و105-120.

[693] من أجل مراعاة موقف محكمة العدل التابعة للاتحاد الأوروبي في قضية «شريمز»، عدلت المفوضية الأوروبية قرارها بشأن البنود التعاقدية المعيارية. القرار التنفيذي للمفوضية الأوروبية (الاتحاد الأوروبي) 2016/2297 المؤرخ في 16 ديسمبر 2016 والمُعدِّل للقرارين EC/2001/497 وEU/2010/87 بشأن البنود التعاقدية المعيارية لنقل البيانات الشخصية إلى الدول الثالثة وإلى المعالجين الكائن مقرهم في هذه البلدان، بموجب الأمر التوجيهي EC/95/46 الصادر عن البرلمان الأوروبي والمجلس ، الجريدة الرسمية L344 2016 إ.

[694] اللائحة العامة لحماية البيانات، المادة 46 (3) (أ).

[695] نفس المرجع السابق، المادة 63 والمادة 64 (1) (هـ).

[696] نفس المرجع السابق، المادة 64 والمادة 65.

توجد الآن مجموعتان من البنود المعيارية المتاحة لعمليات النقل من مراقب إلى مراقب يمكن للمراقب المُصدِّر للبيانات الاختيار من بينهما.[697] أما بالنسبة لعمليات النقل من مراقب إلى معالج، فتوجد مجموعة واحدة فقط من البنود التعاقدية المعيارية.[698] إلا أن هذه البنود التعاقدية المعيارية تخضع حالياً لإجراءات قانونية.

مثال: بعد أن قضت محكمة العدل التابعة للاتحاد الأوروبي ببطلان قرار «الملاذ الآمن»،[699] لم يعد من الممكن أن تستند عمليات نقل البيانات الشخصية إلى الولايات المتحدة على قرار المفوضية حول مدى كفاية الضمانات المرتبطة بحماية البيانات هذا. وبينما كانت المفاوضات مع السلطات الأمريكية جارية، وفي انتظار اعتماد قرار كفاية جديد (تم اعتماده في آخر المطاف في 12 يوليو 2016)،[700] لم يكن من الممكن إجراء عمليات نقل البيانات الشخصية إلا بموجب أسس قانونية أخرى، مثل البنود التعاقدية المعيارية أو قواعد الشركات المُلزِمة. وقد تحولت العديد من الشركات، بما فيها «فيسبوك أيرلندا» (التي رُفعت ضدها القضية التي أدت إلى إبطال قرار «الملاذ الآمن»)، إلى استخدام البنود التعاقدية المعيارية لمواصلة عمليات نقل البيانات بين الاتحاد الأوروبي والولايات المتحدة.
لقد قدم السيد شريمز شكوى إلى الهيئة الإشرافية الأيرلندية، طالباً منها تعليق عمليات نقل البيانات إلى الولايات المتحدة على أساس البنود التعاقدية المعيارية. جوهرياً، ادعى أنه عندما يتم نقل بياناته الشخصية من الشركة الفرعية الأيرلندية التابعة لـ«فيسبوك» إلى «شركة فيسبوك» وإلى الخوادم الموجودة في الولايات المتحدة، فإنه لا يكن هناك ما يضمن حمايتها. وتلتزم «شركة فيسبوك» بالقوانين الأمريكية التي قد تُلزمها بالكشف عن البيانات الشخصية لسلطات إنفاذ القانون الأمريكية، ولا يوجد أي سبيل انتصاف قضائي متاح للأفراد الأوروبيين للاعتراض على هذه الممارسة.[701] لهذه الأسباب، خلصت محكمة العدل التابعة للاتحاد الأوروبي إلى أن قرار «الملاذ الآمن» باطل، وبينما كان حكم المحكمة مقتصراً على فحص هذا القرار فحسب، اعتبر المدعي أن نفس الأمر ينطبق على القضايا الأخرى المثارة عندما يكون نقل البيانات الشخصية مستنداً إلى البنود التعاقدية. وقت كتابة هذا الدليل، كانت القضية قيد النظر أمام المحكمة العليا الأيرلندية. ويبدو أن المدعي يعتزم إحالة القضية إلى محكمة العدل التابعة للاتحاد الأوروبي، حيث يتمثل هدفه في الطعن في صحة قرار المفوضية الأوروبية بشأن البنود التعاقدية المعيارية. وكما هو موضح في الفصل 5، فإن محكمة العدل التابعة للاتحاد الأوروبي وحدها تتمتع بصلاحية إعلان بطلان إحدى أدوات الاتحاد الأوروبي.

**عمليات نقل البيانات الشخصية الخاضعة لقواعد الشركات المُلزِمة**

يسمح **قانون الاتحاد الأوروبي** أيضاً بنقل البيانات الشخصية استناداً إلى قواعد الشركات المُلزِمة بالنسبة لعمليات النقل الدولية التي تتم داخل نفس مجموعة الشركات أو المقاولات المنتمية إلى نشاط اقتصادي مشترك.[702] وقبل أن يصبح ممكناً الاعتماد على قواعد الشركات المُلزِمة كأداة لنقل البيانات الشخصية، تحتاج الهيئة الإشرافية المختصة إلى الموافقة عليها، وفقاً لقواعد الشركات المُلزِمة، مستعينة بآلية الاتساق.

ويجب أن تكون قواعد الشركات المُلزِمة، من أجل الموافقة عليها، مُلزِمة قانوناً، وأن تغطي جميع مبادئ حماية البيانات الأساسية، وأن تنطبق على - ويتم إنفاذها من قبل - كل عضو في المجموعة. ويجب أن تمنح هذه القواعد صراحة حقوقاً قابلة للتنفيذ لأصحاب البيانات، وأن تشمل جميع مبادئ حماية البيانات الأساسية، وأن تمتثل لمتطلبات رسمية معينة، مثل التعريف بهيكل المقاولة، ووصف عمليات النقل وكيف سيتم تطبيق مبادئ حماية البيانات. ويشمل ذلك توفير مثل هذه المعلومات لأصحاب البيانات. كما يجب أن تحدد قواعد الشركات المُلزِمة،

---

[697] المجموعة الأولى واردة في مرفق المفوضية الأوروبية (2001)، قرار المفوضية EC/2001/497 المؤرخ في 15 يونيو 2001 بشأن البنود التعاقدية المعيارية لنقل البيانات الشخصية إلى بلدان ثالثة، بموجب الأمر التوجيهي EC/95/46، الجريدة الرسمية 181 L 2001 OJ؛ المجموعة الثانية واردة في مرفق المفوضية الأوروبية (2004)، قرار المفوضية EC/2004/915 المؤرخ في 27 ديسمبر 2004 والمُعدّل للقرار EC/2001/497 فيما يتعلق بإدخال مجموعة بديلة من البنود التعاقدية المعيارية لنقل البيانات الشخصية إلى دول ثالثة، الجريدة الرسمية 385 L 2004 OJ.

[698] المفوضية الأوروبية (2010)، قرار المفوضية 2010/87 المؤرخ 5 فبراير 2010 بشأن البنود التعاقدية المعيارية لنقل البيانات الشخصية إلى المعالجين الكائن مقرهم في بلدان ثالثة بموجب الأمر التوجيهي EC/95/46 الصادر عن البرلمان الأوروبي والمجلس ، الجريدة الرسمية 39 L 2010 OJ. في وقت صياغة هذا الدليل، كان استخدام البنود التعاقدية المعيارية كأساس لنقل البيانات الشخصية إلى الولايات المتحدة خاضعاً لإجراءات قانونية أمام المحكمة العليا الأيرلندية.

[699] محكمة العدل التابعة للاتحاد الأوروبي، القضية C-362/14، «ماكسيميليان شريمز ضد مفوض حماية البيانات» [الغرفة الكبرى]، 6 أكتوبر 2015.

[700] القرار التنفيذي للمفوضية الأوروبية (الاتحاد الأوروبي) 2016/1250 الصادر في 12 يوليو 2016 وفقاً للأمر التوجيهي EC/95/46 الصادر عن البرلمان الأوروبي والمجلس بشأن كفاية الحماية التي يوفرها «درع الخصوصية بين الاتحاد الأوروبي والولايات المتحدة»، الجريدة الرسمية 207 L OJ.

[701] لمزيد من المعلومات، انظر الشكوى المنقحة ضد شركة «فيسبوك أيرلندا» المحدودة المقدمة إلى مفوض حماية البيانات الأيرلندي من قبل ماكسيميليان شريمز في 1 ديسمبر 2015.

[702] اللائحة العامة لحماية البيانات، المادة 47.

من جملة أمور أخرى، حقوق أصحاب البيانات والمقتضيات المتعلقة بالمسؤولية عن أي خرق للقواعد.[703] وخلال عملية الموافقة على قواعد الشركات المُلزِمة، يتم تشغيل آلية الاتساق لتعاون الهيئات الإشرافية (الموضحة في الفصل 5).

في إطار آلية الاتساق، تستعرض الهيئة الإشرافية الرئيسية قواعد الشركات المُلزِمة المقترحة، وتعتمد مشروع قرار، ثم تقوم بتقديمه للمجلس الأوروبي لحماية البيانات. وبعد ذلك، يصدر المجلس رأياً بشأن هذه المسألة، ليصبح بإمكان الهيئة الإشرافية الرئيسية الموافقة رسمياً على قواعد الشركات المُلزِمة مع إيلاء 'أقصى قدر من الاعتبار' لرأي اللجنة. إن هذا الرأي ليس مُلزِماً قانوناً، ولكن إذا كانت الهيئة الإشرافية تعتزم تجاهله، فسيتم تشغيل آلية تسوية المنازعات وسيجب دعوة المجلس إلى اعتماد قرار مُلزِم قانوناً من طرف الأغلبية المشكَّلة من ثلثي أعضائها.[704]

بموجب **قانون مجلس أوروبا**، تشتمل الضمانات المخصصة أو المعيارية، والمضمنة في وثيقة مُلزِمة قانوناً،[705] على قواعد الشركات الملزمة أيضاً.

## 3.3.7. الاستثناءات المتعلقة بحالات خاصة

بموجب **قانون الاتحاد الأوروبي**، يمكن أن يكون نقل البيانات الشخصية إلى دولة ثالثة مبرَّراً، حتى في حالة عدم وجود قرار الكفاية أو ضمانات، مثل البنود التعاقدية المعيارية أو قواعد الشركات المُلزِمة، في أي من الظروف التالية:

- عندما يعطي صاحب البيانات موافقة صريحة على نقل البيانات؛
- عندما يدخل صاحب البيانات - أو يكون في مرحلة الإعداد للدخول - في علاقة تعاقدية يكون فيها نقل البيانات إلى الخارج ضرورياً؛
- لإبرام عقد بين مراقب بيانات وطرف ثالث لصالح صاحب البيانات؛
- لأسباب مهمة تتعلق بالمصلحة العامة؛
- لإقامة المطالبات القانونية أو تفعيلها أو الدفاع عنها؛
- لحماية المصالح الحيوية لصاحب البيانات؛
- لنقل البيانات من السجلات العامة (هذا مثال على المصالح الطاغية لعامة الجمهور حتى يتمكنوا من الوصول إلى المعلومات المخزنة في السجلات العامة).[706]

في حالة عدم انطباق أي من هذه الشروط، وعندما لا يمكن أن تستند عمليات النقل إلى قرار للمفوضية حول مدى كفاية الضمانات المرتبطة بحماية البيانات أو ضمانات مناسبة، يمكن إجراء النقل فقط عندما لا يكون متكرراً، ويتعلق بعدد محدود من أصحاب البيانات، ويكون ضرورياً لأغراض المصالح الشرعية والمقنعة لمراقب البيانات، شريطة ألا تطغى حقوق صاحب البيانات على هذه الشروط.[707] في هذه الحالات، يحتاج المراقب إلى تقييم الظروف المحيطة بعملية النقل وتوفير الضمانات. كما يجب أيضاً إبلاغ الهيئة الإشرافية وأصحاب البيانات المتأثرين بكل من عملية النقل والمصلحة الشرعية التي تبررها.

يؤكد كون الاستثناءات ملاذاً أخيراً لعمليات النقل القانونية [708] (تُستخدم فقط في حالة عدم وجود قرار الكفاية وفي حالة عدم وجود ضمانات أخرى) على أن طبيعتها هي بالفعل الاستثنائية، ويتم تسليط الضوء على ذلك بشكل أكبر في حيثيات اللائحة العامة لحماية البيانات.[709] وعليه، فإنه يتم قبول الاستثناءات كإمكانية «لإجراء عمليات النقل في ظروف معينة» على أساس الموافقة، وعندما يكون «النقل عَرَضياً وضرورياً»[710] فيما يتعلق بعقد أو مطالبة قانونية.

[703] للاطلاع على وصف أكثر تفصيلاً، انظر اللائحة العامة لحماية البيانات، المادة 47.
[704] نفس المرجع السابق، المواد 57 (1) (ق) و58 (1) (ي) و64 (1) (و) و65 (1) و(2).
[705] الاتفاقية 108 المحدّثة، المادة 14 (3) (ب).
[706] اللائحة العامة لحماية البيانات، المادة 49.
[707] نفس المرجع السابق.
[708] نفس المرجع السابق، المادة 49 (1).
[709] انظر اللائحة العامة لحماية البيانات، المادة 49 (1) (أ) و(ب) و(هـ) والحيثية 113.
[710] نفس المرجع السابق، المادة 49 (أ).

بالإضافة إلى ذلك، ووفقاً لإرشادات فريق عمل المادة 29، يجب أن يكون الاعتماد على الاستثناءات في مواقف محددة أمراً استثنائياً، ومستنداً إلى أساس الحالات الفردية، ولا يمكن استخدامه لإجراء عمليات النقل واسعة النطاق أو المتكررة.[711] وقد أكد المشرف الأوروبي على حماية البيانات بدوره على الطابع الاستثنائي للاستثناءات المستخدمة كأساس قانوني لعمليات النقل بموجب اللائحة 2001/45، مشيراً إلى أنه يجب استخدام هذا الحل 'في حالات محدودة' ولإجراء 'عمليات النقل العَرَضية'.[712]

مثال: توفر إحدى شركات خدمات نظام التوزيع العالمي (GDS) التي يقع مقرها الرئيسي في الولايات المتحدة خدمة نظام الحجوزات عبر الإنترنت للعديد من شركات الطيران والفنادق وشركات الرحلات البحرية في جميع أنحاء العالم، وتعالج بيانات عشرات الملايين من الأشخاص في الاتحاد الأوروبي. لنقل البيانات مبدئياً إلى خوادمها في الولايات المتحدة، تعتمد شركة نظام التوزيع العالمي على استثناء كأساس قانوني لعمليات النقل، ألا وهو ضرورة إبرام عقد. وبالتالي، فإنها لا تقدم أي ضمانات أخرى للبيانات الشخصية التي تنشأ في أوروبا ويتم نقلها إلى الولايات المتحدة ثم إعادة توزيعها إلى الفنادق في جميع أنحاء العالم (مما يعني عدم وجود ضمانات لعمليات النقل اللاحقة أيضاً). إن شركة نظام التوزيع العالمي هذه لا تمتثل لمتطلبات اللائحة العامة لحماية البيانات المتعلقة بعمليات نقل البيانات الدولية القانونية، لأنها تعتمد على استثناء كأساس قانوني لعمليات النقل واسعة النطاق.

ما لم تتخذ المفوضية الأوروبية قراراً حول مدى كفاية الضمانات المرتبطة بحماية البيانات، يخول للاتحاد الأوروبي أو الدول الأعضاء فيه وضع قيود على نقل فئات معينة من البيانات الشخصية إلى دولة ثالثة، على الرغم من استيفاء الشروط الأخرى لعمليات النقل هذه، لأسباب مهمة تتعلق بالمصلحة العامة. ويتعين النظر إلى هذه القيود على أنها استثنائية، ويجب على الدول الأعضاء إطلاع المفوضية الأوروبية بالمقتضيات ذات الصلة.[713]

يسمح قانون **مجلس أوروبا** بتدفقات البيانات إلى المناطق التي لا تتوفر على حماية مناسبة للبيانات في الحالات التالية:

- عندما يعطي صاحب البيانات موافقته؛
- عندما تتطلب مصالح صاحب البيانات إجراء هذا النقل؛
- عند وجود مصالح مشروعة طاغية منصوص عليها في القانون، ولا سيما المصالح العامة المهمة؛
- عندما تشكل عملية النقل تدبيراً ضرورياً ومتناسباً في مجتمع ديمقراطي.[714]

## 4.3.7. عمليات نقل البيانات الشخصية القائمة على أساس الاتفاقات الدولية

يجوز للاتحاد الأوروبي أن يبرم اتفاقات دولية، مع دول ثالثة، تنظم نقل البيانات الشخصية لأغراض محددة. ويجب أن توفر تلك الاتفاقات ضمانات مناسبة لحماية البيانات الشخصية للأفراد المعنيين. إن وجود اللائحة العامة لحماية البيانات لا يخل بهذه الاتفاقيات الدولية.[715]

ويجوز للدول الأعضاء أيضاً إبرام اتفاقات دولية، مع دول ثالثة أو منظمات دولية، توفر مستوىً مناسباً من الحماية للحقوق والحريات الأساسية للأفراد، طالما أن تلك الاتفاقات لا تؤثر على تطبيق اللائحة العامة لحماية البيانات.

هذا وتنص المادة 12 (3) (أ) من الاتفاقية 108 المحدثة على قاعدة مماثلة.
من بين الأمثلة على الاتفاقات الدولية التي تنطوي على نقل البيانات الشخصية اتفاقات سجلات أسماء الركاب (PNR).

[711] لفريق عمل المادة 29 (2005)، وثيقة عمل حول التفسير المشترك للمادة 26 (1) من الأمر التوجيهي EC/95/46 المؤرخ في 24 أكتوبر 1995، WP 114، بروكسيل، 25 نوفمبر 2005.
[712] المشرف الأوروبي على حماية البيانات، نقل البيانات الشخصية إلى دول ثالثة ومنظمات دولية من طرف مؤسسات وهيئات الاتحاد الأوروبي، ورقة موقف، بروكسل، 14 يوليو 2014، ص. 15.
[713] انظر اللائحة العامة لحماية البيانات، المادة 49 (5).
[714] الاتفاقية 108 المحدثة، المادة 14 (4).
[715] اللائحة العامة لحماية البيانات، الحيثية 102.

**سجلات أسماء الركاب**

يتم جمع بيانات سجلات أسماء الركاب من قبل شركات النقل الجوي أثناء عملية حجز الرحلات، وهي تشمل من بين أمور أخرى الأسماء والعناوين وتفاصيل بطاقات الائتمان وأرقام مقاعد الركاب. كما تقوم شركات النقل الجوي أيضاً بجمع هذه المعلومات لأغراض تجارية خاصة بها. لقد أبرم الاتحاد الأوروبي اتفاقات مع دول أخرى معينة (أستراليا وكندا والولايات المتحدة) لنقل بيانات سجلات أسماء الركاب من أجل منع الجرائم الإرهابية أو الجرائم العابرة للحدود والكشف عنها والتحقيق فيها ومقاضاة مرتكبيها. بالإضافة إلى ذلك، اعتمد الاتحاد الأوروبي الأمر التوجيهي (الاتحاد الأوروبي) 861/2016 - المعروف بمسمى «الأمر التوجيهي للاتحاد الأوروبي المتعلق بسجلات أسماء الركاب» [716]- سنة 2016. ويوفر هذا الأمر التوجيهي إطاراً قانونياً للدول الأعضاء في الاتحاد الأوروبي لنقل بيانات سجلات أسماء الركاب إلى السلطات المختصة في دول ثالثة أخرى، وذلك، بصفة مماثلة، لمنع الجرائم الإرهابية والجرائم الخطيرة أو الكشف عنها أو التحقيق فيها أو متابعة مرتكبيها. وتتم عمليات نقل سجلات أسماء الركاب إلى سلطات الدول الثالثة على أساس كل حالة على حدة وتخضع لتقييم فردي حول ما إذا كان النقل ضرورياً للأغراض المحددة في الأمر التوجيهي وما إذا كان يستوفي شرط احترام الحقوق الأساسية.

فيما يتعلق باتفاقات سجلات أسماء الركاب بين الاتحاد الأوروبي والدول الثالثة، فقد تم الطعن في توافقها مع الحقوق الأساسية للخصوصية وحماية البيانات التي يكرسها ميثاق الاتحاد الأوروبي للحقوق الأساسية. فعندما وقع الاتحاد الأوروبي اتفاقاً بشأن نقل ومعالجة بيانات سجلات أسماء الركاب في عام 2014، عقب مفاوضات مع كندا، قرر البرلمان الأوروبي إحالة مسألة تقييم شرعية الاتفاق من منظور قانون الاتحاد الأوروبي إلى محكمة العدل التابعة للاتحاد الأوروبي، ولا سيما المادتان 7 و8 من الميثاق.

مثال: رأت محكمة العدل التابعة للاتحاد الأوروبي، في رأيها حول قانونية اتفاق سجلات أسماء الركاب بين الاتحاد الأوروبي وكندا،[717] أن الاتفاق المتوخى في شكله الحالي لا يتوافق مع الحقوق الأساسية المعترف بها في ميثاق الحقوق الأساسية للاتحاد الأوروبي ، وبالتالي لا يمكن إبرامه. ونظراً لأنه ينطوي على معالجة البيانات الشخصية، فقد شكل تدخلاً في الحق في حماية البيانات الشخصية المحمي بموجب المادة 8 من الميثاق. في الوقت نفسه، يمثل هذا الاتفاق أيضاً تقييداً للحق في احترام الحياة الخاصة، الذي تكرسه المادة 7، نظراً لأن بيانات سجلات أسماء الركاب، في مجملها، يمكن أن يتم تجميعها وتحليلها بطريقة تكشف عادات السفر والعلاقات بين مختلف الأفراد والمعلومات عن أوضاعهم المالية وعاداتهم الغذائية وحالاتهم الصحية، مما يمس بحياتهم الخاصة.

إن التدخل في الحقوق الأساسية الذي أتى به الاتفاق المتوخى يسعى إلى تحقيق هدف متعلق بالمصلحة العامة، ألا وهو الأمن العام ومكافحة الإرهاب والجرائم الخطيرة عبر الوطنية. ومع ذلك، أشارت محكمة العدل التابعة للاتحاد الأوروبي إلى أنه لكي يكون هناك ما يبرر هذا الاتفاق، يجب أن يقتصر التدخل على ما هو ضروري للغاية لتحقيق الهدف المنشود. وبعد تحليل مقتضيات الاتفاق المتوخى، خلصت محكمة العدل التابعة للاتحاد الأوروبي إلى أنه لا يفي بمعيار 'الضرورة القصوى'. من بين العوامل التي أخذتها المحكمة بعين الاعتبار للتوصل إلى هذا الاستنتاج ما يلي:

1. كون الاتفاق المتوخى ينطوي على نقل بيانات حساسة. إذ يمكن أن تتضمن سجلات أسماء الركاب التي يتم جمعها وفقاً للاتفاق المتوخى بيانات حساسة، مثل المعلومات التي تكشف عن الأصل العرقي أو الإثني أو المعتقدات الدينية أو الحالة الصحية للراكب. إن نقل ومعالجة البيانات الحساسة من قبل السلطات الكندية يمكن أن يشكل خطراً على مبدأ عدم التمييز، وبالتالي فإنهما يتطلبان مبرراً دقيقاً وقوياً، يستند إلى أسس أخرى غير الأمن العام ومكافحة الجرائم الخطيرة. إلا أن الاتفاق المتوخى لم يقدم مبرراً من هذا القبيل.[718]

2. يُعتبر التخزين المتواصل — سجلات أسماء الركاب الخاصة بجميع الركاب، لمدة خمس سنوات، حتى بعد مغادرة الركاب كندا، أنه يتجاوز حدود الضرورة القصوى. إذ اعتبرت محكمة العدل التابعة للاتحاد الأوروبي أنه يمكن أن يكون من المسموح للسلطات الكندية الاحتفاظ ببيانات الركاب الذين تشير الأدلة الموضوعية إلى أنهم قد يشكلون تهديداً للأمن العام، حتى بعد مغادرتهم كندا. وعلى النقيض من ذلك، لا يوجد ما يبرر تخزين البيانات الشخصية لجميع الركاب الذين لا توجد حتى أدلة غير مباشرة تشير إلى أنهم يشكلون خطراً على الأمن العام.[719]

[716] الأمر التوجيهي (الاتحاد الأوروبي) 861/2016 الصادر عن البرلمان الأوروبي والمجلس بتاريخ 27 أبريل 2016 بشأن استخدام بيانات سجل أسماء الركاب (PNR) للوقاية من الجرائم الإرهابية والجرائم الخطيرة والكشف عنها والتحقيق فيها ومقاضاة مرتكبيها، الجريدة الرسمية L 119 OJ 2016 .

[717] محكمة العدل التابعة للاتحاد الأوروبي، الرأي 1/15 للمحكمة (الغرفة الكبرى)، 26 يوليو 2017.

[718] نفس المرجع السابق، الفقرة 165.

[719] نفس المرجع السابق، الفقرات 207-204.

قدمت اللجنة الاستشارية للاتفاقية 108 رأياً حول الآثار المترتبة على حماية البيانات لاتفاقات سجلات أسماء الركاب بموجب قانون مجلس أوروبا.[720]

**بيانات المراسلات**

كانت «جمعية الاتصالات المالية العالمية بين البنوك - سويفت» (SWIFT) الواقع مقرها في بلجيكا، وهي المعالج لمعظم التحويلات المالية العالمية من البنوك الأوروبية، تعمل بواسطة مركز 'موازٍ' في الولايات المتحدة، وقد توصلت بطلب للإفصاح عن البيانات لوزارة الخزانة الأمريكية لأغراض التحقيق في الإرهاب بموجب «برنامج تتبع تمويل الإرهاب» التابع للوزارة.[721]

من وجهة نظر الاتحاد الأوروبي، لم يكن هناك أساس قانوني كافٍ للإفصاح عن هذه البيانات - التي تخص بشكل رئيسي المواطنين في الاتحاد الأوروبي - للولايات المتحدة فقط على أساس وجود أحد مراكز معالجة بيانات «سويفت» في الولايات المتحدة.

وقد تم إبرام اتفاق خاص بين الاتحاد الأوروبي والولايات المتحدة، يُعرف بمسمى اتفاق «سويفت»، سنة 2010 لتوفير الأساس القانوني اللازم ولضمان معايير كافية لحماية البيانات.[722]

بموجب هذا الاتفاق، يستمر تقديم البيانات المالية المخزنة من طرف «جمعية الاتصالات المالية العالمية بين البنوك» إلى وزارة الخزانة الأمريكية لأغراض منع الإرهاب أو تمويل الإرهاب والتحقيق فيهما والكشف عنهما ومتابعة مرتكبيهما. ويجوز لوزارة الخزانة الأمريكية طلب البيانات المالية من «جمعية الاتصالات المالية العالمية بين البنوك» وفق الشروط التالية:

- أن يحدد الطلب بأكبر قدر ممكن من الوضوح البيانات ؛
- أن يثبت بوضوح ضرورة الحصول على البيانات؛
- أن يكون مُفصَّلاً بأكبر قدر ممكن من الدقة لتقليل كمية البيانات المطلوبة؛
- ألا يهدف للحصول على أي بيانات تتعلق بـ»منطقة المدفوعات الأوروبية الموحدة» (SEPA).[723]

يجب أن يتلقى اليوروبول نسخة من كل طلب مُقدَّم من وزارة الخزانة الأمريكية وأن يتحقق مما إذا كان يتم الالتزام بمبادئ اتفاق «سويفت» أم لا.[724] فإذا تم التأكد من ذلك، يجب على «جمعية الاتصالات المالية العالمية بين البنوك» تقديم البيانات المالية مباشرة إلى وزارة الخزانة الأمريكية. ويجب على الوزارة تخزين البيانات المالية في بيئة مادية آمنة لا يتم الوصول إليها إلا من قبل المحللين الذين يحققون في قضايا الإرهاب أو تمويله، ويجب ألا تكون البيانات المالية مترابطة مع أية قاعدة بيانات أخرى. بشكل عام، يجب حذف البيانات المالية المُستلَمة من «جمعية الاتصالات المالية العالمية بين البنوك» في أجل لا يتجاوز خمس سنوات من تاريخ استلامها. ويمكن الاحتفاظ بالبيانات المالية ذات الصلة بتحقيقات أو متابعات قضائية محددة فقط طالما تكون تلك البيانات ضرورية لإجراء هذه التحقيقات أو الملاحقات القضائية.

ويجوز لوزارة الخزانة الأمريكية نقل المعلومات من البيانات التي تستلمها من «جمعية الاتصالات المالية العالمية بين البنوك» إلى سلطات إنفاذ القانون أو الأمن العام أو مكافحة الإرهاب داخل الولايات المتحدة أو خارجها حصرياً للتحقيق في قضايا الإرهاب وتمويله أو الكشف عنها أو منعها أو مقاضاة مرتكبيها. وعندما يخص النقل اللاحق للبيانات المالية مواطناً أو مقيماً في دولة عضو في الاتحاد الأوروبي، فإن أي

---

[720] مجلس أوروبا، رأي حول آثار معالجة سجلات أسماء الركاب المترتبة على حماية البيانات، 19 ،18rev (2016) T-PD أغسطس 2016.

[721] انظر، في هذا السياق، فريق عمل المادة 29 (2011)، الرأي 14/2011 بشأن قضايا حماية البيانات المتعلقة بمنع غسل الأموال وتمويل الإرهاب، WP 186، بروكسل، 13 يونيو 2011؛ فريق عمل المادة 29 (2006)، الرأي 10/2006 بشأن معالجة البيانات الشخصية من قبل «جمعية الاتصالات المالية العالمية بين البنوك - سويفت»، WP 128، بروكسل، 22 نوفمبر 2006؛ لجنة حماية الخصوصية البلجيكية 2008) ((Commission de la protection de la vie privée)، 'بدء إجراء المراقبة والتوصية فيما يتعلق بـ»شركة سويفت التعاونية ذات المسؤولية المحدودة» (SWIFT scrl)'، قرار، 9 ديسمبر 2008.

[722] قرار المجلس الأوروبي EU/2010/412 المؤرخ في 13 يوليو 2010 بشأن إبرام الاتفاق بين الاتحاد الأوروبي والولايات المتحدة الأمريكية بشأن معالجة ونقل بيانات المراسلات المالية من الاتحاد الأوروبي إلى الولايات المتحدة لأغراض «برنامج تتبع تمويل الإرهاب»، الجريدة الرسمية 195 L 2010 OJ، الصفحتان 3 و4. نص الاتفاقية مرفق بهذا القرار، الجريدة الرسمية 195 L 2010 OJ، الصفحات 14-5.

[723] نفس المرجع السابق، المادة 4 (2).

[724] أجرت هيئة الإشراف المشتركة لليوروبول عمليات تدقيق على أنشطة اليوروبول في هذا المجال.

مشاركة للبيانات مع سلطات دولة ثالثة تخضع لموافقة مسبقة من السلطات المختصة في الدولة العضو المعنية. ويمكن تطبيق استثناءات عندما تكون مشاركة البيانات ضرورية لمنع تهديد فوري وخطير للأمن العام.

ويقوم مشرفون مستقلون، بمن فيهم شخص معين من قبل المفوضية الأوروبية، بمراقبة الامتثال لمبادئ اتفاق «سويفت». وهم يتمتعون بإمكانية مراجعة جميع عمليات البحث التي طرأت على البيانات المَقدَّمة في الوقت الحقيقي وبأثر رجعي، وطلب معلومات إضافية لتبرير الروابط الإرهابية لعمليات البحث هذه، كما أن لديهم السلطة لمنع أي عمليات بحث يبدو أنها تنتهك الضمانات المنصوص عليها في الاتفاق.

يحق لأصحاب البيانات الحصول على تأكيد الهيئة الإشرافية المختصة التابعة للاتحاد الأوروبي على أنه قد تم الامتثال لحقوقهم في حماية البيانات الشخصية. ويتمتع أيضاً أصحاب البيانات بالحق في تصحيح أو محو أو حجب بياناتهم التي جمعتها الخزانة الأمريكية وخزنتها بموجب اتفاق سويفت. ومع ذلك، قد تخضع حقوق أصحاب البيانات في الولوج إلى بياناتهم لقيود قانونية. وعندما يُرفض الولوج إلى البيانات، يجب إخبار صاحب البيانات كتابياً بالرفض وبحقه في طلب الانتصاف الإداري والقضائي في الولايات المتحدة.

يدوم سريان مفعول اتفاق سويفت لمدة خمس سنوات، وقد استمرت المدة الأولى من صلاحيته إلى غشت 2015. ويمتد الاتفاق تلقائياً لفترات متعاقبة تبلغ كل منها سنة واحدة ما لم يشعر أحد الأطراف الطرف الآخر، قبل ستة أشهر على الأقل، بنيته عدم تمديد الاتفاق. وكان التمديد التلقائي للاتفاق قد طُبق في غشت 2015 و2016 و2017 ويضمن صلاحية اتفاق سويفت حتى غشت 2018 على الأقل.[725]

[725] نفس المرجع السابق، المادة 23 (2).

# 8

# حمايــة البيانــات في سيــاق الشرطـــة والعدالـــة الجنائيـــة

| الاتحاد الأوروبي | المسائل المتناولة | مجلس أوروبا |
|---|---|---|
| الأمر التوجيهي الخاص بحماية البيانات والموجه إلى الشرطة وسلطات العدالة الجنائية | عموماً | الاتفاقية 108 المحدثة |
| | الشرطة | التوصية المتعلقة بالشرطة<br>دليل عملي بشأن استخدام البيانات الشخصية في قطاع الشرطة |
| | المراقبة | المحكمة الأوروبية لحقوق الإنسان، قضية «ب. ب. ضد فرنسا»، القضية رقم 5335/06، 2009<br>المحكمة الأوروبية لحقوق الإنسان، قضية «س. ومارير ضد المملكة المتحدة» [الغرفة الكبرى]، القضيتان رقم 30562/04 ورقم 30566/04، 2008<br>المحكمة الأوروبية لحقوق الإنسان، قضية «ألان ضد المملكة المتحدة»، القضية 48539/99، 2002<br>المحكمة الأوروبية لحقوق الإنسان، قضية «مالون ضد المملكة المتحدة»، القضية رقم 8691/79، 1984<br>المحكمة الأوروبية لحقوق الإنسان، قضية «كلاس وآخرون ضد ألمانيا»، القضية رقم 5029/71، 1978<br>المحكمة الأوروبية لحقوق الإنسان، قضية «شابو وفيسي ضد المجر»، القضية 37138/14، 2016<br>المحكمة الأوروبية لحقوق الإنسان، قضية «فيتر ضد فرنسا»، القضية رقم 59842/00، 2005 |
| | الجريمة السيبرانية | الاتفاقية بشأن بالجرائم السيبرانية |

| صكوك قانونية محددة أخرى | | |
|---|---|---|
| قرار بروم | فيما يخص البيانات الخاصة: بصمات الأصابع والحمض النووي والشعب والمعلومات الخاصة بالمسافرين جواً وبيانات الاتصالات السلكية واللاسلكية، وغيرها من البيانات. | الاتفاقية 108 المحدثة، المادة 6<br>التوصية المتعلقة بالشرطة، دليل عملي بشأن استخدام البيانات الشخصية في قطاع الشرطة |
| المبادرة السويدية (القرار الإطاري الصادر عن المجلس الأوروبي رقم JHA/2006/960) | تبسيط تبادل المعلومات والاستخبارات بين سلطات إنفاذ القانون | المحكمة الأوروبية لحقوق الإنسان، قضية «س. ومارير ضد المملكة المتحدة» [الغرفة الكبرى]، القضيتان رقم30562/04 و30566/04، 2008 |
| الأمر الصادر عن الاتحاد الأوروبي رقم 681/2016 بشأن استخدام بيانات سجلات أسماء الركاب (PNR) لمنع الجرائم الإرهابية والجرائم الخطيرة واكتشافها والتحقيق فيها ومحاكمة مرتكبيها<br>محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-293/12 وC-594/12، الحقوق الرقمية أيرلندا المحدودة وحكومة ولاية كيرنتن وآخرون [الغرفة الكبرى]، 2014<br>محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-203/15 وC-698/15، تيلي 2 السويد المحدودة ووزارة الداخلية ضد طوم واطسون وآخرين [الغرفة الكبرى]، 2016 | الاحتفاظ بالبيانات الشخصية | المحكمة الأوروبية لحقوق الإنسان، قضية «ب. ب. ضد فرنسا»، القضية رقم 5335/06، 2009 |
| اللائحة المتعلقة باليوروبول<br>قرار وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية | من قبل وكالات خاصة | التوصية المتعلقة بالشرطة |
| قرار شينغن 2<br>اللائحة المتعلقة بالنظام المعلوماتي الخاص بالتأشيرات<br>اللائحة المتعلقة بالنظام الأوروبي لمضاهاة بصمات الأصابع (Eurodac)<br>القرار المتعلق بنظام المعلومات الجمركية | بأنظمة معلوماتية مشتركة خاصة | التوصية المتعلقة بالشرطة<br>المحكمة الأوروبية لحقوق الإنسان، داليا ضد فرنسا، القضية رقم 07/964، 2010 |

للتوفيق بين مصالح الأفراد في حماية البيانات ومصالح المجتمع في جمع البيانات لغرض مكافحة الجريمة وضمان السلامة الوطنية و العامة، سن مجلس أوروبا والاتحاد الأوروبي صكوكاً قانونية خاصة. يقدم هذا الجزء لمحة عامة عن قانون مجلس أوروبا (الجزء 1.8) وقانون الاتحاد الأوروبي (الجزء 2.8) فيما يتعلق بحماية البيانات في المسائل المتعلقة بالشرطة والعدالة الجنائية.

## 1.8. قانون مجلس أوروبا بشأن حماية البيانات والأمن الوطني، والمسائل المتعلقة بالشرطة والعدالة الجنائية

### النقاط الرئيسية

- تنطبق الاتفاقية 108 المحدثة وتوصية مجلس أوروبا المتعلقة بالشرطة على حماية البيانات في جميع جوانب عمل الشرطة.
- تُعد الاتفاقية بشأن الجرائم السيبرانية (اتفاقية بودابيست) صكاً قانونياً دولياً ملزماً يتناول الجرائم المرتكبة بواسطة الشبكات الإلكترونية وفي حقها. وتُعنى أيضاً بالتحقيق في الجرائم غير السيبرانية التي تنطوي على أدلة إلكترونية.

من بين أهم الاختلافات بين قانون مجلس أوروبا وقانون الاتحاد الأوروبي أنه خلافاً لقانون الاتحاد الأوروبي، يُطبق **قانون مجلس أوروبا** أيضاً في مجال الأمن الوطني. ويعني ذلك أن الأطراف المتعاقدة تحتاج إلى البقاء ضمن اختصاص المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان حتى فيما يخص الأنشطة المتعلقة بالأمن الوطني. وتهم العديد من الأحكام الصادرة عن المحكمة الأوروبية لحقوق الإنسان أنشطة الدولة في المجالات الحساسة لقانون الأمن الوطني وممارساته.[726]

وفيما يتعلق بالشرطة والعدالة الجنائية، على الصعيد الأوروبي، تشمل الاتفاقية 108 المحدثة جميع مجالات معالجة البيانات الشخصية، ويُقصد بمقتضياتها تنظيم معالجة البيانات الشخصية عموماً. نتيجة لذلك، تنطبق الاتفاقية 108 المحدثة على حماية البيانات في مجال الشرطة والعدالة الجنائية. ولا يُسمح بمعالجة البيانات الجينية، والبيانات الشخصية المتعلقة بالجرائم والدعاوى والإدانات الجنائية وأي تدابير أمنية ذات صلة بها، والبيانات البيومترية التي تحدد هوية الشخص تحديداً فريداً، بالإضافة إلى أي بيانات شخصية حساسة، إلا عندما توجد الضمانات المناسبة التي تقي من الأخطار التي تنشأ عن معالجة تلك البيانات والتي تهدد مصالح أصحاب البيانات وحقوقهم وحرياتهم؛ لا سيما خطر التمييز.[727]

تتطلب المهام القانونية للشرطة وسلطات العدالة الجنائية في غالب الأحيان معالجة البيانات الشخصية، ما قد يكون له عواقب خطيرة على الأفراد المعنيين. وترشد التوصية المتعلقة بالشرطة التي اعتمدها مجلس أوروبا سنة 1987 الدول الأعضاء بشأن كيف ينبغي لها أن تنفذ مبادئ 108 الاتفاقية في سياق معالجة سلطات الشرطة للبيانات الشخصية.[728] واستُكملت التوصية بدليل عملي بشأن استخدام البيانات الشخصية في قطاع الشرطة، اعتمدته اللجنة الاستشارية للاتفاقية 108.[729]

مثال: في قضية «د. ل. ضد بلغاريا»،[730] وضعت المصالح الاجتماعية المدعي في مؤسسة تربوية آمنة وفقاً لقرار صادر عن المحكمة. وتعرضت جميع المراسلات المكتوبة والمحادثات الهاتفية لمراقبة شاملة وعشوائية من قبل المؤسسة. وقضت المحكمة الأوروبية لحقوق الإنسان بوجود انتهاك للمادة 8، نظراً إلى أن الإجراء المعني لم يكن ضرورياً في مجتمع ديموقراطي. وذكرت المحكمة أنه كان من الواجب القيام بأي شيء ممكن لتمكين القاصرين الموضوعين في مؤسسة ما من الاتصال بالعالم الخارجي اتصالاً كافياً، لأن ذلك كان جزءاً لا يتجزأ من حقهم في المعاملة الكريمة، وكان أساسياً لإعدادهم للاندماج في المجتمع. وينطبق ذلك على الزيارات بقدر ما ينطبق على المراسلات المكتوبة أو المحادثات الهاتفية. علاوة على ذلك، لم تميز المراقبة بين الاتصال بأفراد العائلة والمنظمات غير الحكومية التي تمثل حقوق الأطفال أو المحامين. بالإضافة إلى ذلك، لم يستند قرار اعتراض الاتصال إلى تحليل فردي للأخطار في كل حالة معينة.

[725] نفس المرجع السابق، المادة 23 (2).

[726] انظر، على سبيل المثال، المحكمة الأوروبية لحقوق الإنسان، كلاس وآخرون ضد ألمانيا، القضية رقم 5029/71، 6 سبتمبر 1978؛ المحكمة الأوروبية لحقوق الإنسان، روتارو ضد رومانيا [الغرفة الكبرى]، القضية رقم 28341/95، 4 مايو 2000، والمحكمة الأوروبية لحقوق الإنسان، شابو وفيسي ضد المجر، القضية رقم 37138/14، 12 يناير 2016.

[727] الاتفاقية 108 المحدثة، المادة 6.

[728] مجلس أوروبا، لجنة الوزراء (1987)، التوصية رقم Rec(87)15 الموجهة إلى الدول الأعضاء والمنظمة لاستخدام البيانات الشخصية في قطاع الشرطة، 17 سبتمبر 1987.

[729] مجلس أوروبا (2018)، اللجنة الاستشارية للاتفاقية 108، دليل عملي بشأن استخدام البيانات الشخصية في قطاع الشرطة، T-PD (2018) 1.

[730] المحكمة الأوروبية لحقوق الإنسان، د. ل. ضد بلغاريا، القضية رقم 7472/14، 19 مايو 2016.

مثال: في قضية «دراغوبيفيتش ضد كرواتيا»،[731] اشتُبه في ضلوع المدعي في الاتجار بالمخدرات. وأدين بعد أن أجاز قاضي التحقيق استخدام تدابير المراقبة السرية لاعتراض المكالمات الهاتفية للمدعي. وقضت المحكمة الأوروبية لحقوق الإنسان بأن ذلك الإجراء، والذي قُدمت ضده شكوى، شكل تدخلا في الحق في احترام الحياة الخاصة والمراسلات. واستند الترخيص الذي منحه قاضي التحقيق إلى مجرد قول سلطة الادعاء إن «التحقيق لم يكن ممكناً إجراؤه بوسائل أخرى». واشارت المحكمة الأوروبية لحقوق الإنسان أيضاً إلى أن المحاكم الجنائية كانت قد حدت من تقييمها فيما يتعلق باستخدام تدابير المراقبة، وأن الحكومة لم تقدم سبل الانتصاف المتاحة. ونتيجة لذلك، قضت بوجود انتهاك للمادة 8.

## 1.1.8. التوصية المتعلقة بالشرطة

لطالما اعتبرت المحكمة الأوروبية لحقوق الإنسان أن تخزين هيئات الشرطة أو سلطات الأمن الوطني البيانات الشخصية و الاحتفاظ بها يشكل تدخلاً في المادة 8 (1) من الاتفاقية الأوروبية لحقوق الإنسان. وتتناول الكثير من الأحكام الصادرة عن المحكمة الأوروبية لحقوق الإنسان تبرير ذلك التدخل.[732]

مثال: في قضية «ب. ب. ضد فرنسا»،[733] تم الحكم على المدعي لانخراطه في جرائم جنسية في حق قاصرين يبلغون من العمر 15 سنة بصفته شخصاً في موضع ثقة. وأكمل عقوبته الحبسية سنة 2000. وبعد سنة، طلب شطب تلك العقوبة من سجله الجنائي، لكن الطلب قوبل بالرفض. وفي 2004، أنشأ قانون فرنسي قاعدة بيانات قضائية وطنية تتعلق بمرتكبي الجرائم الجنسية وأُخبر المدعي بإدراج اسمه فيها. وقضت المحكمة الأوروبية لحقوق الإنسان بأن إدراج المدان بارتكاب جرائم جنسية في قاعدة البيانات القضائية الوطنية يندرج في إطار المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان. ومع ذلك، وبالنظر إلى أن الضمانات الكافية لحماية البيانات مثل حق صاحب البيانات في محو البيانات، وتحديد مدة تخزين البيانات وتقييد الولوج إلى تلك البيانات، كانت قد نُفذت، فإنه قد تمت الموازنة بصورة عادلة بين المصالح المتضاربة الخاصة والعامة للمعنيين. وخلصت المحكمة إلى عدم انتهاك المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان.

مثال: في قضية «س. ومابر ضد المملكة المتحدة»،[734] كان كلا المدعيين متهمين بارتكاب جرائم جنائية، دون أن يُدانا بها. إلا أن الشرطة احتفظت ببصمات أصابعهما، وعينات خلوية خاصة بهما وصور تحليلية لحمضيهما النوويين وخزنتها. وسمح القانون بالاحتفاظ لمدة غير محدودة بالبيانات البيومترية السابقة الذكر عندما اشتُبه في ارتكاب الشخص لجريمة جنائية، رغم أنه تمت تبرئة المشتبه فيه والإفراج عنه لاحقاً. وقضت المحكمة الأوروبية لحقوق الإنسان بأن الاحتفاظ الشامل والعشوائي بالبيانات الشخصية لم يكن محدود المدة، في حين لم يكن للفردين اللذين تمت تبرئتهما سوى إمكانيات محدودة لطلب حذف البيانات وشكل تدخلاً غير متناسب في حق المدعيين في احترام الحياة الخاصة. وخلصت المحكمة إلى انتهاك المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان.

ومن بين المسائل البالغة الأهمية في سياق الاتصالات الإلكترونية تدخل السلطات العامة في الحقين في حماية الخصوصية والبيانات. هذا ولا يُسمح بوسائل المراقبة الجماعية أو اعتراض الاتصالات، مثل أجهزة الاستماع أو التنصت، إلا إذا كان القانون ينص على ذلك ويشكل إجراءً ضرورياً في مجتمع ديموقراطي لمصلحة ما يلي:

- حماية أمن الدولة؛
- السلامة العامة؛
- المصالح المالية للدولة؛
- قمع الجرائم الجنائية؛
- أو حماية صاحب البيانات أو حقوق الآخرين وحرياتهم.

[731] المحكمة الأوروبية لحقوق الإنسان، دراغوبيفيتش ضد كرواتيا، القضية رقم 68955/11، 15 يناير 2015.

[732] انظر، على سبيل المثال، المحكمة الأوروبية لحقوق الإنسان، لينجر ضد السويد، القضية رقم 9248/81، 26 مارس1987؛ المحكمة الأوروبية لحقوق الإنسان، م. م. ضد المملكة المتحدة، القضية رقم 24029/07، 13 نوفمبر 2012؛ المحكمة الأوروبية لحقوق الإنسان، م. ك. ضد فرنسا، القضية رقم 19522/09، 18 أبريل 2013، أو المحكمة الأوروبية لحقوق الإنسان، أيكاغير ضد فرنسا، القضية رقم 8806/12، 22 يونيو 2017.

[733] المحكمة الأوروبية لحقوق الإنسان، ب. ب. ضد فرنسا، القضية رقم 5335/06، 17 ديسمبر 2009.

[734] المحكمة الأوروبية لحقوق الإنسان، س. ومارب ضد المملكة المتحدة [الغرفة الكبرى]، القضيتان رقم 30562/04 و30566/04، 04 ديسمبر 2008، الفقرتان 119 و125.

وتتناول العديد من الأحكام الأخرى الصادرة عن المحكمة الأوروبية لحقوق الإنسان تبرير التدخل في الحق في الخصوصية من خلال تنفيذ المراقبة.

مثال: في قضية «ألان ضد المملكة المتحدة»،[735] سجلت السلطات سراً المحادثات الخاصة بين سجين وصديق له في قاعة الزيارات في السجن ومحادثات السجين مع متهم آخر في إحدى زنزانات السجن. قضت المحكمة الأوروبية لحقوق الإنسان بأن استخدام أجهزة التسجيل السمعي والمرئي في زنزانة المدعي وفي قاعة الزيارات بالسجن وبشأن سجين زميل كان بمثابة التدخل في حق المدعي في الحياة الخاصة. ونظراً إلى عدم وجود نظام قانوني ينظم استخدام الشرطة أجهزة التسجيل السرية في الوقت المعني، لم يكن ذلك التدخل متوافقاً مع القانون. وخلصت المحكمة إلى انتهاك المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان.

مثال: في قضية «رومان زاخاروف ضد روسيا»،[736] أقام المدعي دعوى قضائية في حق ثلاثة من مشغلي شبكة الهاتف النقال. واحتج بأن حقه في احترام خصوصية اتصالاته الهاتفية كان قد انتُهك، لأن المشغلين كانوا قد ركبوا جهازاً يسمح لدائرة الأمن الاتحادي باعتراض اتصالاته الهاتفية دون ترخيص قضائي مسبق. وقضت المحكمة الأوروبية لحقوق الإنسان بأن المقتضيات القانونية الوطنية التي تنظم اعتراض الاتصالات لم تتح ضمانات كافية وفعالة للوقاية من التعسف وخطر الشطط في استعمال السلطة، على وجه التخصيص، لا يقتضي القانون الوطني حذف البيانات المخزنة بعد الإيفاء بغرض التخزين. علاوة على ذلك، على الرغم من طلب الترخيص القضائي، إلا أن التدقيق القضائي كان محدوداً.

مثال: في قضية «شابو وفيسي ضد المجر»،[737] زعم المدعيان أن التشريعات المجرية انتهكت المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان، لأنها لم تكن مفصلة أو دقيقة بما يكفي. علاوة على ذلك، تم الاحتجاج بأن التشريعات لم تتح الضمانات الكافية للوقاية من الشطط في استعمال السلطة والتعسف. وقضت المحكمة الأوروبية لحقوق الإنسان بأن القانون المجري لم يقتض إخضاع المراقبة لترخيص المحكمة. ومع ذلك، لاحظت المحكمة أنه على الرغم من أن ذلك الإشراف كان خاضعاً لموافقة وزارة العدل، إلا أنه كان سياسياً أساساً وعاجزاً عن ضمان التقييم المطلوب 'للضرورة الملحة'. بالإضافة إلى ذلك، لم ينص القانون الوطني على المراجعة القضائية، نظراً إلى عدم إرسال أي إشعار إلى أصحاب البيانات. وخلصت المحكمة إلى انتهاك المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان.

نظراً إلى أن معالجة سلطات الشرطة للبيانات قد يكون لها أثر كبير على الأشخاص المعنيين، تُعد قواعد حماية البيانات المفصلة الخاصة بمعالجة البيانات الشخصية ضرورية على وجه خاص في ذلك المجال. وسعت توصية مجلس أوروبا المتعلقة بالشرطة إلى معالجة هذه المسألة بتقديم الإرشاد بشأن كيف ينبغي للبيانات الشخصية أن تُجمع لغرض عمل الشرطة؛ وكيف ينبغي الاحتفاظ بملفات البيانات في ذلك المجال؛ ومن الذي يُسمح له بالولوج إلى تلك الملفات، بما في ذلك شروط نقل البيانات الشخصية إلى سلطات الشرطة الأجنبية؛ وكيف ينبغي تمكين أصحاب البيانات لممارسة حقهم في حماية البيانات؛ وكيف ينبغي للهيئات المستقلة أن تنفذ المراقبة. كما تمت دراسة الالتزام بإتاحة أمن البيانات الملائم.

لا تنص التوصية على جمع سلطات الشرطة البيانات الشخصية بطريقة غير محددة وعشوائية. وتحصر التوصية جمع سلطات الشرطة البيانات الشخصية فيما يكون ضرورياً لمنع خطر حقيقي أو محاكمة مرتكبي جرائم جنائية معينة. ويجب أن يستند جمع بيانات إضافية إلى تشريعات وطنية معينة. وينبغي لمعالجة البيانات الحساسة أن تقتصر على ما يكون ضرورياً للغاية في سياق تحقيق خاص.

عندما تُجمع البيانات الشخصية دون علم صاحب البيانات، يجب إخبار هذا الأخير بجمع البيانات طالما أن ذلك الكشف لا يضر بالتحقيق. ويجب أن يستند جمع البيانات بالمراقبة التقنية أو غيرها من الوسائل الآلية إلى أساس قانوني معين.

[735] المحكمة الأوروبية لحقوق الإنسان، ألان ضد المملكة المتحدة، القضية رقم 48539/99، 05 نوفمبر 2002.
[736] المحكمة الأوروبية لحقوق الإنسان، رومان زاخاروف ضد روسيا، القضية رقم 47143/06، 04 ديسمبر 2015.
[737] المحكمة الأوروبية لحقوق الإنسان، شابو وفيسي ضد المجر، القضية رقم 37138/14، 12 يناير 2016.
[738] المحكمة الأوروبية لحقوق الإنسان، فيرسيني-كامبينكي وكراسنيانسكي ضد فرنسا، القضية رقم 49176/11، 16 يونيو 2016.

مثال: في قضية «فيرسيني-كاميينكي وكراسنيانسكي ضد فرنسا»،[738] أجرت المدعية، وهي محامية، محادثة هاتفية مع موكل كان خطه الهاتفي يُعترض بناءً على طلب قاضي التحقيق. وأظهر نص المحادثة أنها كانت قد كشفت عن معلومات مشمولة بالامتياز المهني القانوني. وأرسل المدعي العام تلك المعلومات إلى مجلس نقابات المحامين الذي فرض عقوبة على المدعية. وأقرت المحكمة الأوروبية لحقوق الإنسان بحدوث تدخل في الحق في احترام الحياة الخاصة والمراسلات، ليس فيما يخص الشخص الذي تعرض هاتفه للتنصت فحسب، وإنما أيضاً فيما يخص المدعية التي تم اعتراض اتصالها وتدوين محتواه. وكان التدخل قد حدث بما يتوافق مع القانون وسعى إلى الهدف الشرعي لمنع حدوث الإخلال بالنظام. وكانت المدعية قد حصلت على مراجعة لمشروعية تقديم نص تسجيلات التنصت على الهاتف في سياق الإجراءات التأديبية التي اتُّخذت في حقها. وعلى الرغم من أنها لم تكن قادرة على التقدم بطلب لإلغاء نص المحادثة الهاتفية، فإن المحكمة الأوروبية لحقوق الإنسان رأت أنه قد كان ثمة تدقيق فعال بإمكانه أن يحصر التدخل المشتكى منه فيما يكون ضرورياً في مجتمع ديموقراطي. وقضت المحكمة الأوروبية لحقوق الإنسان بأن الحجة القائلة بأن إمكانية إقامة دعوى جنائية في حق محام استناداً إلى نص المحادثة قد يكون له تأثير يقيد حرية الاتصال بين محام وموكله، وبالتالي يقيد حقوق الموكل في الدفاع، لم تكن معقولة حيث أن الإفصاح الذي قامت به المحامية نفسها كان من شأنه أن يكون بمنزلة السلوك غير القانوني من جانبها. ونتيجة لذلك، لم يُستنتج انتهاك المادة 8.

تنص توصية مجلس أوروبا المتعلقة بالشرطة على أنه عندما يتعلق الأمر بتخزين البيانات الشخصية، يجب التمييز تمييزاً واضحاً بين: البيانات الإدارية وبيانات الشرطة؛ وبين البيانات الشخصية لمختلف أنواع أصحاب البيانات، مثل المشتبه فيهم، والأشخاص المدانين، والضحايا والشهود؛ وبين البيانات التي تعتبر حقائق ثابتة والبيانات التي تستند إلى الشكوك والتكهنات.

يجب أن يُحصر الغرض الذي من أجله قد تُستخدم بيانات الشرطة حصراً صارماً. وهوما يترتب عنه عواقب بالنسبة لكشف بيانات الشرطة للأطراف الثالثة: ينبغي تنظيم نقل تلك البيانات أو كشفها داخل قطاع الشرطة من خلال وجود أو انعدام مصلحة شرعية في مشاركة المعلومات. ولا ينبغي السماح بنقل تلك البيانات أو كشفها خارج قطاع الشرطة إلا في حالة وجود التزام أو ترخيص قانوني واضح.

مثال: في قضية «كارابيوغلو ضد تركيا»،[739] تمت مراقبة الخطوط الهاتفية للمدعي، وهو قاضي، في سياق تحقيق جنائي في منظمة غير قانونية اشتُبه في انتمائه إليها، أو اعتُقد أنه يقدم إليها المساعدة والدعم. وبعد قرار عدم المتابعة، أتلف المدعي العام المكلف بالتحقيق الجنائي التسجيلات المعنية. ومع ذلك، بقيت نسخة من التسجيلات في حوزة المحققين القضائيين الذين استخدموا فيما بعد المواد المعنية في سياق تحقيق تأديبي في حق المدعي. وقضت المحكمة الأوروبية لحقوق الإنسان بأن التشريعات ذات الصلة كانت قد انتُهكت لأن المعلومات كانت قد استُخدمت لأغراض غير تلك الأغراض التي كانت قد جُمعت من أجلها، وأن المعلومات لم تُدمر في حدود الأجل القانوني. وكان التدخل في حق المدعي في احترام حياته الخاصة قد خالف القانون فيما يتعلق بالإجراءات التأديبية التي اتُّخذت في حقه.

يجب أن يقتصر نقل البيانات أو كشفها دولياً على سلطات الشرطة الأجنبية وأن يستند إلى مقتضيات قانونية خاصة، وربما اتفاقات دولية، ما لم يكن ضرورياً لغرض منع خطر جسيم ووشيك.

يجب أن تخضع معالجة البيانات من قبل الشرطة لإشراف مستقل لضمان الامتثال لقوانين حماية البيانات الوطنية. ويجب أن يتمتع أصحاب البيانات بجميع حقوق الولوج الواردة في الاتفاقية 108 المحدثة. وفي الحالة التي تكون فيها حقوق أصحاب البيانات في الولوج إليها قد تم تقييدها استناداً إلى المادة 9 من الاتفاقية 108 المحدثة، لمصلحة تحقيقات الشرطة الفعالة وتنفيذ العقوبات الجنائية، يجب أن يتمتع صاحب البيانات، بموجب القانون الوطني، بالحق في الاستئناف لدى الهيئة الوطنية المعنية بالإشراف على حماية البيانات أو هيئة مستقلة أخرى.

[739] المحكمة الأوروبية لحقوق الإنسان، كارابيوغلو ضد تركيا، القضية رقم 30083/10، 07 يونيو 2016.

### 2.1.8. اتفاقية بودابيست بشأن الجرائم السيبرانية

مع تزايد استخدام الأنشطة الإجرامية لأنظمة معالجة البيانات الإلكترونية والتأثير فيها، ظهرت الحاجة إلى مقتضيات قانونية جنائية جديدة للتصدي لذلك التحدي. واعتمد مجلس أوروبا، نتيجة لذلك، صكاً قانونياً دولياً - أي الاتفاقية بشأن الجرائم السيبرانية، المعروفة أيضاً باتفاقية بودابيست - لمعالجة مسألة الجرائم المرتكبة بوسائل الشبكات الإلكترونية وفي حقها.[740] وتُعد الاتفاقية مفتوحة لغير أعضاء مجلس أوروبا[741] للانضمام إليها. في بداية سنة 2018، كانت 14 دولة من خارج مجلس أوروبا أطرافاً في الاتفاقية وكانت سبع دول أخرى غير أعضاء في المجلس قد دُعيت إلى الانضمام إلى الاتفاقية.

تظل الاتفاقية بشأن الجرائم السيبرانية المعاهدة الدولية الأكثر تأثيراً في مجال التصدي لانتهاكات القانون على شبكة الإنترنت أو غيرها من شبكات المعلومات. وتقتضي من الأطراف تحديث قوانينها الجنائية ومواءمتها للوقاية من الاختراق وغيره من الانتهاكات الأمنية، بما في ذلك انتهاك حقوق التأليف والنشر، والاحتيال بوسيلة الحاسوب، واستغلال الأطفال في إنتاج المواد الإباحية وغيرها من الأنشطة السيبرانية غير المشروعة. وتنص الاتفاقية أيضاً على صلاحيات إجرائية تشمل تفتيش شبكات الحواسيب واعتراض الاتصالات في سياق مكافحة الجرائم الإلكترونية. وأخيراً، تمكن الاتفاقية من التعاون الدولي الفعال. ويتناول بروتوكول إضافي للاتفاقية تجريم الدعاية للعنصرية ولكراهية الأجانب في شبكات الحواسيب.

على الرغم من أن الاتفاقية ليست صكاً يهدف إلى التشجيع على حماية البيانات، إلا أنها تجرم الأنشطة التي من المرجح أن تنتهك حق صاحب البيانات في حماية بيانته. بالإضافة إلى ذلك، تقتضي الاتفاقية من الأطراف المتعاقدة اعتماد تدابير تشريعية لتمكين هيئاتها الوطنية من اعتراض حركة مرور شبكة الإنترنت وبيانات المحتوى.[742] وتلزم أيضاً الأطراف المتعاقدة، عند تنفيذ الاتفاقية، بنص حماية كافية لحقوق الإنسان والحريات، بما في ذلك الحقوق المضمونة بموجب الاتفاقية الأوروبية لحقوق الإنسان، مثل الحق في حماية البيانات.[743] ولا يُشترط على الأطراف المتعاقدة الانضمام أيضاً إلى الاتفاقية 108 حتى تستطيع الانضمام إلى اتفاقية بودابيست المتعلقة بالجرائم السيبرانية.

## 2.8. قانون حماية البيانات الأوروبي في مجال الشرطة والعدالة الجنائية

### النقاط الرئيسية

- داخل الاتحاد الأوروبي، تم تنظيم حماية البيانات في قطاع الشرطة والعدالة الجنائية في سياق معالجة البيانات الوطنية والعابرة للحدود على حد سواء من قبل سلطات الشرطة وسلطات العدالة الجنائية التابعة للدول الأعضاء والأطراف الفاعلة للاتحاد الأوروبي.
- على صعيد الدول الأعضاء، يحتاج الأمر التوجيهي الخاص بحماية البيانات والموجه إلى الشرطة وسلطات العدالة الجنائية إلى إدماجه في القانون الوطني.
- تنظم صكوك قانونية معينة حماية البيانات في قطاع الشرطة والتعاون عبر الحدود في مجال إنفاذ القانون، لا سيما في مكافحة الإرهاب والجريمة العابرة للحدود.
- توجد قواعد خاصة لحماية البيانات تتعلق بمكتب الشرطة الأوروبي (Europol)، ووكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية (Eurojust)، ومكتب المدعي العام الأوروبي الذي أنشئ حديثاً، وهي هيئات تابعة للاتحاد الأوروبي تساعد على إنفاذ القانون عبر الحدود وتشجع عليه.
- توجد أيضاً قواعد خاصة لحماية البيانات تتعلق بالأنظمة المعلوماتية المشتركة معمول بها على صعيد الاتحاد الأوروبي لتبادل المعلومات عبر الحدود بين الشرطة والهيئات القضائية المختصة، ومن بين الأمثلة الهامة الجيل الثاني من نظام شنغن للمعلومات (SIS II)، ونظام معلومات التأشيرة (VIS)، والنظام الأوروبي لمضاهاة بصمات الأصابع (Eurodac)، وهو نظام مركزي يتضمن بيانات بصمات الأصابع الخاصة بمواطني الدول الثالثة والأشخاص عديمي الجنسية الذين يلتمسون اللجوء في إحدى الدول الأعضاء في الاتحاد الأوروبي.
- إن الاتحاد الأوروبي في طور تحديث مقتضيات حماية البيانات المذكورة أعلاه حتى تتماشى مع الأمر التوجيهي الخاص بحماية البيانات والموجه إلى الشرطة وسلطات العدالة الجنائية.

---

[740] مجلس أوروبا، لجنة الوزراء (2001)، الاتفاقية المتعلقة بالجرائم السيبرانية، سلسلة معاهدات مجلس أوروبا رقم 185، بودابيست، 23 نوفمبر 2001، التي دخلت حيز النفاذ في 01 يوليو 2004.

[741] أستراليا، كندا، الشيلي، كولومبيا، جمهورية الدومينيك، إسرائيل، اليابان، الموريشيوس، بنما، السنغال، سريلانكا، طونغا، تونس والولايات المتحدة. إطلع على قائمة التوقيعات والتصديقات على المعاهدة رقم 185، حسب الوضع القائم إلى غاية يوليو 2017.

[742] مجلس أوروبا، لجنة الوزراء (2001)، الاتفاقية المتعلقة بالجرائم السيبرانية، سلسلة معاهدات مجلس أوروبا رقم 185، بودابيست، 23 نوفمبر 2001، المادتان 20 و21.

[743] نفس المرجع السابق، المادة 15 (1).

## 1.2.8. الأمر التوجيهي الخاص بحماية البيانات والموجه إلى الشرطة وسلطات العدالة الجنائية

يهدف الأمر التوجيهي EU/2016/680 المتعلق بحماية الأشخاص الذاتيين فيما يتعلق بمعالجة الهيئات المختصة للبيانات الشخصية لأغراض منع الجرائم الجنائية أو التحقيق فيها أو اكتشافها أو متابعة مرتكبيها أو تنفيذ العقوبات الجنائية، وبحرية نقل تلك البيانات (الأمر التوجيهي الخاص بحماية البيانات والموجه إلى الشرطة وسلطات العدالة الجنائية) إلى حماية البيانات الشخصية التي جُمعت وعولجت لأغراض العدالة الجنائية التي تتراوح بين:

- منع الجرائم الجنائية أو التحقيق فيها أو اكتشافها أو محاكمة مرتكبيها أو تنفيذ العقوبات الجنائية، بما في ذلك صون الأمن العام من التهديدات ومنعها؛
- وتنفيذ عقوبة جنائية؛
- وفي الحالات التي تتصرف فيها هيئات الشرطة وغيرها من سلطات إنفاذ القانون لاحترام القانون وصون الأمن العام والحقوق الأساسية للمجتمع من التهديدات التي قد تشكل جرائم جنائية ومنعها.

يحمي الأمر التوجيهي الخاص بحماية البيانات والموجه إلى الشرطة وسلطات العدالة الجنائية مختلف فئات البيانات الشخصية الخاصة بالأفراد المعنيين بالدعاوى الجنائية، مثل الشهود، والمخبرين، والضحايا، والمشتبه فيهم، والشركاء في الجرائم. وتلتزم الشرطة وسلطات العدالة الجنائية بالامتثال لمقتضيات الأمر التوجيهي كلما عالجت تلك البيانات الشخصية لأغراض إنفاذ القانون، ضمن نطاقي الأمر التوجيهي الشخصي والمادي.[745]

ومع ذلك، يُسمح أيضاً باستخدام البيانات لغرض مختلف في ظروف معينة. ولا يُسمح بمعالجة البيانات لغرض آخر من أغراض إنفاذ القانون غير ذلك الذي جُمعت من أجله إلا إذا كان ذلك مشروعاً وضرورياً ومتناسباً استناداً إلى القانون الوطني أو قانون الاتحاد الأوروبي.[746] فيما يخص الأغراض الأخرى، تُطبق قواعد اللائحة العامة لحماية البيانات. ويُعد حفظ السجلات عن عمليات مشاركة البيانات وتوثيقها من بين الواجبات المحددة للسلطات المختصة للمساعدة على توضيح المسؤوليات الناشئة عن الشكاوى.

تُعد السلطات المختصة العاملة في مجال الشرطة والعدالة الجنائية سلطات عامة، أو سلطات يخولها القانون الوطني أو السلطات العامة لأداء وظائف سلطة عامة،[747] مثل تفويض تسيير السجون إلى جهات خاصة.[748] ويشمل تطبيق الأمر التوجيهي معالجة البيانات سواء على الصعيد الوطني وعبر الحدود بين هيئات الشرطة والسلطات القضائية التابعة للدول الأعضاء، كما يشمل عمليات نقل البيانات دولياً من قبل السلطات المختصة إلى دول ثالثة ومنظمات دولية.[749] ولا يشمل الأمر التوجيهي الأمن الوطني أو معالجة مؤسسات الاتحاد الأوروبي وهيئاته ومكاتبه ووكالاته البيانات الشخصية.[750]

يعتمد الأمر التوجيهي، بقدر كبير، على المبادئ والتعاريف الواردة في اللائحة العامة لحماية البيانات، مراعياً الطبيعة الخاصة لمجالي الشرطة والعدالة الجنائية. وقد يُنفذ الإشراف من قبل نفس هيئات الدول الأعضاء التي تمارس الإشراف أيضاً بموجب اللائحة العامة لحماية البيانات. وقد أُدرج في الأمر التوجيهي تعيين مسؤولين عن حماية البيانات وتنفيذ تقييمات الأثر على حماية البيانات بصفتهما التزامات جديدة تهم هيئات الشرطة وسلطات العدالة الجنائية.[751] وعلى الرغم من أن تلك المبادئ استُوحيت من اللائحة العامة لحماية البيانات، إلا أن الأمر

---

[744] الأمر التوجيهي EU/2016/680 الصادر عن البرلمان الأوروبي وعن المجلس في 27 أبريل 2016 والمتعلق بحماية الأشخاص الذاتيين فيما يتعلق بمعالجة الهيئات المختصة للبيانات الشخصية لأغراض منع الجرائم الجنائية والتحقيق فيها واكتشافها ومحاكمة مرتكبيها أو تنفيذ العقوبات الجنائية، وبحرية حركة تلك البيانات، والذي يلغي قرار المجلس الإطاري JHA/2008/977، الجريدة الرسمية L 119 2016 OJ، ص. 89 (الأمر التوجيهي الخاص بحماية البيانات والموجه إلى الشرطة وسلطات العدالة الجنائية).

[745] الأمر التوجيهي الخاص بحماية البيانات والموجه إلى الشرطة وسلطات العدالة الجنائية، المادة 2 (1).

[746] نفس المرجع السابق، المادة 4 (2).

[747] نفس المرجع السابق، المادة 3 (7).

[748] المفوضية الأوروبية (2016)، بلاغ صادر عن المفوضية وموجه إلى البرلمان الأوروبي وفقاً للمادة 294 (6) من المعاهدة المنظمة لعمل الاتحاد الأوروبي يتعلق بموقف المجلس بشأن اعتماد أمر توجيهي صادر عن البرلمان الأوروبي والمجلس بشأن حماية الأفراد فيما يتعلق بمعالجة الهيئات المختصة للبيانات الشخصية لأغراض منع الجرائم الجنائية والتحقيق فيها واكتشافها ومحاكمة مرتكبيها أو تنفيذ العقوبات الجنائية، وبشأن حرية حركة تلك البيانات، والذي يلغي قرار مجلس أوروبا الإطاري JHA/2008/977، النسخة النهائية(2016) COM 2013 ، بروكسيل، 11 أبريل 2016.

[749] الأمر التوجيهي الخاص بحماية البيانات والموجه إلى الشرطة وسلطات العدالة الجنائية، الفصل 5.

[750] نفس المرجع السابق، المادة 2 (3).

[751] نفس المرجع السابق، المادتان 32 و27 على التوالي.

التوجيهي يتطرق إلى الطبيعة الخاصة لهيئات الشرطة وسلطات العدالة الجنائية. ومقارنة بمعالجة البيانات لأغراض تجارية، والتي تنظمها اللائحة، قد تتطلب معالجة البيانات المرتبطة بالأمن مستوىً معيناً من المرونة. على سبيل المثال، قد يعني تزويد أصحاب البيانات بنفس المستوى من الحماية فيما يتعلق بحقوقهم في المعلومات، والولوج إلى البيانات الشخصية أو حذفها كما هو الشأن بموجب اللائحة العامة لحماية البيانات أن أي عملية مراقبة تُنفذ لأغراض إنفاذ القانون ستصبح غير فعالة في سياق إنفاذ القانون. ونتيجة لذلك، لا يتضمن الأمر التوجيهي مبدأ الشفافية. على نحو مماثل، يحتاج أيضاً كل من مبدأ تقليل البيانات إلى الحد الأدنى ومبدأ حصر الغرض، اللذان يقتضيان حصر البيانات الشخصية فيما يكون ضرورياً فحسب فيما يخص الأغراض التي تُعالج من أجلها، ومعالجتها لتحقيق أهداف معينة وصريحة، إلى تطبيقهما تطبيقاً مرناً في المعالجة المرتبطة بالأمن. وقد تثبت المعلومات التي جمعتها السلطات المختصة وخزنتها في حالة معينة أهميتها البالغة في حل القضايا مستقبلاً.

**مبادئ متعلقة بالمعالجة**

يحدد الأمر التوجيهي الخاص بحماية البيانات والموجه إلى الشرطة وسلطات العدالة الجنائية بعضاً من الضمانات الرئيسية التي تتعلق باستخدام البيانات الشخصية، ويوضح المبادئ التي ترشد معالجة تلك البيانات. وتحتاج الدول الأعضاء إلى أن تضمن أن البيانات الشخصية:

- تُعالج معالجة مشروعة وعادلة؛
- تُجمع لأغراض معينة وصريحة وشرعية ولا تُعالج بما يخالف تلك الأغراض؛
- ملاءمة وذات صلة بالموضوع وغير مفرطة فيما يتعلق بالأغراض التي تُعالج من أجلها؛
- صحيحة و،عند الضرورة، محدثة ؛ ويجب اتخاذ الخطوات المعقولة لضمان محو وتصحيح البيانات الشخصية الخاطئة، فيما يتعلق بالأغراض التي تُعالج من أجلها، دون تأخير؛
- يُحتفظ بها في شكل يسمح بتحديد هوية أصحاب البيانات لمدة لا تتجاوز ما هو ضروري للأغراض التي تُعالج من أجلها؛
- تُعالج بما يضمن الأمن اللائق بالبيانات الشخصية، بما في ذلك الوقاية من المعالجة غير المرخصة وغير المشروعة ومن الضياع أو الدمار أو التلف العرضي، باستخدام التدابير التقنية والتنظيمية المناسبة.[752]

بموجب الأمر التوجيهي، لا تكون المعالجة مشروعة إلا عندما تحدث بالقدر الضروري لأداء المهمة المعنية. علاوة على ذلك، ينبغي أن تنجز المعالجة من قبل الهيئة المختصة تحقيقاً للأهداف المحددة في الأمر التوجيهي وأن تستند إلى قانون الاتحاد الأوروبي أو القانون الوطني. ولا يجب الاحتفاظ بالبيانات لمدة أطول مما يكون ضرورياً ويجب محوها أو مراجعتها دورياً داخل آجال معينة. ولا يجب استخدام البيانات إلا من قبل السلطة المختصة وللغرض الذي بسببه جُمعت أو أُرسلت أو أُتيحت.

**حقوق صاحب البيانات**

يحدد الأمر التوجيهي أيضاً حقوق صاحب البيانات، والتي تشمل ما يلي:

• الحق في تلقي المعلومات. يجب على الدول الأعضاء أن تلزم مراقب البيانات بتزويد صاحب البيانات بما يلي: 1) هوية المراقب وبيانات الاتصال الخاصة به، و2) بيانات الاتصال الخاصة بالمسؤول عن حماية البيانات، و3) أغراض المعالجة المقررة، و4) الحق في تقديم شكوى إلى الهيئة الإشرافية وفي الحصول على بيانات الاتصال الخاصة بها، و5) الحق في الولوج إلى البيانات الشخصية أو تصحيحها أو محوها وتقييد معالجتها.[754] بالإضافة إلى تلك المتطلبات من المعلومات، ينص الأمر التوجيهي على أنه، في حالات بعينها، ولتمكينهم من ممارسة حقوقهم، يجب على المراقبين تزويد أصحاب البيانات بمعلومات بشأن الأساس القانوني للمعالجة وبشأن مدة التخزين، إذا تعين إرسال البيانات الشخصية إلى متلقين آخرين، بما في ذلك إلى دول ثالثة أو منظمات دولية ، يجب إخبار أصحاب البيانات بفئات هؤلاء المتلقين. وأخيراً، يجب على المراقبين إتاحة أي معلومات إضافية، مع مراعاة الظروف الخاصة التي تُعالج فيها البيانات - على سبيل المثال، عندما تُجمع البيانات الشخصية خلال المراقبة السرية، أي دون علم صاحب بالبيانات، ويضمن ذلك معالجة عادلة فيما يتعلق بصاحب البيانات.[755]

[752] نفس المرجع السابق، المادة 4 (1).
[753] نفس المرجع السابق، المادة 8.
[754] نفس المرجع السابق، المادة 13 (1).
[755] نفس المرجع السابق، المادة 13 (2).

• الحق في الولوج إلى البيانات الشخصية. يجب على الدول الأعضاء أن تضمن تمتع صاحب البيانات بالحق في معرفة ما إذا كانت بياناته الشخصية قيد المعالجة أم لا. فإذا كانت قيد المعالجة، ينبغي لصاحب البيانات الولوج إلى معلومات معينة، مثل فئات البيانات الشخصية قيد المعالجة.[756] إلا أن ذلك قد يتم تقييده - على سبيل المثال، لمنع عرقلة التحقيق أو الإضرار بمحاكمة مرتكبي الجرائم، أو لحماية الأمن العام وحقوق الآخرين وحرياتهم.[757]

• الحق في تصحيح البيانات الشخصية. تلتزم الدول الأعضاء بأن تضمن أن صاحب البيانات يمكن له، دون تأخير لا مبرر له، الحصول على تصحيح البيانات الشخصية الخاطئة. علاوة على ذلك، يتمتع صاحب البيانات أيضاً بالحق في استكمال البيانات الشخصية الناقصة.[758]

• الحق في محو البيانات الشخصية وتقييد المعالجة. في حالات معينة، يحتاج المراقب إلى محو البيانات الشخصية. بالإضافة إلى ذلك، قد يضمن صاحب البيانات محو بياناته الشخصية، لكن فقط عندما تكون قيد المعالجة غير المشروعة.[759] في حالات معينة، قد تُقيد معالجة البيانات الشخصية بدلا عن محوها، ويمكن أن يحدث ذلك في الحالات التالية: 1) عندما يُعترض على صحة البيانات دون القدرة على إثبات ذلك، و2) عندما تكون هناك حاجة إلى البيانات الشخصية لغرض الأدلة.[760]

كلما رفض المراقب تصحيح البيانات الشخصية أو محوها، أو تقييد معالجة البيانات، يجب إخبار صاحب البيانات بذلك كتابياً. وقد تقيد الدول الأعضاء الحق في المعلومات لحماية الأمن العام وحقوق الآخرين وحرياتهم، من بين أشياء أخرى، لنفس الأسباب التي استدعت تقييد الحق في الولوج.[761]

يحق لصاحب البيانات عادة أن يحصل على معلومات عن معالجة بياناته الشخصية، كما يحق له الولوج إلى بياناته ، أو تصحيحها، أو محوها، أو تقييد المعالجة وهي الحقوق التي يمارسها مباشرة بالاشتراك مع المراقب. وكخيار بديل، يمكن أيضاً لأصحاب البيانات أن يمارسوا حقوقهم بطريقة غير مباشرة، من خلال الهيئة الإشرافية المكلفة بحماية بياناتهم، بموجب الأمر التوجيهي الخاص بحماية البيانات والموجه إلى الشرطة وسلطات العدالة الجنائية، الذي يدخل حيز النفاذ عندما يقيد المراقب حق صاحب البيانات.[762] تقتضي المادة 17 من الأمر التوجيهي من الدول الأعضاء اعتماد تدابير تضمن إمكانية ممارسة أصحاب البيانات حقوقهم من خلال الهيئة الإشرافية المكلفة بحماية بياناتهم. وذلك ما يوجب على مراقب البيانات إخبار صاحب البيانات بإمكانية الولوج غير المباشر.

**التزامات المراقب والمعالج**

في سياق الأمر التوجيهي الخاص بحماية البيانات والموجه إلى الشرطة وسلطات العدالة الجنائية، يُعد المراقبون هيئات عامة مختصة، أو هيئات أخرى لها سلطات عامة أو صلاحيات العامة ذات صلة، تحدد أغراض معالجة البيانات الشخصية ووسائلها. ويضع الأمر التوجيهي عدة التزامات فيما يخص مراقبي البيانات لضمان مستوى عال من الحماية للبيانات الشخصية لأغراض إنفاذ القانون.

يجب على الهيئات المختصة الاحتفاظ بسجلات لعمليات المعالجة التي تنجزها في أنظمة المعالجة الآلية. ويجب الاحتفاظ بالسجلات على الأقل لأغراض جمع البيانات الشخصية، وتعديلها، والاطلاع عليها، والكشف عنها بما في ذلك عمليات نقلها أو دمجها أو محوها.[763] وينص الأمر التوجيهي على أن سجلات الاطلاع والكشف يجب أن تمكن من تحديد تاريخ العمليات ووقتها، وتبريرها، وبقدر المستطاع، هوية الشخص الذي اطلع على النظام أو كشف عن البيانات الشخصية، ومتلقي البيانات الشخصية المعنيين. ولا يجب أن تُستخدم السجلات إلا بهدف التحقق من مشروعية المعالجة، والمراقبة الذاتية، وضمان سلامة البيانات الشخصية وأمنها، ولغرض الدعاوى الجنائية.[764] بناءً على طلب الهيئة الإشرافية، يجب على المراقب والمعالج إتاحة السجلات لها.

[756] نفس المرجع السابق، المادة 14.
[757] نفس المرجع السابق، المادة 15.
[758] نفس المرجع السابق، المادة 16 (1).
[759] نفس المرجع السابق، المادة 16 (2).
[760] نفس المرجع السابق، المادة 16 (3).
[761] نفس المرجع السابق، المادة 16 (4).
[762] نفس المرجع السابق، المادة 17.
[763] نفس المرجع السابق، المادة 25 (1).
[764] نفس المرجع السابق، المادة 25 (2).

على وجه الخصوص، ثمة التزام عام من جانب المراقبين بتنفيذ التدابير التقنية والتنظيمية المناسبة لضمان القيام بالمعالجة وفقاً للأمر التوجيهي، وللتمكن من إثبات مشروعية تلك المعالجة.[765] عند تصميم تلك التدابير، يحتاج المراقبون إلى مراعاة طبيعة المعالجة، ونطاقها، وسياقها، والأهم من ذلك، أي أخطار يحتمل أن تطال حقوق الأفراد وحرياتهم. وينبغي للمراقبين اعتماد سياسات داخلية وتنفيذ تدابير تيسر الامتثال لمبادئ حماية البيانات، لا سيما مبدأ حماية البيانات منذ التصميم وتلقائياً.[766] عندما يُحتمل أن تفضي المعالجة إلى حدوث خطر كبير على حقوق الأفراد - بسبب استخدام التكنولوجيات الجديدة، مثلاً، يجب على المراقبين إجراء تقييم الأثر على حماية البيانات قبل الشروع في المعالجة.[767] ويعدد الأمر التوجيهي أيضاً التدابير التي يجب على المراقبين تنفيذها لضمان أمن المعالجة، وتتضمن تلك التدابير منع الولوج غير المرخص إلى البيانات الشخصية التي يعالجونها لضمان أن الأشخاص المرخصين لا يلجون إلا إلى البيانات الشخصية التي يشملها ترخيص الولوج الخاص بهم، وأن نظام المعالجة يؤدي وظائفه أداءً سليماً، وأن البيانات الشخصية المخزنة لا يمكن إفسادها عن طريق خلل في النظام.[768] إذا حدث خرق للبيانات الشخصية فعلاً، فحينها يجب على المراقبين إخبار الهيئة الإشرافية في غضون ثلاثة أيام، مع وصف طبيعة الخرق، وعواقبه المحتملة، وفئات البيانات الشخصية المعنية والعدد التقريبي لأصحاب البيانات المتضررين. ويجب إبلاغ صاحب البيانات بخرق البيانات الشخصية «دون تأخير لا موجب له» عندما يُحتمل أن يفضي الخرق إلى خطر كبير على حقوقه وحرياته.[769]

يتضمن الأمر التوجيهي مبدأ المساءلة الذي يفرض واجباً على المراقبين لتنفيذ تدابير تضمن الامتثال لذلك المبدأ. ويجب على المراقبين الاحتفاظ بسجلات لجميع فئات أنشطة المعالجة في نطاق مسؤوليتهم: تم تحديد المحتوى المفصل لتلك السجلات في المادة 24 من الأمر التوجيهي. وتجب إتاحة السجلات للهيئة الإشرافية بناءً على طلبها حتى تتمكن من مراقبة عمليات المعالجة التي يقوم بها المراقب. ومن بين التدابير الهامة الأخرى لتعزيز المساءلة تعيين مسؤول عن حماية البيانات (DPO). يجب على المراقبين تعيين مسؤول عن حماية البيانات، على الرغم من أن الأمر التوجيهي يسمح للدول الأعضاء بأن تعفي من ذلك الالتزام المحاكم وغيرها من السلطات القضائية المستقلة.[770] وتشبه واجبات المسؤول عن حماية البيانات الواجبات الواردة في اللائحة العامة لحماية البيانات. ويراقب المسؤول الامتثال للأمر التوجيهي، ويقدم المعلومات ذات الصلة كما يزود الموظفين القائمين على معالجة البيانات بالمشورة اللازمة بشأن التزاماتهم بموجب التشريعات المتعلقة بحماية البيانات. ويسدي المسؤول عن حماية البيانات أيضاً المشورة بشأن الحاجة إلى إجراء تقييم الأثر على حماية البيانات ويتصرف بصفته جهة الاتصال الخاصة بالهيئة الإشرافية.

**عمليات نقل البيانات إلى البلدان الثالثة أو المنظمات الدولية**

على غرار اللائحة العامة لحماية البيانات، يحدد الأمر التوجيهي شروط نقل البيانات الشخصية إلى البلدان الثالثة أو المنظمات الدولية. إذا نُقلت البيانات الشخصية بحرية خارج نطاق الولاية القضائية للاتحاد الأوروبي، فإن ذلك من شأنه أن يقوض الضمانات والحماية القوية التي ينص عليها قانون الاتحاد الأوروبي. ومع ذلك، فإن الشروط تختلف تماماً عن الشروط الواردة في اللائحة العامة لحماية البيانات. ولا يُسمح بنقل البيانات الشخصية إلى البلدان الثالثة أو المنظمات الدولية إلا في الحالات التالية:[771]

- إذا كان النقل ضرورياً لتحقيق أهداف الأمر التوجيهي؛
- إذا تم نقل البيانات الشخصية إلى سلطة مختصة، ضمن مفهوم الأمر التوجيهي، تابعة للبلد الثالث أو منظمة دولية- على الرغم من وجود استثناء من هذه القاعدة في حالات فردية ومعينة؛[772]
- وإذا كان نقل بيانات شخصية تم تلقيها في سياق التعاون عبر الحدود إلى البلدان الثالثة أو المنظمات الدولية حصل على ترخيص الدولة العضو التي أتت منها البيانات، على الرغم من وجود إعفاءات في حالات طارئة؛
- وإذا كانت المفوضية الأوروبية قد اعتمدت قراراً حول مدى كفاية الضمانات المرتبطة بحماية البيانات (قرار الكفاية اختصاراً)، وتم وضع الضمانات المناسبة، أو يُطبق الاستثناء لعمليات النقل في حالات معينة؛

[765] نفس المرجع السابق، المادة 19.
[766] نفس المرجع السابق، المادة 20.
[767] نفس المرجع السابق، المادة 27.
[768] نفس المرجع السابق، المادة 29.
[769] نفس المرجع السابق، المادتان 30 و31.
[770] نفس المرجع السابق، المادة 32.
[771] نفس المرجع السابق، المادة 35.
[772] نفس المرجع السابق، المادة 39.

• عمليات النقل اللاحقة للبيانات الشخصية إلى بلد آخر ثالث أو منظمة دولية تتطلب ترخيصاً مسبقاً من السلطة المختصة في البلد الذي أتت منه البيانات، والتي ستراعي، من بين أمور أخرى، خطورة الجريمة ومستوى حماية البيانات في بلد الوجهة حيث سيتم النقل الدولي الثاني.[773]

وبموجب الأمر التوجيهي، قد تحدث عمليات نقل البيانات إذا تم استيفاء أحد الشروط الثلاثة التالية: أولها هو عندما تصدر المفوضية الأوروبية قرار الكفاية بموجب الأمر التوجيهي. يمكن للقرار أن يُطبق على أراضي البلد الثالث بأكملها، أو في قطاعات معينة من البلد الثالث أو المنظمة الدولية. ومع ذلك، لا يمكن القيام بذلك إلا إذا تم ضمان مستوى ملائم من الحماية واستيفاء الشروط المحددة في الأمر التوجيهي.[774] في تلك الحالات، لا يكون نقل البيانات الشخصية خاضعاً لترخيص الدولة العضو.[775] ويتعين على المفوضية الأوروبية مراقبة التطورات التي من شأنها أن تمس بأداء قرارات الكفاية. علاوة على ذلك، يجب أن يشتمل القرار على آلية لفرض المراجعة الدورية. ويجوز أيضاً للمفوضية أن تلغي قراراً أو تعدله أو تعلقه عندما تظهر المعلومات المتاحة أن الشروط ذات الصلة في البلد الثالث أو المنظمة الدولية لم تعد تضمن مستوىً ملائماً من الحماية. إذا كان الأمر كذلك، يتعين على المفوضية الدخول في مشاورات مع البلد الثالث أو المنظمة الدولية ، ساعية إلى تصحيح ذلك الوضع.

في حال انعدام قرار الكفاية، يمكن لعمليات النقل أن تستند إلى الضمانات المناسبة. فإما أن يتم التنصيص على تلك الضمانات في صك ملزم قانوناً وإما أن ينجز المراقب تقييماً ذاتياً للظروف المحيطة بنقل البيانات الشخصية ويستنتج وجود الضمانات المناسبة. ويجب أن يراعي التقييم الذاتي إمكانية إبرام اتفاقات تعاون بين اليوروبول أو وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية والبلد الثالث أو المنظمة الدولية ، ووجود التزامات بالسرية وحصر الغرض بالإضافة إلى الضمانات بأن البيانات لن تُستخدم لأي شكل من أشكال المعاملة القاسية و اللاإنسانية ، بما في ذلك عقوبة الإعدام.[776] في هذه الحالة، يحتاج المراقب إلى إخبار الهيئة الإشرافية المختصة بفئات عمليات النقل التي تشملها هذه الفئة.[777]

في حال لم يتم اعتماد أي قرار كفاية ولم يتم استحداث ضمانات مناسبة، تظل عمليات النقل مسموحاً بها في حالات معينة واردة في الأمر التوجيهي. وتشمل تلك الحالات، من بين أمور أخرى ، حماية المصالح الحيوية لصاحب البيانات أو شخص آخر ومنع تهديد خطير ووشيك يتعلق بالأمن العام للدولة العضو أو البلد الثالث.[778]

في حالات فردية ومعينة، قد تنفذ السلطات المختصة عمليات النقل إلى متلقين موجودين في بلدان ثالثة ليسوا بسلطات مختصة، إذا استُوفيت الشروط الإضافية المنصوص عليها في المادة 39 من الأمر التوجيهي، فضلاً عن استيفاء أحد الشروط الثلاثة الموصوفة سلفاً. على وجه الخصوص، يجب أن يكون النقل جد ضروري لأداء السلطة المختصة الناقلة لمهمة ما، وهي المسؤولة أيضاً عن البت في عدم وجود حقوق أو حريات أساسية للأفراد تغلب على المصلحة العامة التي تبرر ذلك النقل. وتحتاج عمليات النقل تلك إلى توثيقها ويتعين على السلطة المختصة الناقلة إخبار الهيئة الإشرافية المختصة.[779]

أخيراً، فيما يتعلق بالبلدان الثالثة والمنظمات الدولية ، يقتضي الأمر التوجيهي أيضاً وضع آليات للتعاون الدولي لتيسير التنفيذ الفعال للتشريعات، وبذلك يساعد الهيئات الإشرافية المكلفة بحماية البيانات على التعاون مع نظيراتها الأجنبية.[780]

---

[773] نفس المرجع السابق، المادة 35 (1).
[774] نفس المرجع السابق، المادة 36.
[775] نفس المرجع السابق، المادة 36 (1).
[776] نفس المرجع السابق، الحيثية 71.
[777] نفس المرجع السابق، المادة 37 (1).
[778] نفس المرجع السابق، المادة 38 (1).
[779] نفس المرجع السابق، المادة 37 (3).
[780] نفس المرجع السابق، المادة 40.

**الإشراف المستقل وسبل الانتصاف فيما يخص أصحاب البيانات**

يجب على كل دولة عضو أن تضمن أن هيئة إشرافية وطنية مستقلة واحدة أو أكثر تتحمل مسؤولية إسداء المشورة بشأن تطبيق المقتضيات المعتمدة ومراقبة تطبيقها وفقاً للأمر التوجيهي.[781] وقد تكون الهيئة الإشرافية التي أُسست لغرض الأمر التوجيهي هي نفسها الهيئة الإشرافية التي أُسست بموجب اللائحة العامة لحماية البيانات، لكن الدول الأعضاء لها الحرية في تعيين هيئة مختلفة، شريطة أن تفي بمعايير الاستقلالية. وتنظر الهيئات الإشرافية أيضاً في الادعاءات التي يقدمها أي شخص والتي تخص حماية حقوقه أو حرياته فيما يتعلق بمعالجة الهيئات المختصة للبيانات الشخصية.

عندما يتم رفض ممارسة صاحب البيانات لحقوقه لأسباب قاهرة ، يجب تمتيع صاحب البيانات بحق الاستئناف لدى الهيئة الإشرافية الوطنية المختصة و/أو لدى المحكمة. إذا تكبد شخص ضرراً بسبب انتهاك للقانون الوطني الذي ينفذ الأمر التوجيهي، يحق له الحصول على تعويض من قبل المراقب أو أي سلطة مختصة أخرى بموجب قانون الدولة العضو.[782] عموماً، يجب أن يحصل أصحاب البيانات على سبل الانتصاف القضائية عن أي انتهاك لحقوقهم المكفولة بموجب القانون الوطني الذي ينفذ الأمر التوجيهي.[783]

## 3.8. صكوك قانونية محددة أخرى بشأن حماية البيانات في قضايا إنفاذ القانون

بالإضافة إلى الأمر التوجيهي الخاص بحماية البيانات والموجه إلى الشرطة وسلطات العدالة الجنائية، ينظم عدد من الصكوك القانونية تبادل المعلومات التي بحوزة الدول الأعضاء في مجالات معينة - مثل قرار المجلس الأوروبي الإطاري JHA/2009/315 بشأن تنظيم ومضامين تبادل المعلومات المستخلصة من السجل الجنائي بين الدول الأعضاء، وقرار المجلس رقم JHA/2000/642 المتعلق بترتيبات التعاون بين وحدات الاستخبارات المالية التابعة للدول الأعضاء فيما يتعلق بتبادل المعلومات، وقرار المجلس الأوروبي الإطاري رقم 2006/960/ JHA الصادر في 18 ديسمبر 2006 بشأن تبسيط تبادل المعلومات والاستخبارات بين هيئات إنفاذ القانون التابعة للدول الأعضاء في الاتحاد الأوروبي.[784]

والأهم من ذلك هو أن التعاون عبر الحدود[785] بين الهيئات المختصة ينطوي بصورة متزايدة على تبادل بيانات الهجرة. ولا يعد ذلك المجال من القانون جزءاً من قضايا الشرطة والعدالة الجنائية لكنه يتصل في كثير من الجوانب بعمل هيئات الشرطة والسلطات القضائية. ويصدق الأمر نفسه فيما يخص السلع التي يصدرها الاتحاد الأوروبي أو يستوردها. وأدى إلغاء مراقبة الحدود داخل منطقة شنغن إلى تعاظم خطر الاحتيال، ما حتم على الدول الأعضاء تكثيف التعاون، لا سيما بتعزيز تبادل المعلومات عبر الحدود، لاكتشاف الأشخاص المنتهكين لقانون الجمارك الوطني وقانون الجمارك الأوروبي ومحاكمتهم بفعالية أكثر. بالإضافة إلى ذلك، عرف العالم في السنوات الأخيرة ارتفاعاً في الجريمة المنظمة والخطيرة والإرهاب، ما بإمكانه أن يشمل السفر على الصعيد الدولي وأبرز الحاجة إلى زيادة التعاون عبر الحدود بين هيئات الشرطة وسلطات إنفاذ القانون في حالات كثيرة.[786]

**قرار «برووم» (Prüm)**

يُعد قرار المجلس الأوروبي رقم JHA/2008/615 مثالاً هاماً عن التعاون عبر الحدود المؤسسي من خلال تبادل المعلومات التي يُحتفظ بها على الصعيد الوطني، إلى جانب المقتضيات التي تنفذه الواردة في القرار رقم JHA/2008/615 بشأن زيادة التعاون عبر الحدود، لا سيما في

[781] نفس المرجع السابق، المادة 41.

[782] نفس المرجع السابق، المادة 56.

[783] نفس المرجع السابق، المادة 54.

[784] مجلس الاتحاد الأوروبي (2009)، قرار المجلس الإطاري رقم JHA/2009/315 الصادر في 26 فبراير 2009 بشأن تنظيم ومضامين تبادل المعلومات المستخلصة من السجل الجنائي بين الدول الأعضاء، الجريدة الرسمية L 93 2009 OJ؛ مجلس الاتحاد الأوروبي (2000)، قرار المجلس رقم JHA/2000/642 الصادر في 17 أكتوبر 2000 والمتعلق بترتيبات التعاون بين وحدات الاستخبارات المالية التابعة للدول الأعضاء فيما يتعلق بتبادل المعلومات، الجريدة الرسمية L 271 2000 OJ؛ قرار المجلس الإطاري رقم JHA/2006/960 الصادر في 18 ديسمبر 2006 بشأن تبسيط تبادل المعلومات والاستخبارات بين هيئات إنفاذ القانون التابعة للدول الأعضاء في الاتحاد الأوروبي، الجريدة الرسمية L 386 OJ.

[785] المفوضية الأوروبية (2012)، بلاغ صادر عن المفوضية وموجه إلى البرلمان الأوروبي والمجلس- تعزيز التعاون في مجال إنفاذ القانون في الاتحاد الأوروبي: نموذج تبادل المعلومات الأوروبي (EIXM)، النسخة النهائية735 (2012)COM ، بروكسيل، 07 ديسمبر 2012.

[786] إطلع على المفوضية الأوروبية (2011)، مقترح بأمر توجيهي عن البرلمان الأوروبي والمجلس بشأن استخدام بيانات سجلات أسماء الركاب لمنع الجرائم الإرهابية والجريمة الخطيرة واكتشافها والتحقيق فيها ومحاكمة مرتكبيها، النسخة النهائية32 (2011)COM ، بروكسيل، 02 فبراير 2011، ص. 1.

مجالي مكافحة الإرهاب والجريمة عبر الحدود (قرار «بروم»)، والذي أدمج معاهدة بروم في قانون الاتحاد الأوروبي سنة 2008.[787] وكانت معاهدة بروم اتفاقاً للتعاون الدولي بين هيئات الشرطة وُقعت سنة 2005 من قبل النمسا وبلجيكا وفرنسا وألمانيا ولوكسمبورغ وهولندا وإسبانيا.[788]

يهدف قرار بروم إلى مساعدة الدول الأعضاء الموقعة على المعاهدة على تحسين تبادل المعلومات لغرض منع الجرائم ومكافحتها في ثلاثة ميادين، وهي: الإرهاب والجريمة عبر الحدود والهجرة غير الشرعية. لذلك الغرض، يحدد القرار مقتضيات تتعلق بما يلي:

- الولوج الآلي إلى ملفات الحمض النووي ، وبيانات بصمات الأصابع، وبعض البيانات المتعلقة بتسجيل السيارات على الصعيد الوطني؛
- التزويد بالبيانات فيما يتعلق بالأحداث الرئيسية التي لها امتداد عبر الحدود؛
- التزويد بالمعلومات لمنع الجرائم الإرهابية؛
- تدابير أخرى لزيادة تعاون هيئات الشرطة عبر الحدود.

ينظم القانون الوطني كلياً قواعد البيانات المتاحة بموجب قرار بروم، لكن تبادل البيانات يُنظم بالإضافة إلى ذلك من طرف ذلك القرار، والذي يجب تقييم توافقه مع الأمر التوجيهي الخاص بحماية البيانات والموجه إلى الشرطة وسلطات العدالة الجنائية. وتُعد الهيئات المختصة بالإشراف على تدفقات تلك البيانات الهيئات الإشرافية الوطنية المعنية بحماية البيانات.

**القرار الإطاري رقم JHA/2006/960 - المبادرة السويدية**

يمثل القرار الإطاري رقم JHA/2006/960 (المبادرة السويدية)[789] مثالاً آخراً عن التعاون عبر الحدود فيما يخص تبادل البيانات التي تحتفظ بها سلطات إنفاذ القانون على الصعيد الوطني. وتركز المبادرة خصوصاً على تبادل الاستخبارات والمعلومات وتنص على قواعد معينة لحماية البيانات في المادة 8.

وفقاً لذلك الصك، يجب أن تخضع المعلومات والاستخبارات المتبادلة لمقتضيات حماية البيانات الوطنية المطبقة في الدولة العضو المتلقية للمعلومات، وفقاً لنفس القواعد كما لو جُمعت في تلك الدولة العضو. وتذهب المادة 8 إلى أبعد من ذلك بالنص على أنه عند التزويد بالمعلومات والاستخبارات، يجوز لسلطة إنفاذ القانون المختصة فرض شروط تتوافق مع قانونها الوطني عند استخدامها من قبل سلطة إنفاذ القانون المختصة المتلقية لها. وقد تُطبق تلك الشروط أيضاً على الإبلاغ عن نتيجة التحقيق الجنائي أو على عمليات الاستخبارات الجنائية التي اقتضت تبادل تلك المعلومات والاستخبارات. ومع ذلك، حينما ينص القانون الوطني على استثناءات من القيود المفروضة على الاستخدام، (فيما يخص السلطات القضائية، والهيئات التشريعية، وغيرها) لا يجوز استخدام المعلومات والاستخبارات إلا بعد التشاور المسبق مع الدولة العضو المرسلة.

يجوز استخدام المعلومات والاستخبارات في:

- الأغراض التي استدعت تزويدها؛
- منع تهديد وشيك وخطير على الأمن العام.

لا يُسمح بالمعالجة لأغراض أخرى إلا بناءً على ترخيص مسبق من الدولة العضو المرسلة.

---

[787] مجلس الاتحاد الأوروبي (2008)، قرار المجلس رقم JHA/2008/615 الصادر في 23 يونيو 2008 بشأن زيادة التعاون عبر الحدود، لا سيما في مجالي مكافحة الإرهاب والجريمة عبر الحدود، الجريدة الرسمية 210 L 2008 OJ.

[788] الاتفاقية المبرمة بين مملكة بلجيكا وجمهورية ألمانيا الاتحادية ومملكة إسبانيا وجمهورية فرنسا ودوقية لوكسمبورغ الكبرى ومملكة هولندا وجمهورية النمسا بشأن زيادة التعاون عبر الحدود، لا سيما في مجالات مكافحة الإرهاب والجريمة عبر الحدود والهجرة غير الشرعية.

[789] مجلس الاتحاد الأوروبي (2006)، قرار المجلس الإطاري رقم JHA/2006/960 الصادر في 18 ديسمبر 2006 بشأن تبسيط تبادل المعلومات والاستخبارات بين سلطات إنفاذ القانون التابعة للدول الأعضاء في الاتحاد الأوروبي، الجريدة الرسمية 386/89 L OJ الصادرة في 29 ديسمبر 2006.

وتنص المبادرة السويدية أيضاً على وجوب حماية البيانات الشخصية المعالجة وفقاً للصكوك الدولية مثل:

- اتفاقية مجلس أوروبا لحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية؛[790]
- البروتوكول الإضافي الملحق بتلك الاتفاقية الصادر في 8 نونبر 2001 والمتعلق بالهيئات الإشرافية وتدفقات البيانات عبر الحدود؛[791]
- التوصية رقم R(87) 15 الصادرة عن مجلس أوروبا والمنظمة لاستخدام البيانات الشخصية في قطاع الشرطة.[792]

**الأمر التوجيهي للاتحاد الأوروبي حول سجل أسماء الركاب**

ترتبط بيانات سجل أسماء الركاب بالمعلومات الخاصة بالمسافرين جواً التي يتم جمعها والاحتفاظ بها في أنظمة مراقبة الحجوزات والمغادرة التابعة لشركات الطيران لأغراضها التجارية. وتشمل هذه البيانات أنواعاً مختلفة من المعلومات، مثل تواريخ السفر وخط سير الرحلات ومعلومات خاصة بالتذاكر ومعلومات الاتصال ووكيل السفر الذي حَجزت الرحلة عنده ووسائل الدفع المستخدمة ورقم المقعد والمعلومات المتعلقة بالأمتعة.[793] قد تساعد معالجة بيانات سجل أسماء الركاب سلطات إنفاذ القانون في تحديد المشتبه بهم المعروفين أو المحتملين وإجراء التقييمات بناءً على أنماط السفر ومؤشرات أخرى مرتبطة عادةً بالأنشطة الإجرامية. كما يسمح تحليل بيانات سجل أسماء الركاب بتتبع مسارات السفر وجهات الاتصال الخاصة بالأشخاص المشتبه في تورطهم في أنشطة إجرامية بشكل استرجاعي، مما يمكن سلطات إنفاذ القانون من تحديد الشبكات الإجرامية.[794] وقد أبرم الاتحاد الأوروبي بعض الاتفاقيات مع دول أخرى لتبادل بيانات سجلات أسماء الركاب، كما هو موضح في الجزء 7. إضافة إلى ذلك، فقد أدرج معالجة بيانات سجلات أسماء الركاب داخل الاتحاد الأوروبي، من خلال الأمر التوجيهي رقم EU/2016/681 الخاص باستخدام بيانات سجلات أسماء الركاب لمنع الجرائم الإرهابية والجرائم الخطيرة والكشف عنها والتحقيق فيها ومقاضاة مرتكبيها (الأمر التوجيهي للاتحاد الأوروبي الخاص بسجلات أسماء الركاب).[795] ويلزم هذا الأمر التوجيهي شركات النقل الجوي بإرسال بيانات سجلات أسماء الركاب إلى السلطات المختصة، ويضع ضمانات صارمة خاصة بحماية البيانات لمعالجة هذه البيانات وجمعها. ولا ينطبق الأمر التوجيهي الخاص بسجلات أسماء الركاب للاتحاد الأوروبي على الرحلات الجوية الدولية من الاتحاد الأوروبي وإليه فحسب، وإنما على الرحلات داخل الاتحاد الأوروبي أيضاً إذا قررت دولة عضو ذلك.[796]

يجب أن تقتصر بيانات سجلات أسماء الركاب التي تم جمعها على المعلومات التي يسمح بها الأمر التوجيهي الخاص بسجلات أسماء الركاب للاتحاد الأوروبي. كما يتعين الاحتفاظ بها في وحدة معلوماتية واحدة في مكان آمن في كل دولة عضو. ويجب تجريد بيانات سجلات أسماء الركاب من السمات الشخصية بعد ستة أشهر من نقلها من شركة النقل الجوي والاحتفاظ بها لمدة لا تتجاوز خمس سنوات.[797] هذا ويتم تبادل بيانات سجلات أسماء الركاب ما بين الدول الأعضاء وبين الدول الأعضاء واليوروبول؛ كما يمكن تبادلها مع بلدان أخرى، ولكن فقط على أساس كل حالة على حدة.

يجب أن يتماشى نقل ومعالجة بيانات سجلات أسماء الركاب والحقوق المكفولة لأصحاب البيانات مع الأمر التوجيهي الخاص بحماية البيانات والموجه للشرطة وسلطات العدالة الجنائية وينبغي أن يضمن مستوى عالٍ من حماية الخصوصية والبيانات الشخصية التي ينص عليها كل من الميثاق والاتفاقية 108 المحدثة والاتفاقية الأوروبية لحقوق الإنسان.

---

[790] مجلس أوروبا (1981)، اتفاقية حماية الأفراد فيما يتعلق بمعالجة البيات الشخصية الآلية، سلسلة المعاهدات الأوروبية رقم 108.

[791] مجلس أوروبا (2001)، البروتوكول الإضافي الملحق باتفاقية حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية الآلية فيما يخص الهيئات الإشرافية وتدفقات البيانات عبر الحدود، سلسلة المعاهدات الأوروبية رقم 108.

[792] مجلس أوروبا (1987)، التوصية رقم R (87) 15 الصادرة عن لجنة الوزراء والموجهة إلى الدول الأعضاء والمنظمة لاستخدام البيانات الشخصية في قطاع الشرطة (والتي اعتمدتها لجنة الوزراء في 17 سبتمبر1987 خلال الاجتماع رقم 410 لنواب الوزراء.)

[793] المفوضية الأوروبية (2011)، مقترح أمر توجيهي خاص بالبرلمان الأوروبي والمجلس حول استعمال بيانات سجلات أسماء الركاب لمنع الجرائم الإرهابية والجرائم الخطيرة والكشف عنها والتحقيق فيها ومقاضاة مرتكبيها، النسخة النهائية32 (2011)COM ، بروكسل، 2 فبراير 2011، ص. 1.

[794] المفوضية الأوروبية (2015)، صحيفة وقائع محاربة الإرهاب على مستوى الاتحاد الأوروبي، لمحة عامة عن أعمال المفوضية وتدابيرها ومبادراتها، بروكسل 11 يناير 2015.

[795] الأمر التوجيهي (الاتحاد الأوروبي) رقم 2016/681 للبرلمان الأوروبي والمجلس بتاريخ 27 أبريل 2016 بشأن استخدام بيانات سجلات أسماء الركاب لمنع الجرائم الإرهابية والجرائم الخطيرة والكشف عنها والتحقيق فيها ومقاضاة مرتكبيها، الجريدة الرسمية 119 L 2016 0J، ص. 132.

[796] الأمر التوجيهي الخاص بسجلات أسماء الركاب، 119 L، ص. 132، المادة 1 (1) والمادة 2 (1).

[797] نفس المرجع السابق، المادة 12 (1) والمادة 12 (2).

وتعد الهيئات الإشرافية الوطنية المستقلة المختصة بموجب الأمر التوجيهي الخاص بحماية البيانات والموجه للشرطة وسلطات العدالة الجنائية مسؤولة أيضاً عن تقديم المشورة بشأن تطبيق المقتضيات التي اعتمدتها الدول الأعضاء ومتابعته، وفقاً للأمر التوجيهي . للاتحاد الأوروبي الخاص بسجلات أسماء الركاب

**الاحتفاظ ببيانات الاتصالات**

ألزم الأمر التوجيهي الخاص بالاحتفاظ بالبيانات[798] - الذي أُصدر قرار بعدم صلاحيته في 8 أبريل 2014 - في قضية «ديجيتال رايتس آيرلاند» - مقدمي خدمات الاتصالات بالاحتفاظ بالبيانات الوصفية المتاحة لغرض محدد يتجلى في مكافحة الجرائم الخطيرة، وذلك لمدة تتراوح بين ستة أشهر على الأقل و24 شهراً كحد أقصى، بغض النظر عما إذا كان لا يزال مقدم الخدمة بحاجة إلى هذه البيانات لأغراض الفوترة أو لتقديم الخدمة من الناحية التقنية.

ومن الواضح أن الاحتفاظ ببيانات الاتصالات يتدخل في الحق في حماية البيانات.[799] و، لقد تم الطعن فيما إذا كان هذا التدخل مبرراً أم لا في العديد من الإجراءات القضائية بالدول الأعضاء في الاتحاد الأوروبي.[800]

مثال: في قضيتي «ديجيتال رايتس آيرلاند» و»حكومة كيرنتن وآخرين»،[801] رفعت مجموعة «ديجيتال رايتس» والسيد سيتلينغر دعوى أمام المحكمة العليا في أيرلندا والمحكمة الدستورية في النمسا على التوالي، للطعن في قانونية الإجراءات الوطنية التي تسمح بالاحتفاظ ببيانات الاتصالات الإلكترونية. وطلبت مجموعة «ديجيتال رايتس» من المحكمة الأيرلندية أن تقضي بعدم صلاحية الأمر التوجيهي رقم 2006/24 وجزء من القانون الجنائي الوطني المتعلق بالجرائم الإرهابية. وبالمثل، طعن السيد سيتلينغر وأكثر من 11 ألف مدعٍ آخر أحد مقتضيات التشريع النمساوي الخاص بالاتصالات الذي اعتمد الأمر التوجيهي رقم وطالبوا بإلغائه 2006/24.

عند بتها في طلبات إصدار الأحكام الأولية، قضت محكمة العدل التابعة للاتحاد الأوروبي بعدم صلاحية الأمر التوجيهي الخاص بالاحتفاظ بالبيانات. ووفقاً للمحكمة ، فإن البيانات التي يمكن الاحتفاظ بها بموجب الأمر التوجيهي قدمت معلومات دقيقة حول الأفراد عند النظر إليها في مجملها. علاوة على ذلك، بتت المحكمة في مدى خطورة التدخل في الحقوق الأساسية المتعلقة باحترام الحياة الخاصة وحماية البيانات الشخصية، وتبين لها أن الاحتفاظ بالبيانات يستجيب لهدف من أهداف المصلحة العامة - ألا وهو مكافحة الجرائم الخطيرة، وبالتالي الأمن العام. ومع ذلك، أشارت المحكمة أن مشرع الاتحاد الأوروبي قد انتهك مبدأ التناسبية من خلال اعتمادالأمر التوجيهي. وعلى الرغم من أن الأمر التوجيهي قد يكون مناسباً لتحقيق الهدف المطلوب، فإن «التدخل واسع النطاق والخطير بشكل خاص للأمر التوجيهي في الحقين الأساسيين المتمثلين في احترام الخصوصية وحماية البيانات الشخصية غير مقيد بما يكفي ليضمن أن هذا التدخل يقتصر بالفعل على ما هو ضروري للغاية».

يُسمح بالاحتفاظ بالبيانات، في غياب تشريع محدد خاص بالاحتفاظ بالبيانات، كاستثناء لسرية بيانات الاتصالات بموجب الأمر التوجيهي EC/2002/58 (الأمر التوجيهي الخاص بالخصوصية والاتصالات الإلكترونية)،[802] كتدبير وقائي، لكن يجب أن يقتصر فقط على غرض محاربة الجريمة الخطيرة. ويجب أن يكون هذا الاحتفاظ مقتصراً على ما هو ضروري للغاية وذلك فيما يتعلق بفئات البيانات المحتفظ بها ووسائل الاتصال المتأثرة والأشخاص المعنيين ومدة الاحتفاظ المختارة. ويجوز للسلطات العامة الوصول إلى البيانات المحتفظ بها وفقا لشروط صارمة، بما في ذلك المراجعة المسبقة من قبل هيئة مستقلة. هذا ويجب الاحتفاظ بالبيانات داخل الاتحاد الأوروبي.

---

[798] الأمر التوجيهي EC/2006/24 للبرلمان الأوروبي والمجلس بتاريخ 15 مارس 2006 بشأن الاحتفاظ بالبيانات التي تم توليدها أو معالجتها فيما يتعلق بتوفير خدمات الاتصالات الإلكترونية المتاحة للعامة أو شبكات الاتصالات العامة والأمر التوجيهي المعدّل رقم EC/2002/58، الجريدة الرسمية L 105 2006 OJ.

[799] المشرف الأوروبي على حماية البيانات (2011)، رأي بتاريخ 31 مايو 2011 بشأن تقرير التقييم المقدم من المفوضية إلى البرلمان الأوروبي والمجلس بشأن الأمر التوجيهي الخاص بالاحتفاظ بالبيانات (الأمر التوجيهي EC)، 31/2006/24 مايو 2011.

[800] ألمانيا، المحكمة الدستورية الاتحادية 1 BvR 256/08 ،(Bundesverfassungsgericht)، 2 مارس 2010؛ رومانيا، المحكمة الدستورية الرومانية (Curtea Constituţională a României)، رقم 1258، 8 أكتوبر 2009؛ جمهورية التشيك، المحكمة الدستورية 94/2011 Coll ،(Ústavní soud Ceské republiky) 22 مارس 2011.

[801] محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-293/12 وC-594/12، قضية «شركة 'ديجيتال رايتس آيرلاند' المحدودة ضد وزير الاتصالات والموارد البحرية والطبيعية وآخرين' و'حكومة كيرنتن وآخرون'» [الغرفة الكبرى]، 8 أبريل 2014، الفقرة 65.

[802] الأمر التوجيهي رقم EC/2002/58 للبرلمان الأوروبي والمجلس بتاريخ 12 يوليو 2002 بخصوص معالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الإلكترونية (الأمر التوجيهي الخاص بالخصوصية والاتصالات الالكترونية)، الجريدة الرسمية L 201 2002 OJ.

مثال: عقب الحكم الصادر في قضيتي «ديجيتال رايتس آيرلاند» و»حكومة كيرنتن وآخرين»،[803] رُفعت قضيتان أخريان أمام محكمة العدل التابعة للاتحاد الأوروبي تتعلقان بالالتزام العام المفروض في السويد وفي المملكة المتحدة على مقدمي خدمات الاتصالات الإلكترونية بالاحتفاظ ببيانات الاتصالات، كما نص عليه الأمر التوجيهي الملغى الخاص بالاحتفاظ بالبيانات. وفي قضيتي «'تيلي 2 السويد المحدودة' ضد الإدارة السويدية للبريد والاتصالات» و»توم واتسون وآخرين»،[804] حكمت محكمة العدل التابعة للاتحاد الأوروبي بأن التشريع الوطني الذي نص على الاحتفاظ غير التمييزي والعام للبيانات دون فرض وجود علاقة بين البيانات التي يتعين الاحتفاظ بها وخطر يهدد الأمن العام، ودون وضع شروط - مثل مدة الاحتفاظ بالبيانات والمنطقة الجغرافية ومجموعة الأشخاص الذين يرجح تورطهم في جريمة خطيرة - يتجاوز حدود ما هو ضروري ولا يمكن أن يعتبر مبرراً في مجتمع ديمقراطي، كما هو منصوص عليه في الأمر التوجيهي EC/2002/58، (قراءة في ضوء ميثاق الحقوق الأساسية للاتحاد الأوروبي).

**الآفاق**

في يناير 2017، نشرت المفوضية الأوروبية مقترحاً خاصاً بلائحة تتعلق باحترام الحياة الخاصة وحماية البيانات الشخصية في مجال الاتصالات الإلكترونية، وكان يقصد به إلغاء واستبدال الأمر التوجيهي EC/2002/58. [805] ولا يشمل المقترح أي مقتضيات خاصة بالاحتفاظ بالبيانات. غير أنه ينص على إمكانية تقييد الدول الأعضاء لبعض الالتزامات والحقوق الواردة في اللائحة بواسطة القانون، عندما يكون هذا التقييد تدبيراً ضرورياً ومتناسباً لصون مصالح عامة محددة، بما فيها الأمن الوطني أو الدفاع أو الأمن العام أو منع الجرائم الجنائية والتحقيق فيها والكشف عنها وملاحقة مرتكبيها أو تنفيذ العقوبات الجنائية.[806] لذلك، ستكون الدول الأعضاء قادرة على وضع أو الإبقاء على أطر وطنية خاصة بالاحتفاظ بالبيانات تنص على تدابير الاحتفاظ المستهدفة، طالما أن هذه الأطر تمتثل لقانون الاتحاد، مع مراعاة السوابق القضائية لمحكمة العدل التابعة للاتحاد الأوروبي بشأن تفسير الأمر التوجيهي الخاص بالخصوصية الإلكترونية وميثاق الحقوق الأساسية للاتحاد الأوروبي.[807] تجدر الإشارة على أنه عند صياغة الدليل، كانت المناقشات بشأن اعتماد اللائحة جارية.

**الاتفاق الشامل بين الاتحاد الأوروبي والولايات المتحدة بشأن حماية البيانات الشخصية المتبادلة لأغراض إنفاذ القانون**

دخل الاتفاق الشامل بين الاتحاد الأوروبي والولايات المتحدة المتعلق بمعالجة البيانات الشخصية لمنع الجرائم الجنائية والتحقيق فيها والكشف عنها ومقاضاة مرتكبيها حيز التنفيذ في 1 فبراير 2017. [808] ويهدف هذا الاتفاق إلى ضمان مستوى عالٍ من حماية البيانات لمواطني الاتحاد الأوروبي بالموازاة مع تعزيز التعاون بين سلطات إنفاذ القانون في الاتحاد الأوروبي والولايات المتحدة. فهو يكمل الاتفاقيات القائمة بين الاتحاد الأوروبي والولايات المتحدة وبين الدول الأعضاء والولايات المتحدة المبرمة بين سلطات إنفاذ القانون، فيما يساعد أيضاً في وضع قواعد حماية بيانات واضحة ومتناسقة مع الاتفاقيات المستقبلية في هذا المجال. وفي هذا الصدد، يهدف الاتفاق إلى وضع إطار قانوني دائم لتسهيل تبادل المعلومات.

لا يوفر الاتفاق في حد ذاته أساساً قانونياً مناسباً لتبادل البيانات الشخصية، ولكنه يوفر بدلاً من ذلك ضمانات حماية مناسبة للبيانات للأفراد المعنيين. هذا ويشمل جميع عمليات معالجة البيانات الشخصية اللازمة لمنع الجرائم الجنائية، بما في ذلك الإرهاب، والتحقيق فيها وكشفها ومقاضاة مرتكبيها.[809]

---

[803] محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-293/12 وC-594/12، قضية «شركة 'ديجيتال رايتس آيرلاند' المحدودة ضد وزير الاتصالات والموارد البحرية والطبيعية وآخرين' و'حكومة كيرنتن وآخرون'» [الغرفة الكبرى]، 8 أبريل 2014.

[804] محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان رقم C-203/15 وC-698/15، قضية «'تيلي 2 السويد المحدودة' ضد الإدارة السويدية للبريد والاتصالات»، وقضية «وزير الدولة المكلف بالشؤون الداخلية ضد توم واتسون وآخرين» [الغرفة الكبرى]، 21 ديسمبر 2016.

[805] المفوضية الأوروبية (2017)، مقترح لائحة للبرلمان الأوروبي والمجلس يتعلق باحترام الحياة الخاصة وحماية البيانات الشخصية في مجال الاتصالات الإلكترونية والملغي للأمر التوجيهي EC/2002/58 (اللائحة الخاصة بالخصوصية والاتصالات الإلكترونية)، النسخة النهائية10 ، 10 COM(2017) يناير 2017.

[806] نفس المرجع السابق، الحيثية 26.

[807] انظر المذكرة التفسيرية لمقترح اللائحة المتعلقة بالخصوصية والاتصالات الإلكترونية، النسخة النهائية10 COM(2017) ، النقطة 3.1.

[808] انظر مجلس الاتحاد الأوروبي (2016)، «حقوق حماية البيانات المعززة لمواطني الاتحاد الأوروبي في إطار التعاون في مجال إنفاذ القانون: الاتحاد الأوروبي والولايات المتحدة يوقعان اتفاقا شاملاً»، بيان صحفي 305/16، 2 يونيو 2016

[809] اتفاق بين الولايات المتحدة الأمريكية والاتحاد الأوروبي بشأن حماية المعلومات الشخصية المتعلقة بمنع الجرائم الجنائية والتحقيق فيها والكشف عنها ومقاضاة مرتكبيها بتاريخ 18 مايو 2016، (OR.en 8557/16)، المادة 3 (1). انظر أيضا إشعار المفوضية بشأن مفاوضات اتفاق حماية البيانات بين الاتحاد الأوروبي والولايات المتحدة بتاريخ 26 مايو 2010، MEMO/10/216 والبيان الصحفي الصادر عن المفوضية الأوروبية (2010) بشأن معايير الخصوصية العالية في اتفاق حماية البيانات بين الاتحاد الأوروبي والولايات المتحدة بتاريخ 26 مايو 2010، IP/10/609.

يحدد الاتفاق عدداً من الضمانات التي تحرص على استعمال البيانات الشخصية للأغراض المحددة في الاتفاق دون غيرها. كما أنه يقدم على وجه الخصوص الحماية التالية لمواطني الاتحاد الأوروبي:

- قيود استعمال البيانات: يجوز أن تستعمل البيانات الشخصية فقط لغرض منع الجرائم الجنائية أو التحقيق فيها أو الكشف عنها أو مقاضاة مرتكبيها؛
- الحماية ضد التمييز التعسفي وغير المبرر؛
- عمليات النقل اللاحقة: يجب أن يخضع أي نقل لاحق إلى بلد خارج الولايات المتحدة أو خارج الاتحاد الأوروبي أو منظمة دولية لموافقة مسبقة من السلطة المختصة في البلد الذي نقل البيانات في الأصل؛
- جودة البيانات: يتعين الإبقاء على البيانات الشخصية مع مراعاة دقتها وملاءمتها وحسن توقيتها واكتمالها؛
- أمن المعالجة، بما في ذلك الإشعار باختراقات البيانات الشخصية؛
- لا يُسمح بمعالجة البيانات الحساسة إلا بوجود ضمانات متناسبة وفقاً للقانون؛
- فترات الاحتفاظ بالبيانات: لا يجوز الاحتفاظ بالبيانات لمدة أطول مما هو ضروري أو مناسب؛
- حقوق الوصول والتصحيح: يحق لأي فرد الوصول إلى بياناته الشخصية، وفقاً لشروط معينة، وسيكون قادراً على طلب تصحيح البيانات إذا كانت غير دقيقة؛
- تتطلب القرارات الآلية ضمانات مناسبة، بما في ذلك إمكانية التدخل البشري؛
- المراقبة الفعالة، بما في ذلك التعاون بين سلطات الرقابة التابعة للاتحاد الأوروبي والولايات المتحدة؛
- الإنصاف القضائي وقابلية الإنفاذ: يحق لمواطني الاتحاد الأوروبي[810] طلب الإنصاف القضائي أمام المحاكم الأمريكية في الحالات التي ترفض فيها السلطات الأمريكية السماح لهم بالوصول إلى البيانات أو تصحيحها، أو تكشف بشكل غير مشروع عن بياناتهم الشخصية.

بموجب «الاتفاق الشامل»، تم أيضاً وضع نظام لإشعار الهيئة الإشرافية المختصة في الدولة العضو بالأفراد المتأثرين بأي انتهاكات لحماية البيانات، عند الاقتضاء. وتحرص الضمانات القانونية المنصوص عليها في الاتفاق على ضمان المساواة في المعاملة بين مواطني الاتحاد الأوروبي في الولايات المتحدة في حال وجود انتهاك للخصوصية.[811]

## 1.3.8. حماية البيانات في وكالات إنفاذ القانون والوكالات القضائية بالاتحاد الأوروبي

**مكتب الشرطة الأوروبي («اليوروبول»)**

يقع مقر اليوروبول الرئيسي، وهي الوكالة الأوروبية لإنفاذ القانون ، في لاهاي. ويوجد في كل دولة عضو وحدات يوروبول وطنية. وقد تأسست الوكالة في 1998، ويعتمد وضعها القانوني الحالي كمؤسسة تابعة للاتحاد الأوروبي على لائحة وكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون (اللائحة التنظيمية لليوروبول).[812] ويتمثل الهدف من اليوروبول في المساعدة في منع الجريمة المنظمة والإرهاب والأشكال الأخرى للجريمة الخطيرة التي تؤثر على دولتين أو أكثر من الدول الأعضاء والتحقيق فيها، كما هو مدرج في الملحق الأول من اللائحة التنظيمية لليوروبول. ويتم ذلك من خلال تبادل المعلومات والعمل كمركز معلوماتي في الاتحاد الأوروبي، وتوفير تحليلات استخباراتية وتقييمات للتهديدات.

ولتحقيق أهدافه، أحدث اليوروبول نظام اليوروبول للمعلومات، الذي يوفر قاعدة بيانات للدول الأعضاء لتبادل المعلومات الاستخبارية والمعلومات الجنائية من خلال وحدات اليوروبول الوطنية الخاصة بها. ويمكن استخدام نظام اليوروبول للمعلومات لتوفير البيانات المتعلقة بـ: الأشخاص المشتبه بهم أو الذين أدينوا بارتكاب جريمة جنائية تخضع لاختصاص اليوروبول؛ أو الأشخاص الذين توجد دلائل واقعية على أنهم

[810] تم التوقيع على مشروع قانون الإنصاف القضائي الأمريكي ليصبح قانوناً من قبل الرئيس أوباما في 24 فبراير 2016.

[811] أصدر المشرف الأوروبي على حماية البيانات رأياً بشأن اتفاق الاتحاد الأوروبي والولايات المتحدة، حيث يوصي، ضمن جملة من أمور أخرى، بالتعديلات التالية: 1) إضافة «للأغراض المحددة التي تم نقلها من أجلها» إلى المادة التي تتناول الاحتفاظ بالبيانات لمدة لا تزيد عما هو ضروري ومناسب، و2) استثناء النقل بالجملة للبيانات الحساسة، والذي قد يكون ممكناً. انظر المشرف الأوروبي على حماية البيانات، الرأي 2016/1، «رأي أولي بشأن الاتفاق المبرم بين الولايات المتحدة الأمريكية والاتحاد الأوروبي بشأن حماية المعلومات الشخصية المتعلقة بمنع الجرائم الجنائية والتحقيق فيها والكشف عنها ومقاضاة مرتكبيها، الفقرة 35.

[812] لائحة (الاتحاد الأوروبي) 794/2016 للبرلمان الأوروبي والمجلس بتاريخ 11 مايو 2016 بشأن وكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون (اليوروبول) التي استبدلت وألغت قرارات المجلس JHA/2009/371، وJHA/2009/934، وJHA/2009/935، وJHA/2009/936، وJHA/2009/968، الجريدة الرسمية 135 لـ 2016 OJ، ص. 53.

سيرتكبون مثل هذه الجرائم. وقد يقوم كل من اليوروبول ووحدات اليوروبول الوطنية بإدخال البيانات مباشرة في نظام معلومات اليوروبول واستخراجها. ويجوز فقط للطرف الذي أدخل البيانات في النظام تعديلها أو تصحيحها أو حذفها. هذا ويمكن لهيئات الاتحاد الأوروبي والدول الأخرى والمنظمات الدولية أيضاً تقديم المعلومات لليوروبول.

يمكن لليوروبول أيضاً الحصول على المعلومات، بما في ذلك البيانات الشخصية، من المصادر المتاحة للعموم مثل الإنترنت. ولا يُسمح بنقل البيانات الشخصية إلى هيئات الاتحاد الأوروبي إلا إذا كان ذلك ضرورياً لأداء مهمة خاصة باليوروبول أو هيئة الاتحاد الأوروبي المتلقية. ولا يُسمح بنقل البيانات الشخصية إلى دول أخرى أو منظمات دولية إلا إذا قررت المفوضية الأوروبية أن الدولة أو المنظمة الدولية المعنية تضمن مستوى مناسباً من حماية البيانات («قرار الكفاية»)، أو إذا كانت هناك اتفاقية دولية أو اتفاقية تعاون. كما يمكن لليوروبول تلقي ومعالجة البيانات الشخصية من الأطراف الخاصة والأشخاص العاديين في ظل شروط صارمة تتمثل في نقل هذه البيانات بواسطة وحدة اليوروبول الوطنية وفقاً لقانونها الوطني، عن طريق نقطة اتصال في بلد ثالث أو منظمة دولية يجمعها بالوكالة تعاون راسخ من خلال اتفاقية تعاون، أو من خلال سلطة دولة ثالثة أو منظمة دولية تخضع لقرار الكفاية أو أبرم الاتحاد الأوروبي معها اتفاقية دولية. وتتم جميع عمليات تبادل المعلومات من خلال تطبيق شبكة تبادل المعلومات الآمنة (SIENA).

واستجابة للتطورات الجديدة، تم إنشاء مراكز متخصصة داخل اليوروبول، مثل المركز الأوروبي للجرائم الإلكترونية الذي أحدث في 2013،[813] و الذي يعمل كمركز معلومات للاتحاد الأوروبي بشأن الجرائم الإلكترونية، حيث يساهم في تسريع الاستجابة في حال وقوع جرائم عبر الإنترنت، وتطوير قدرات الاستدلال الرقمي واعتمادها وتقديم أفضل الممارسات في التحقيقات في الجرائم السيبرانية. ويركز المركز على الجرائم السيبرانية التي:

- ترتكبها جماعات منظمة لتحقيق أرباح إجرامية كبيرة، مثل الاحتيال الإلكتروني؛
- تسبب ضرراً جسيماً للضحية، مثل الاستغلال الجنسي للأطفال عبر الإنترنت؛
- تؤثر على البنية التحتية الحيوية أو أنظمة المعلومات داخل الاتحاد الأوروبي.

وقد تم إنشاء المركز الأوروبي لمكافحة الإرهاب (ECTC) في يناير 2016 لتقديم الدعم التشغيلي للدول الأعضاء في التحقيقات المتعلقة بالجرائم الإرهابية. ويقوم بالتحقق من البيانات التشغيلية الحية ومقارنتها مع البيانات التي يمتلكها اليوروبول بالفعل، مما يكشف عن الأدلة المالية بسرعة، ويحلل جميع تفاصيل التحقيق المتاحة للمساعدة في تجميع صورة مهيكلة لشبكة إرهابية.[814]

كما أُسس المركز الأوروبي الخاص بتهريب المهاجرين (EMSC) في فبراير 2016، عقب اجتماع المجلس في نوفمبر 2015، لدعم الدول الأعضاء في استهداف وتفكيك الشبكات الإجرامية المتورطة في تهريب المهاجرين، وهو يعمل كمركز للمعلومات يدعم مكاتب فرق العمل الإقليمية التابعة للاتحاد الأوروبي في كاتانيا (إيطاليا) وبيرايوس (اليونان)، والتي تساعد السلطات الوطنية في العديد من المجالات، بما في ذلك تبادل المعلومات الاستخباراتية والتحقيقات الجنائية ومتابعة شبكات تهريب الأشخاص الإجرامية.[815]

تم تحسين نظام حماية البيانات الذي ينظم أنشطة اليوروبول حيث إنه يستند إلى مبادئ لائحة حماية البيانات الخاصة بمؤسسات الاتحاد الأوروبي[816] ويتوافق أيضا مع الأمر التوجيهي الخاص بحماية البيانات والموجه للشرطة وسلطات العدالة الجنائية، والاتفاقية 108 المحدثة والتوصية الخاصة بالشرطة.

---

[813] انظر أيضا المشرف الأوروبي على حماية البيانات (2012)، رأي المشرف الأوروبي على حماية البيانات بشأن مراسلة المفوضية الأوروبية الموجهة إلى المجلس والبرلمان الأوروبي بشأن إحداث المركز الأوروبي للجرائم الإلكترونية، بروكسل، 29 يونيو 2012.

[814] انظر صفحة اليوروبول حول المركز الأوروبي لمكافحة الإرهاب.

[815] انظر صفحة اليوروبول حول المركز الأوروبي الخاص بتهريب المهاجرين.

[816] اللائحة (الجماعة الأوروبية) رقم45/2001 للبرلمان الأوروبي والمجلس بتاريخ 18 ديسمبر 2000 بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية من قبل مؤسسات وهيئات الجماعة وحرية حركة هذه البيانات، الجريدة الرسمية L 8 2001 OJ.

ويُسمح بمعالجة البيانات الشخصية فيما يتعلق بضحايا الجرائم الجنائية أو الشهود أو الأشخاص الآخرين الذين يمكنهم تقديم معلومات تخص الجرائم الجنائية، أو فيما يتعلق بالأشخاص الذين تقل أعمارهم عن 18 عاماً، إذا كانت ضرورية ومتناسبة تماماً لمنع أو مكافحة الجريمة التي تندرج ضمن أهداف اليوروبول.[817] وتحظر معالجة البيانات الشخصية الحساسة، ما لم تكن ضرورية ومتناسبة تماماً لمنع أو مكافحة الجريمة التي تندرج ضمن أهداف اليوروبول وإذا كانت هذه البيانات مكملة للبيانات الشخصية الأخرى التي تتم معالجتها من قبل اليوروبول.[818] وفي كلتا الحالتين، لا يمكن الوصول إلى البيانات ذات الصلة إلا من قبل اليوروبول.[819]

لا يُسمح بتخزين البيانات إلا لفترة زمنية ضرورية ومتناسبة ويخضع استمراره لمراجعة كل ثلاث سنوات، يتم بدونها مسح البيانات تلقائياً.[820]

ويُسمح لليوروبول، في ظل ظروف معينة، بنقل البيانات الشخصية إلى هيئة تابعة للاتحاد الأوروبي أو إلى سلطة دولة أخرى أو إلى منظمة دولية بشكل مباشر.[821] وإذا كان من المحتمل أن يؤثر اختراق البيانات بشكل خطير وسلبي على حقوق وحريات أصحاب البيانات، فيجب إبلاغهم به دون تأخير لا مبرر له.[822] وعلى مستوى الدول الأعضاء، سيتم تعيين هيئة إشرافية وطنية لتتبع معالجة اليوروبول للبيانات الشخصية.[823]

إن المشرف الأوروبي على حماية البيانات الشخصية مسؤول عن تتبع وضمان حماية الحقوق والحريات الأساسية للأشخاص الطبيعيين فيما يتعلق بمعالجة اليوروبول للبيانات الشخصية، وكذلك عن تقديم المشورة لليوروبول وأصحاب البيانات بشأن جميع الأمور المتعلقة بمعالجة البيانات الشخصية. وتحقيقاً لهذه الغاية، يضطلع المشرف الأوروبي على حماية البيانات بدور هيئة للتحقيق وتلقي الشكايات ويعمل بتعاون وثيق مع الهيئات الإشرافية الوطنية.[824] ويجتمع المشرف الأوروبي على حماية البيانات والهيئات الإشرافية الوطنية مرتين في السنة على الأقل في مجلس التعاون، الذي يؤدي وظيفة استشارية.[825] وتلتزم الدول الأعضاء بإحداث هيئة إشرافية بموجب القانون، تختص بمراقبة جواز نقل البيانات الشخصية من الدولة إلى اليوروبول واسترجاع البيانات الشخصية وأي ارسال للبيانات الشخصية إلى اليوروبول من قبل الدولة العضو.[826] ويتعين على الدول الأعضاء أيضا ضمان إمكانية تصرف الهيئة الإشرافية الوطنية بشكل مستقل تماماً أثناء أداء مهامها وواجباتها بموجب اللائحة التنظيمية لليوروبول.[827] وللتحقق من قانونية معالجة البيانات وتتبع أنشطته ذاتياً وضمان سلامة البيانات وأمنها، يحتفظ اليوروبول بسجلات أو وثائق لأنشطة معالجة البيانات الخاصة به. وتشتمل هذه السجلات على معلومات حول عمليات المعالجة في أنظمة المعالجة الآلية المتعلقة بالجمع والتعديل والاستشارة والإفصاح والتوليف والمحو.[828]

يمكن استئناف قرار للمشرف الأوروبي على حماية البيانات أمام محكمة العدل التابعة للاتحاد الأوروبي.[829] ويحق لأي فرد تعرض لضرر نتيجة لعملية معالجة بيانات غير مشروعة الحصول على تعويض عن الضرر الذي لحق به، إما من اليوروبول أو من الدولة العضو المسؤولة، وذلك عن طريق رفع دعوى أمام محكمة العدل التابعة للاتحاد الأوروبي في الحالة الأولى، أو أمام المحكمة الوطنية المختصة في الحالة الثانية.[830] بالإضافة إلى ذلك، يمكن لمجموعة تدقيق برلمانية مشتركة متخصصة من البرلمانات الوطنية والبرلمان الأوروبي التدقيق في أنشطة اليوروبول.[831] كما أن لكل فرد الحق في الوصول إلى أي بيانات شخصية قد يحتفظ بها اليوروبول، بالإضافة إلى الحق في طلب التحقق من هذه البيانات الشخصية أو تصحيحها أو محوها، وقد تخضع هذه الأخيرة لإعفاءات وقيود.

[817] اللائحة التنظيمية لليوروبول، المادة 30 (1).
[818] نفس المرجع السابق، المادة 30 (2).
[819] نفس المرجع السابق، المادة 30 (3).
[820] نفس المرجع السابق، المادة 31.
[821] نفس المرجع السابق، المادة 24 والمادة 25 على التوالي.
[822] نفس المرجع السابق، المادة 35.
[823] اللائحة التنظيمية لليوروبول، المادة 42.
[824] نفس المرجع السابق، المادتان 43 و44.
[825] نفس المرجع السابق، المادة 45.
[826] نفس المرجع السابق، المادة 42 (1).
[827] نفس المرجع السابق، المادة 42 (1).
[828] نفس المرجع السابق، المادة 40.
[829] نفس المرجع السابق، المادة 48.
[830] نفس المرجع السابق، المادة 50.
[831] نفس المرجع السابق، المادة 51.

**وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية («يوروجست»)**

تأسست وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية في 2002، وهي هيئة تابعة للاتحاد الأوروبي يوجد مقرها في لاهاي، وتعمل على تعزيز التعاون القضائي في التحقيقات والمتابعات القضائية المتعلقة بالجرائم الخطيرة فيما يتعلق بدولتين عضوين على الأقل.[832] وتتجلى اختصاصات الوكالة فيما يلي:

- تحفيز وتحسين تنسيق التحقيقات والمتابعات بين السلطات المختصة في مختلف الدول الأعضاء.
- تسهيل تنفيذ الطلبات والقرارات المتعلقة بالتعاون القضائي.

يؤدي الأعضاء الوطنيون وظائف وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية. وتقوم كل دولة عضو بإرسال قاض أو مدع عام إلى الوكالة، ويخضع وضعه القانوني للقانون الوطني ويتمتع بالصلاحيات اللازمة لأداء المهام اللازمة لتحفيز وتحسين التعاون القضائي. بالإضافة إلى ذلك، يعمل الأعضاء الوطنيون بشكل مشترك كمَجمع (أي هيئة مصغرة) لأداء المهام الخاصة لوكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية.

يجوز لوكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية معالجة البيانات الشخصية طالما كان ذلك ضرورياً لتحقيق أهدافها. ومع ذلك، يقتصر هذا الأمر على معلومات محددة تتعلق بالأشخاص المشتبه في ارتكابهم جريمة جنائية تخضع لاختصاص وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية أو المشاركة فيها أو الذين أدينوا بارتكابها. كما يجوز للوكالة معالجة بعض المعلومات المتعلقة بشهود أو ضحايا الجرائم الخاضعة لاختصاصها.[833] وفي ظروف استثنائية، يجوز للوكالة، لفترة محدودة من الوقت، معالجة بيانات شخصية أكثر شمولاً تتعلق بظروف الجريمة حيث تكون هذه البيانات ذات صلة مباشرة بالتحقيق الجاري. وفي نطاق اختصاصها، يجوز للوكالة الاتحاد الأوروبي التعاون مع مؤسسات وهيئات ووكالات الاتحاد الأوروبي الأخرى وتبادل البيانات الشخصية معها. ويجوز للوكالة أيضاً التعاون مع دول ومنظمات أخرى وتبادل البيانات الشخصية معها.

فيما يتعلق بحماية البيانات، يجب أن تضمن وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية مستوى من الحماية يعادل على الأقل مبادئ الاتفاقية 108 المحدثة وتعديلاتها اللاحقة. وفي حالات تبادل البيانات، يجب مراعاة القواعد والقيود المحددة، والتي يتم وضعها إما في اتفاقية تعاون أو ترتيبات عمل وفقاً لقرارات مجلس الوكالة وقواعد حماية البيانات الأوروبية التابعة لها.[834]

وقد تم إحداث هيئة إشرافية مشتركة ومستقلة في وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية أوكلت لها مهمة تتبع معالجة البيانات الشخصية التي تقوم بها الوكالة. ويجوز للأفراد الاستئناف أمام الهيئة الإشرافية المشتركة والمستقلة إذا لم يكونوا راضين عن قرار وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية فيما يخص طلب الوصول إلى البيانات الشخصية أو تصحيحها أو حجبها أو محوها. وعندما تقوم الوكالة بمعالجة البيانات الشخصية بشكل غير مشروع، فإنها ستكون مسؤولة وفقاً للقانون الوطني للدولة العضو حيث يقع مقرها الرئيسي، أي هولندا، عن أي ضرر يلحق بصاحب البيانات.

**الآفاق**

قدمت المفوضية الأوروبية مقترحاً بشأن لائحة لإصلاح وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية في يوليو 2013. وكان هذا المقترح مصحوباً باقتراح لإحداث مكتب المدعي العام الأوروبي (انظر أدناه). وتهدف هذه اللائحة إلى تبسيط الوظائف والهيكل

---

[832] مجلس الاتحاد الأوروبي (2002)، قرار المجلس JHA/2002/187 بتاريخ 28 فبراير 2002 بشأن إحداث وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية بهدف تعزيز مكافحة الجرائم الخطيرة، الجريدة الرسمية L 63 2002 OJ؛ مجلس الاتحاد الأوروبي (2003)، قرار المجلس JHA/2003/659 بتاريخ 18 يونيو 2003 المعدل للقرار JHA/2002/187 بشأن إحداث وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية بهدف تعزيز مكافحة الجرائم الخطيرة، الجريدة الرسمية L 44 2003 OJ؛ مجلس الاتحاد الأوروبي (2009)، قرار المجلس JHA/2009/426 بتاريخ 16 ديسمبر 2008 بشأن تعزيز وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية المعدل للقرار JHA/2002/187 بشأن إحداث وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية بهدف تعزيز مكافحة الجرائم الخطيرة، الجريدة الرسمية L 138 2009 OJ (قرارات وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية).

[833] نسخة مجمعة من قرار المجلس JHA/2002/187 بصيغته المعدلة بموجب قرار المجلس JHA/2003/659 وقرار المجلس JHA/2009/426، المادة 15 (2).

[834] القواعد الإجرائية الخاصة بمعالجة وحماية البيانات الشخصية في وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية، الجريدة الرسمية C 68/01، 19 OJ 2005 مارس 2005، ص. 1.

[835] انظر الصفحة الإلكترونية للمفوضية الأوروبية حول وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية.

لتتماشى مع معاهدة لشبونة. علاوة على ذلك، يتمثل هدف الإصلاح في الفصل بشكل واضح بين المهام التشغيلية لوكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية، التي يؤديها مَجمع «يوروجست»، ومهامها الإدارية. وسيمكن ذلك الدول الأعضاء من التركيز بشكل أكبر على المهام التشغيلية. وسيتم إنشاء مجلس تنفيذي جديد لمساعدة المَجمع في أداء المهام الإدارية.[835]

**مكتب المدعي العام الأوروبي**

تتمتع الدول الأعضاء بالاختصاص الحصري في متابعة الجرائم الجنائية والاحتيال والتطبيق غير السليم لميزانية الاتحاد الأوروبي، والتي لها أيضا آثار يحتمل أن تكون عابرة للحدود. وقد ازدادت أهمية التحقيق مع مرتكبي هذه الجرائم ومقاضاتهم وتقديمهم للعدالة، لا سيما في ظل الأزمة الاقتصادية المستمرة.[836] وقد اقترحت المفوضية الأوروبية لائحة بشأن إنشاء مكتب مستقل للمدعي العام الأوروبي[837] بهدف مكافحة الجرائم الجنائية التي تؤثر على المصالح المالية للاتحاد الأوروبي. وسيتم إحداث مكتب المدعي العام الأوروبي من خلال مسطرة التعاون المعزز، والتي تسمح لتسع دول أعضاء على الأقل بإقامة تعاون متقدم في مجال معين داخل هياكل الاتحاد الأوروبي، دون مشاركة دول الاتحاد الأوروبي الأخرى.[838] وقد انضمت كل من بلجيكا وبلغاريا وكرواتيا وقبرص وجمهورية التشيك وإستونيا وفنلندا وفرنسا وألمانيا واليونان ولاتفيا وليتوانيا ولوكسمبورغ والبرتغال ورومانيا وسلوفينيا وسلوفاكيا وإسبانيا إلى التعاون المعزز؛ كما أعربت النمسا وإيطاليا عن نيتهما للانضمام.[839]

سيشمل اختصاص مكتب المدعي العام الأوروبي التحقيق في جرائم الاحتيال في الاتحاد الأوروبي والجرائم الأخرى التي تؤثر على مصالحه المالية ومتابعة مرتكبيها، وذلك بهدف التنسيق الفعال للتحقيقات والمتابعات القضائية عبر الأنظمة القانونية الوطنية المختلفة وتحسين استخدام الموارد وتبادل المعلومات على المستوى الأوروبي.[840]

سيترأس هذه الهيئة مدع عام أوروبي ، مع تعيين مدع عام أوروبي واحد على الأقل في كل دولة عضو يتولى إنجاز التحقيقات والمتابعات القضائية فيها.

يضع المقترح ضمانات قوية لضمان حقوق الأشخاص المشاركين في تحقيقات مكتب المدعي العام الأوروبي على النحو المنصوص عليه في القانون الوطني وقانون الاتحاد الأوروبي وميثاق الحقوق الأساسية للاتحاد الأوروبي. وسوف تستدعي إجراءات التحقيق التي تمس في الغالب بالحقوق الأساسية إذناً مسبقاً من محكمة وطنية.[841] وستخضع تحقيقات مكتب المدعي العام الأوروبي للمراجعة القضائية من قبل المحاكم الوطنية.[842]

سيتم تطبيق لائحة حماية البيانات الخاصة بمؤسسات الاتحاد الأوروبي[843] على معالجة البيانات الشخصية الإدارية التي يقوم بها مكتب المدعي العام الأوروبي. وفيما يخص معالجة البيانات الشخصية المتعلقة بالمسائل التشغيلية، على غرار اليوروبول ، سيكون لدى مكتب المدعي العام الأوروبي نظام مستقل لحماية البيانات مشابه للنظام الذي يؤطر أنشطة اليوروبول ووكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية، نظراً لأن ممارسة وظائف مكتب المدعي العام الأوروبي ستشمل معالجة البيانات الشخصية مع سلطات إنفاذ القانون وسلطات الادعاء على مستوى الدول الأعضاء. لذلك، فإن قواعد حماية البيانات الخاصة بمكتب المدعي العام الأوروبي مطابقة تقريباً لقواعد الأمر التوجيهي الخاص بحماية البيانات الموجه للشرطة وسلطات العدالة الجنائية. ووفقاً لمقترح إحداث مكتب المدعي العام الأوروبي، يجب أن تمتثل معالجة البيانات الشخصية لمبادئ المشروعيةوالإنصاف وحصر الغرض وتقليل البيانات إلى الحد الأدنى والدقة والسلامة

[835] انظر الصفحة الإلكترونية للمفوضية الأوروبية حول وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية.

[836] انظر المفوضية الأوروبية (2013)، مقترح بخصوص لائحة المجلس المتعلقة بإحداث مكتب المدعي العام الأوروبي، النسخة النهائية 534 (2013)COM، بروكسل، 17 يوليو 2013 و الصفحة الإلكترونية للمفوضية الأوروبية حول وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية.

[837] انظر المفوضية الأوروبية (2013)، مقترح بخصوص لائحة المجلس المتعلقة بإحداث مكتب المدعي العام الأوروبي، النسخة النهائية 534 (2013)COM، بروكسل، 17 يوليو 2013.

[838] المعاهدة المنظمة لعمل الاتحاد الأوروبي، المادة 86 (1) والمادة 329 (1).

[839] انظر مجلس الاتحاد الأوروبي (2017)، «20 دولة عضو توافق على حيثيات تأسيس مكتب المدعي العام الأوروبي»، بيان صحفي، 8 يونيو 2017.

[840] المفوضية الأوروبية (2013)، مقترح بخصوص لائحة المجلس المتعلقة بإحداث مكتب المدعي العام الأوروبي، النسخة النهائية 534 (2013)COM، بروكسل، 17 يوليو 2013، ص. 1 وص. 51. انظر أيضا الصفحة الإلكترونية للمفوضية حول مكتب المدعي العام الأوروبي.

[841] المفوضية الأوروبية (2013)، مقترح بخصوص لائحة المجلس المتعلقة بإحداث مكتب المدعي العام الأوروبي، النسخة النهائية 534 (2013)COM، بروكسل، 17 يوليو 2013، المادة 26 (4).

[842] نفس المرجع السابق، المادة 36.

[843] اللائحة (الجماعة الأوروبية) رقم45/2001 للبرلمان الأوروبي والمجلس بتاريخ 18 ديسمبر 2000 بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية من قبل مؤسسات وهيئات الجماعة الأوروبية وحرية حركة هذه البيانات، الجريدة الرسمية L 8 2001 OJ.

والسرية. وينبغي على مكتب المدعي العام الأوروبي، قدر الإمكان، التمييز بوضوح بين البيانات الشخصية لفئات أصحاب البيانات المختلفة، مثل الأشخاص المدانين بارتكاب جريمة جنائية، والأشخاص المشتبه بهم فقط، والضحايا والشهود. كما يجب أن تسعى إلى التحقق من جودة البيانات الشخصية التي تتم معالجتها والتمييز، قدر الإمكان، بين البيانات الشخصية المبنية على حقائق مستمدة من البيانات الشخصية التي تقوم على تقييمات شخصية.

يضم المقترح مقتضيات بشأن حقوق أصحاب البيانات، ولا سيما الحق في المعلومة، والحق في الوصول إلى بياناتهم الشخصية، والحق في تصحيحها ومحوها وتقييد المعالجة، وينص على أنه يمكن ممارسة هذه الحقوق أيضا بشكل غير مباشر، من خلال المشرف الأوروبي على حماية البيانات. كما أنه يجسد مبادئ أمن المعالجة والمساءلة، ما يستدعي من مكتب المدعي العام الأوروبي تنفيذ التدابير التقنية والتنظيمية المناسبة لضمان مستوى أمن يتناسب مع المخاطر التي تشكلها المعالجة، والاحتفاظ بسجلات جميع أنشطة المعالجة وتنفيذ تقييم أثر حماية البيانات قبل المعالجة، حيث من المحتمل أن يؤدي نوع معين من المعالجة (على سبيل المثال، المعالجة التي تنطوي على استخدام تقنيات جديدة) إلى مخاطر عالية على حقوق الأفراد. وأخيراً، ينص الاقتراح على تعيين المَجمع (أي الهيئة المصغرة) لمسؤول عن حماية البيانات، يجب أن يشارك بشكل ملائم في جميع الأمور المتعلقة بحماية البيانات الشخصية ويجب أن يضمن امتثال مكتب المدعي العام الأوروبي للتشريع المعمول به فيما يخص حماية البيانات.

## 2.3.8. حماية البيانات في أنظمة المعلومات المشتركة على صعيد الاتحاد الأوروبي

بالإضافة إلى تبادل البيانات بين الدول الأعضاء وإحداث هيئات متخصصة لمكافحة الجريمة العابرة للحدود تابعة للاتحاد الأوروبي، مثل اليوروبول ووكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية ومكتب المدعي العام الأوروبي، تم وضع العديد من أنظمة المعلومات المشتركة على صعيد الاتحاد الأوروبي لتمكين وتسهيل التعاون وتبادل البيانات بين الهيئات الوطنية المختصة وتلك التابعة للاتحاد الأوروبي لأغراض محددة في مجالات حماية الحدود والهجرة واللجوء والجمارك. ونظراً لأن إنشاء منطقة شنغن جاء من خلال اتفاقية دولية تعمل بشكل مستقل عن قانون الاتحاد الأوروبي، فقد استند تطوير نظام معلومات شنغن إلى اتفاقيات متعددة الأطراف وتم إلحاقه بقانون الاتحاد الأوروبي فيما بعد. وتم وضع نظام معلومات التأشيرات (VIS) واللائحة المتعلقة بالنظام الأوروبي لمضاهاة بصمات الأصابع (Eurodac) ونظام مراقبة الحدود الأوروبية (Eurosur) ونظام المعلومات الجمركية (CIS) كأدوات ينظمها قانون الاتحاد الأوروبي.

وتتشارك كل من الهيئات الإشرافية الوطنية والمشرف الأوروبي على حماية البيانات في الإشراف على هذه الأنظمة. ولضمان مستوى عالٍ من الحماية، تتعاون هذه الهيئات ضمن مجموعات تنسيق الإشراف، والتي تشير إلى أنظمة تكنولوجيا المعلومات واسعة النطاق التالية: 1) اللائحة المتعلقة بالنظام الأوروبي لمضاهاة بصمات الأصابع؛ 2) نظام معلومات التأشيرات؛ 3) نظام معلومات شنغن؛ 4) نظام المعلومات الجمركية و5) نظام معلومات السوق الداخلي.[844] وعادة ما تلتقي مجموعات تنسيق الإشراف مرتين في السنة، تحت رئاسة رئيس منتخب، وتعتمد المبادئ التوجيهية، وتناقش الحالات العابرة للحدود أو تضع أطر عمل مشتركة لعمليات التفتيش.

تتولى الوكالة الأوروبية لأنظمة تكنولوجيا المعلومات واسعة النطاق،[845] التي تأسست في عام 2012، مسؤولية الإدارة التشغيلية للجيل الثاني من نظام معلومات شنغن ونظام معلومات التأشيرات واللائحة المتعلقة بالنظام الأوروبي لمضاهاة بصمات الأصابع. وتتجلى مهمتها الأساسية في ضمان التشغيل الفعال والآمن والمستمر لأنظمة تكنولوجيا المعلومات. كما أنها مسؤولة عن اتخاذ الإجراءات اللازمة لضمان أمن الأنظمة وأمن البيانات.

**نظام معلومات شنغن**

في 1985، دخلت العديد من الدول الأعضاء في الجماعة الأوروبية السابقة في الاتفاقية المبرمة بين دول اتحاد البنلوكس الاقتصادي وألمانيا وفرنسا بشأن الإلغاء التدريجي لعمليات التفتيش على حدودها المشتركة (اتفاقية شنغن)، وذلك بهدف إنشاء منطقة يتنقل فيها

[844] انظر الصفحة الإلكترونية للمشرف الأوروبي على حماية البيانات حول تنسيق الإشراف.

[845] لائحة (الاتحاد الأوروبي) رقم 1077/2011 للبرلمان الأوروبي والمجلس بتاريخ 25 أكتوبر 2011، المؤسسة للوكالة الأوروبية للإدارة التشغيلية لأنظمة المعلومات واسعة النطاق في مجال الحرية والأمن والعدالة، الجريدة الرسمية 286 L 2011 ص.

الأشخاص بحرية، دون عوائق الضوابط الحدودية داخل أراضي منطقة شنغن.[846] ولموازنة التهديد الأمني العام الذي يمكن أن ينشأ عن فتح الحدود، تم وضع ضوابط معززة على الحدود الخارجية لمنطقة شنغن، فضلاً عن التعاون الوثيق بين الشرطة الوطنية وسلطات العدالة.

ونتيجة انضمام دول أخرى إلى اتفاقية شنغن، تم إدراج نظام شنغن أخيراً في الإطار القانوني للاتحاد الأوروبي من خلال معاهدة أمستردام،[847] وقد دخل هذا القرار حيز التنفيذ في عام 1999. كما بدأ تشغيل أحدث إصدار من نظام معلومات شنغن، المعروف باسم الجيل الثاني من نظام معلومات شنغن في 9 أبريل 2013. وهو يستعمل الآن في معظم الدول الأعضاء في الاتحاد الأوروبي،[848] بالإضافة إلى أيسلندا وليختنشتاين والنرويج وسويسرا.[849] هذا ويمكن لليوروبول ووكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية أيضاً الوصول إلى الجيل الثاني من نظام معلومات شنغن.

يتكون الجيل الثاني من نظام معلومات شنغن من نظام مركزي، ونظام وطني في كل دولة عضو، وبنية تحتية للاتصالات بين النظام المركزي والأنظمة الوطنية. ويشتمل نظام معلومات شنغن المركزي على بيانات معينة أدخلتها الدول الأعضاء عن الأشخاص والأشياء. ويتم استخدام نظام معلومات شنغن من قبل سلطات مراقبة الحدود الوطنية والشرطة والجمارك والتأشيرات والسلطات القضائية في جميع أنحاء منطقة شنغن. وتقوم كل دولة من الدول الأعضاء بتشغيل نسخة وطنية من نظام معلومات شنغن المركزي، والمعروفة باسم أنظمة معلومات شنغن الوطنية، والتي يتم تحديثها باستمرار، وبالتالي تحديث نظام معلومات شنغن المركزي. وهناك أنواع مختلفة من التنبيهات في نظام معلومات شنغن:

- لا يحق للشخص الدخول إلى أراضي منطقة شنغن أو الإقامة فيها؛ أو
- يكون الشخص أو الشيء مبحوثاً عنه من قبل السلطات القضائية أو سلطات إنفاذ القانون (مثل مذكرات التوقيف الأوروبية، وطلبات الفحص السري)؛ أو
- تم الإبلاغ عن اختفاء الشخص؛ أو
- تم الإبلاغ عن سلع، مثل الأوراق النقدية والسيارات والشاحنات الصغيرة والأسلحة النارية والوثائق التعريفية، على أنها ممتلكات مسروقة أو مفقودة.

عندما يكون هناك تنبيه، يتم الشروع في أنشطة متابعة من خلال مكاتب طلبات المعلومات التكميلية عند الإدخالات الوطنية. هذا ويشمل الجيل الثاني من نظام معلومات شنغن وظائف جديدة من قبيل إمكانية إدخال: البيانات البيومترية كبصمات الأصابع والصور؛ أو فئات جديدة من التنبيهات، كالسفن والطائرات والحاويات أو وسائل الدفع المسروقة؛ والتنبيهات المعززة حول الأشخاص والأغراض؛ ونسخ من مذكرات التوقيف الأوروبية الخاصة بالأشخاص المطلوب القبض عليهم أو تسليمهم أو ترحيلهم.

ويرتكز الجيل الثاني من نظام معلومات شنغن على صكين يكمل كل منهما الأخرى: القرار الخاص بالجيل الثاني من نظام معلومات شنغن 850 واللائحة الخاصة بالجيل الثاني من نظام معلومات شنغن.[851] وقد استخدم مشرع الاتحاد الأوروبي أساساً قانونياً مختلفاً لاعتماد القرار واللائحة. حيث ينظم القرار استخدام الجيل الثاني من نظام معلومات شنغن للأغراض التي يشملها التعاون بين الشرطة والقضاء في المسائل الجنائية (الركيزة الثالثة للاتحاد الأوروبي سابقاً)، بينما تنطبق اللائحة على إجراءات التنبيه التي تندرج ضمن المسائل الخاصة بالتأشيرات واللجوء

---

[846] اتفاق بين حكومات دول اتحاد البنلوكس الاقتصادي ، وجمهورية ألمانيا الاتحادية، والجمهورية الفرنسية بشأن الإلغاء التدريجي لعمليات التحقق على حدودها المشتركة، الجريدة الرسمية 239 L 2000 OJ.

[847] الجماعات الأوروبية (1997)، معاهدة أمستردام المعدلة لمعاهدة الاتحاد الأوروبي، والمعاهدات المؤسسة للجماعات الأوروبية وبعض القوانين ذات الصلة، الجريدة الرسمية OJ C 340 1997.

[848] تقوم كرواتيا وقبرص وأيرلندا بأنشطة تحضيرية للاندماج في الجيل الثاني من نظام معلومات شنغن، لكنها لم تصبح بعد جزءاً فيه. انظر المعلومات الخاصة بنظام معلومات شنغن المتاحة على الموقع الإلكتروني للمديرية العامة للهجرة والشؤون الداخلية التابعة للمفوضية الأوروبية.

[849] اللائحة (الجماعة الأوروبية) رقم 1987/2006 للبرلمان الأوروبي والمجلس بتاريخ 20 ديسمبر 2006 بشأن وضع وتشغيل واستخدام الجيل الثاني من نظام معلومات شنغن، الجريدة الرسمية II SIS) 381 L 2006 OJ) ومجلس الاتحاد الأوروبي (2007)، قرار المجلس JHA/2007/533 بتاريخ 12 يونيو 2007 بشأن وضع وتشغيل واستخدام الجيل الثاني من نظام معلومات شنغن، الجريدة الرسمية 205 L 2007 OJ.

[850] قرار المجلس JHA/2007/533 بتاريخ 12 يونيو 2007 بشأن وضع وتشغيل واستخدام الجيل الثاني من نظام معلومات شنغن، الجريدة الرسمية7 ، 205 L أغسطس 2007.

[851] اللائحة (الجماعة الأوروبية) رقم1987/2006 الصادرة عن البرلمان الأوروبي والمجلس بتاريخ 20 ديسمبر 2006 بشأن وضع وتشغيل واستخدام الجيل الثاني من نظام معلومات شنغن، الجريدة الرسمية28 ، 381 L OJ ديسمبر 2006.

والهجرة وغيرها من السياسات المتعلقة بحرية تنقل الأشخاص (الركيزة الأولى سابقاً). ووجب تنظيم إجراءات التنبيه لكل ركيزة من خلال قوانين منفصلة، نظراً إلى أن الصكين القانونيين قد تم اعتمادهما قبل معاهدة لشبونة وإلغاء هيكل الركائز.

ويضم كلا الصكين قواعد بشأن حماية البيانات. حيث يحظر القرار الخاص بالجيل الثاني من نظام معلومات شنغن معالجة البيانات الحساسة،[852] فيما ينبغي أن تدخل معالجة البيانات الشخصية ضمن نطاق الاتفاقية 108 المحدثة.[853] علاوة على ذلك، يحق للأشخاص الوصول إلى البيانات الشخصية المتعلقة بهم والتي يتم إدخالها في الجيل الثاني من نظام معلومات شنغن.[854]

وتنظم اللائحة الخاصة بالجيل الثاني من نظام معلومات شنغن الشروط والإجراءات الخاصة بإدخال ومعالجة التنبيهات المتعلقة برفض دخول أو إقامة مواطنين قادمين من خارج الاتحاد الأوروبي. كما تحدد القواعد المتعلقة بتبادل المعلومات التكميلية والإضافية لأغراض الدخول أو الإقامة في دولة عضو.[855] وتشمل هذه اللائحة أيضاً قواعد بشأن حماية البيانات. هذا ولا يُسمح بمعالجة فئات البيانات الحساسة [856] المشار إليها في المادة 9 (1) من اللائحة العامة لحماية البيانات. وتضم اللائحة الخاصة بالجيل الثاني من نظام معلومات شنغن أيضاً حقوقاً خاصة بأصحاب البيانات، وهي:

- الحق في الوصول إلى البيانات الشخصية المتعلقة بصاحب البيانات؛[857]
- الحق في تصحيح البيانات غير الدقيقة وقائعيا؛[858]
- الحق في حذف البيانات المخزنة بطريقة غير مشروعة؛[859]
- الحق في إخبار صاحب البيانات إذا كان هناك تنبيه صادر ضده. ويجب أن يكون هذا الإخطار مكتوبا ومرفقا بنسخة أو إشارة إلى القرار الوطني المتعلق بإصدار التنبيه.[860]

لا ينبغي منح الحق في الإخبار إذا: 1) لم يتم الحصول على البيانات الشخصية من صاحب البيانات وكان تقديم تلك المعلومات مستحيلاً أو يتطلب مجهوداً غير متناسب، 2) كان صاحب البيانات يملك بالفعل المعلومات أو 3) كان القانون الوطني يسمح بفرض قيود على أساس حماية الأمن الوطني أو منع الجرائم الجنائية، من ضمن أمور أخرى.[861]

وبالنسبة لكل من القرار واللائحة الخاصين بالجيل الثاني من نظام معلومات شنغن، يجوز للأفراد ممارسة حقوق الوصول للجيل الثاني من نظام معلومات شنغن في أي دولة عضو، وسيتم التعامل معها وفقاً للقانون الوطني لتلك الدولة العضو.[862]

مثال: في قضية «داليا ضد فرنسا»،[863] مُنع المدعي من الحصول على تأشيرة لزيارة فرنسا، حيث أبلغت السلطات الفرنسية نظام معلومات شنغن أنه ينبغي رفض دخوله. وسعى المدعي دون جدوى إلى الوصول إلى البيانات وتصحيحها أو حذفها أمام لجنة حماية البيانات الفرنسية، ومن ثم أمام مجلس الدولة. وقد رأت المحكمة الأوروبية لحقوق الإنسان أن التبليغ عن المدعي لدى نظام معلومات شنغن كان متوافقاً مع القانون وكان يسعى إلى تحقيق الهدف المشروع المتمثل في حماية الأمن الوطني. ونظراً لأن المدعي لم يُثبت الآثار السلبية الناتجة عن رفض دخوله إلى منطقة شنغن، وبما أنه تم اتخاذ تدابير كافية لحمايته من القرارات التعسفية، فإن التدخل في حقه في احترام الحياة الخاصة كان متناسباً. وهكذا قضت المحكمة أن شكاية المدعي بموجب المادة 8 غير مقبولة.

[852] القرار الخاص بالجيل الثاني من نظام معلومات شنغن، المادة 56؛ اللائحة الخاصة بالجيل الثاني من نظام معلومات شنغن، المادة 40.
[853] القرار الخاص بالجيل الثاني من نظام معلومات شنغن، المادة 57.
[854] القرار الخاص بالجيل الثاني من نظام معلومات شنغن، المادة 58؛ اللائحة الخاصة بالجيل الثاني من نظام معلومات شنغن، المادة 41.
[855] اللائحة الخاصة بالجيل الثاني من نظام معلومات شنغن، المادة 2.
[856] نفس المرجع السابق، المادة 40.
[857] نفس المرجع السابق، المادة 41 (1).
[858] نفس المرجع السابق، المادة 41 (5).
[859] نفس المرجع السابق، المادة 41 (5).
[860] نفس المرجع السابق، المادة 42 (1).
[861] نفس المرجع السابق، المادة 42 (2).
[862] اللائحة الخاصة بالجيل الثاني من نظام معلومات شنغن، المادة 41 (1) والقرار الخاص بالجيل الثاني من نظام معلومات شنغن، المادة 58.
[863] المحكمة الأوروبية لحقوق الإنسان، قضية «داليا ضد فرنسا»، رقم 964/07، 2 فبراير 2010.

تشرف الهيئة الإشرافية الوطنية المختصة في كل دولة عضو على نظام معلومات شنغن الوطني. ويتعين على الهيئة الإشرافية الوطنية أن تضمن إجراء تدقيق لعمليات معالجة البيانات داخل نظام معلومات شنغن الوطني كل أربع سنوات على الأقل.[864] وتتعاون الهيئات الإشرافية الوطنية مع المشرف الأوروبي على حماية البيانات وتضمن الإشراف المنسق على نظام معلومات شنغن الوطني، بينما يتولى المشرف الأوروبي على حماية البيانات مسؤولية الإشراف على نظام معلومات شنغن المركزي. وحرصاً على الشفافية، يجب إرسال تقرير مشترك عن الأنشطة إلى كل من البرلمان الأوروبي والمجلس ووكالة الاتحاد الأوروبي للإدارة التشغيلية لأنظمة تكنولوجيا المعلومات واسعة النطاق في مجال الحرية والأمن والعدالة كل سنتين. وقد تم إحداث مجموعة تنسيق الإشراف الخاصة بالجيل الثاني من نظام معلومات شنغن لضمان تنسيق الإشراف على مستوى النظام وتجتمع في حدود المرتين سنوياً.

وتتألف هذه المجموعة من المشرف الأوروبي على حماية البيانات وممثلي الهيئات الإشرافية للدول الأعضاء التي طبقت الجيل الثاني من نظام معلومات شنغن، إلى جانب أيسلندا وليختنشتاين والنرويج وسويسرا، نظراً لكون نظام معلومات شنغن ينطبق عليها أيضاً، ولكونها من بين أعضاء شنغن.[865] من جهتها، فإن قبرص وكرواتيا وأيرلندا لم تصبح بعد جزءاً من الجيل الثاني من نظام معلومات شنغن، وبالتالي فهي تشارك فقط بصفتها دول مراقبة في مجموعة تنسيق الإشراف. وفي سياق مجموعة تنسيق الإشراف، يتعاون المشرف الأوروبي على حماية البيانات فعلياً مع الهيئات الإشرافية الوطنية ، من خلال تبادل المعلومات وتقديم المساعدة المتبادلة في إجراء عمليات التدقيق والتفتيش وإعداد مقترحات منسقة لحلول مشتركة للمشاكل المحتملة وتعزيز الوعي بحقوق حماية البيانات.[866] هذا وقد اعتمدت مجموعة تنسيق الإشراف التابعة للجيل الثاني من نظام معلومات شنغن إرشادات لمساعدة أصحاب البيانات. ولعل أحد الأمثلة على ذلك هو الدليل الصادر لمساعدة أصحاب البيانات في ممارسة حقوقهم المتعلقة بالوصول.[867]

**الآفاق**

في 2016، أجرت المفوضية الأوروبية تقييماً لنظام معلومات شنغن[868] والذي أظهر أنه تم وضع آليات وطنية لتمكين أصحاب البيانات من الوصول إلى بياناتهم الشخصية وتصحيحها وحذفها في الجيل الثاني من نظام معلومات شنغن أو الحصول على تعويض فيما يتعلق بالبيانات غير الدقيقة. ولتحسين كفاءة الجيل الثاني من نظام معلومات شنغن وفعاليته، اقترحت المفوضية الأوروبية ثلاث لوائح:

- لائحة خاصة بوضع وتشغيل واستخدام نظام معلومات شنغن في مجال عمليات التفتيش على الحدود، والتي ستلغي لائحة الجيل الثاني من نظام معلومات شنغن؛
- لائحة خاصة بوضع وتشغيل واستخدام نظام معلومات شنغن في مجال تعاون الشرطة والتعاون القضائي في المسائل الجنائية، التي ستلغي من ضمن أمور أخرى، القرار الخاص بالجيل الثاني من نظام معلومات شنغن؛ و
- لائحة خاصة باستخدام نظام معلومات شنغن لعودة رعايا الدول الثالثة المقيمين بشكل غير قانوني.

وتجدر الإشارة إلى أن المقترحات تسمح بمعالجة فئات أخرى من البيانات البيومترية - بالإضافة إلى الصور وبصمات الأصابع، والتي هي بالفعل جزء من الجيل الثاني من نظام معلومات شنغن الحالي. وسيتم أيضاً تخزين بصمات الوجه وبصمات الكف وملفات تعريف الحمض النووي في قاعدة بيانات نظام معلومات شنغن. بالإضافة إلى ذلك، بينما تنص اللائحة والقرار الخاصين بالجيل الثاني من نظام معلومات شنغن على إمكانية البحث باستخدام بصمات الأصابع لتحديد هوية الشخص، فإن المقترحات تجعل هذا البحث إلزامياً إذا كان لا يمكن التحقق من هوية الشخص بأي طريقة أخرى. وسيتم استخدام صور الوجه والصور الفوتوغرافية وبصمات الكف للبحث في النظام وتحديد هوية الأشخاص، حين يصير ذلك ممكناً من الناحية التقنية. وتشكل القواعد الجديدة المتعلقة بالسمات البيومترية مخاطر معينة على حقوق الأفراد. فقد لاحظ المشرف الأوروبي على حماية البيانات في رأيه حول مقترحات اللجنة[869] أن البيانات البيومترية حساسة للغاية وأن إدخالها في

---

[864] اللائحة الخاصة بالجيل الثاني من نظام معلومات شنغن، المادة 60 (2).

[865] انظر الصفحة الإلكترونية للمشرف الأوروبي على حماية البيانات حول نظام معلومات شنغن.

[866] اللائحة الخاصة بالجيل الثاني من نظام معلومات شنغن، المادة 46؛ القرار الخاص بالجيل الثاني من نظام معلومات شنغن، المادة 62.

[867] انظر مجموعة تنسيق الإشراف التابعة للجيل الثاني من نظام معلومات شنغن. دليل ممارسة حق الوصول، متاح على موقع المشرف الأوروبي على حماية البيانات.

[868] المفوضية الأوروبية (2016)، تقرير من المفوضية إلى البرلمان الأوروبي والمجلس بشأن تقييم الجيل الثاني من نظام معلومات شنغن وفقاً للمادة 24 (5) و43 (3) و50 (5) من اللائحة (الجماعة الأوروبية) رقم 1987/2006 والمادة 59 (3) و66 (5) من القرار JHA/2007/533 ، النسخة النهائية 880 (2016)COM ، بروكسل، 21 ديسمبر 2016-

[869] المشرف الأوروبي على حماية البيانات (2017)، رأي المشرف الأوروبي على حماية البيانات بشأن الأساس القانوني الجديد لنظام معلومات شنغن، الرأي 7/2017، 2 مايو 2017.

قاعدة بيانات كبيرة يجب أن يعتمد على تقييم يرتكز على أدلة تثبت الحاجة إلى تضمينها في نظام معلومات شنغن. بمعنى آخر، يجب إثبات ضرورة معالجة السمات الجديدة. كما اعتبر المشرف الأوروبي على حماية البيانات أن هناك حاجة لمزيد من التوضيح فيما يتعلق بنوع المعلومات التي يمكن تضمينها في ملف تعريف الحمض النووي. ونظراً لأن ملف تعريف الحمض النووي يمكن أن يتضمن معلومات حساسة (ولعل أبرز مثال على ذلك هو الكشف عن المشاكل الصحية)، فإنه ينبغي أن تضم ملفات تعريف الحمض النووي المخزنة في نظام معلومات شنغن «الحد الأدنى فقط من المعلومات الضرورية للغاية لتحديد هوية الأشخاص المفقودين والاستبعاد بشكل صريح للمعلومات الصحية والمتعلقة بالأصل العرقي وأي معلومات حساسة أخرى».[870] ومع ذلك، تضع المقترحات ضمانات إضافية للحد من جمع البيانات ومعالجتها لما هو ضروري للغاية ومطلوب للتشغيل، ويقتصر الوصول إليها على الأشخاص الذين لديهم حاجة تشغيلية لمعالجة البيانات الشخصية.[871] وتمكّن هذه المقترحات أيضاً وكالة الاتحاد الأوروبي للإدارة التشغيلية لأنظمة تكنولوجيا المعلومات واسعة النطاق في مجال الحرية والأمن والعدالة من إصدار التقارير المتعلقة بجودة البيانات للدول الأعضاء على مدى فترات منتظمة، من أجل مراجعة التنبيهات بانتظام لضمان جودة البيانات.

**نظام معلومات التأشيرات**

تم تطوير نظام معلومات التأشيرات، الذي تديره أيضاً وكالة الاتحاد الأوروبي للإدارة التشغيلية لأنظمة تكنولوجيا المعلومات واسعة النطاق في مجال الحرية والأمن والعدالة، لدعم تنفيذ سياسة تأشيرة الاتحاد الأوروبي المشتركة.[873] ويسمح نظام معلومات التأشيرات لدول منطقة شنغن بتبادل البيانات المتعلقة بمقدمي طلبات الحصول على التأشيرة من خلال نظام مركزي بالكامل يربط قنصليات وسفارات دول شنغن الواقعة في دول خارج الاتحاد الأوروبي بنقاط العبور الحدودية الخارجية لجميع دول شنغن. ويعالج نظام معلومات التأشيرات البيانات المتعلقة بطلبات الحصول على تأشيرات الإقامة القصيرة للزيارة أو للمرور عبر منطقة شنغن. ويمكّن نظام معلومات التأشيرات سلطات الحدود من التحقق، بمساعدة السمات البيومترية ولا سيما بصمات الأصابع، مما إذا كان الشخص الذي يقدم التأشيرة هو صاحبها المشروع أم لا، وتحديد الأشخاص الذين ليس لديهم مستندات أو الذين يملكون وثائق مزورة.

تنظم اللائحة (الجماعة الأوروبية) رقم767/2008 للبرلمان الأوروبي والمجلس بشأن نظام معلومات التأشيرات وتبادل البيانات بين الدول الأعضاء بشأن تأشيرات الإقامة القصيرة (اللائحة الخاصة بنظام معلومات التأشيرات) شروط وإجراءات نقل البيانات الشخصية المتعلقة بطلبات الحصول على تأشيرات الإقامة القصيرة. كما تراقب القرارات المتخذة بشأن الطلبات، بما في ذلك قرارات إلغاء التأشيرة أو إبطالها أو تمديدها.[874] وتشمل اللائحة الخاصة بنظام معلومات التأشيرات بشكل أساسي البيانات المتعلقة بمقدم الطلب، وتأشيراته، وصوره، وبصمات أصابعه، وروابط طلباته السابقة، وملفات طلبات الأشخاص المرافقين له، أو البيانات المتعلقة بالأشخاص الذين يدعونه.[875] ويقتصر الوصول إلى نظام معلومات التأشيرات من أجل إدخال البيانات أو تعديلها أو حذفها حصرياً على سلطات التأشيرات، في حين يتم تخويل إمكانية الاطلاع على البيانات لسلطات التأشيرات والسلطات المختصة بالتحقق في نقاط عبور الحدود الخارجية والتفتيش الخاص بالهجرة واللجوء.

في ظل ظروف معينة، قد تطلب سلطات الشرطة الوطنية المختصة واليوروبول الوصول إلى البيانات المدخلة في نظام معلومات التأشيرات لغرض منع الجرائم الإرهابية والجنائية أو الكشف عنها أو التحقيق فيها.[876] ونظراً لكون نظام معلومات التأشيرات قد صمم كأداة

---

[870] نفس المرجع السابق، الفقرة 22.

[871] المفوضية الأوروبية (2016)، مقترح لائحة للبرلمان الأوروبي والمجلس بشأن وضع وتشغيل واستخدام نظام معلومات شنغن في مجال تعاون الشرطة والتعاون القضائي في المسائل الجنائية، المعدل للائحة (الاتحاد الأوروبي) رقم515/2014 والملغي للائحة (الجماعة الأوروبية) رقم 1986/2006، قرار المجلس رقم JHA/2007/533 وقرار المفوضية 2010/261/EU، النسخة النهائية883 (2016)COM ، بروكسل، 21 ديسمبر 2016.

[872] نفس المرجع السابق، الفقرة 15.

[873] مجلس الاتحاد الأوروبي (2004)، قرار المجلس EC/2004/512 بتاريخ 8 يونيو 2004 بشأن وضع نظام معلومات التأشيرات، الجريدة الرسمية213 L 2004 OJ ؛ اللائحة (الجماعة الأوروبية) رقم767/2008 الصادرة عن البرلمان الأوروبي والمجلس في 9 يوليو 2008 بشأن نظام معلومات التأشيرات وتبادل البيانات بين الدول الأعضاء بشأن تأشيرات الإقامة القصيرة، الجريدة الرسمية218 L 2008 OJ (اللائحة الخاصة بنظام معلومات التأشيرات)؛ مجلس الاتحاد الأوروبي (2008)، قرار المجلس JHA/2008/633 بتاريخ 23 يونيو 2008 بشأن الوصول للاطلاع على نظام معلومات التأشيرات من قبل السلطات المعينة في الدول الأعضاء ومن قبل اليوروبول لأغراض منع الجرائم الإرهابية والجرائم الجنائية الخطيرة الأخرى والكشف عنها والتحقيق فيها، الجريدة الرسمية 218 L 2008 OJ.

[874] اللائحة الخاصة بنظام معلومات التأشيرات، المادة 1.

[875] المادة 5 من اللائحة (الجماعة الأوروبية) رقم 767/2008 للبرلمان الأوروبي والمجلس بتاريخ 9 يوليو 2008 بشأن نظام معلومات التأشيرات وتبادل البيانات بين الدول الأعضاء بشأن تأشيرات الإقامة القصيرة (اللائحة الخاصة بنظام معلومات التأشيرات)، الجريدة الرسمية 218 L 2008 OJ.

[876] مجلس الاتحاد الأوروبي (2008)، قرار المجلس JHA/2008/633 بتاريخ 23 يونيو 2008 بشأن اطلاع السلطات المعينة في الدول الأعضاء واليوروبول على نظام معلومات التأشيرات لأغراض منع الجرائم الإرهابية والجرائم الجنائية الخطيرة الأخرى والكشف عنها والتحقيق فيها، الجريدة الرسمية 218 L 2008 OJ.

لدعم تنفيذ سياسة التأشيرات المشتركة، فإن مبدأ حصر الغرض الذي، كما هو موضح في الفصل 2.3، يتطلب معالجة البيانات الشخصية فقط لأغراض محددة، وواضحة ومشروعة، ويجب أن تكون البيانات الشخصية ملائمة وذات صلة وغير مبالغ فيها فيما يتعلق بالأغراض التي تتم معالجتها من أجلها، وسيقع انتهاك هذا المبدأ إذا تم تحويل نظام معلومات التأشيرات إلى أداة لإنفاذ القانون.

لهذا السبب، لا يتم منح سلطات إنفاذ القانون الوطنية واليوروبول وصولاً روتينياً إلى قاعدة بيانات نظام معلومات التأشيرات، ولا يجوز تخويل حق الوصول إلا على أساس كل حالة على حدة ويكون محصوراً بضمانات صارمة. وقد تم تنظيم شروط وضمانات الوصول إلى نظام معلومات التأشيرات والاطلاع عليه من قبل هذه السلطات في قرار المجلس JHA/2008/633.[877]

علاوة على ذلك، تنص اللائحة الخاصة بنظام معلومات التأشيرات على حقوق أصحاب البيانات، وهي:

- الحق في الإخبار من قبل الدولة العضو المسؤولة بهوية ومعلومات الاتصال الخاصة بمراقب البيانات المسؤول عن معالجة البيانات الشخصية داخل تلك الدولة العضو، والأغراض التي ستتم معالجة بياناتهم الشخصية من أجلها داخل نظام معلومات التأشيرات، وفئات الأشخاص الذين يمكن نقل البيانات إليهم (الجهات المتلقية) وفترة الاحتفاظ بالبيانات. بالإضافة إلى ذلك، يجب إبلاغ المتقدمين للحصول على التأشيرات بأن جمع بياناتهم الشخصية بموجب نظام معلومات التأشيرات إلزامي لدراسة طلباتهم، بينما يجب على الدول الأعضاء أيضاً إبلاغهم بحقهم في الوصول إلى بياناتهم، وطلب تصحيحها أو حذفها، وبالإجراءات التي تمكنهم من ممارسة هذه الحقوق.[878]
- الحق في الوصول إلى البيانات الشخصية المتعلقة بهم والتي تم تسجيلها في نظام معلومات التأشيرات.[879]
- الحق في تصحيح البيانات الخاطئة.[890]
- الحق في حذف البيانات المخزنة بشكل غير مشروع.[881]

لضمان الإشراف على نظام معلومات التأشيرات، تم إنشاء فريق تنسيق الإشراف على نظام معلومات التأشيرات (VIS SCG)، وهو يتألف من ممثلين عن المشرف الأوروبي على حماية البيانات والهيئات الإشرافية الوطنية، والذين يجتمعون مرتين في السنة. ويتكون هذا الفريق من ممثلي 28 دولة عضو في الاتحاد الأوروبي ومن أيسلندا وليختنشتاين والنرويج وسويسرا.

**النظام الأوروبي لمضاهاة بصمات الأصابع (يوروداك)**

النظام الأوروبي لمضاهاة بصمات الأصابع («يوروداك»)[882] هو نظام مركزي يحتوي على بيانات بصمات الأصابع لمواطني البلدان الثالثة والأشخاص عديمي الجنسية الذين يتقدمون بطلب للحصول على اللجوء في إحدى الدول الأعضاء في الاتحاد الأوروبي.[883] وقد بدأ تشغيل النظام منذ يناير 2003، باعتماد لائحة المجلس 2725/2000؛ ثم أصبحت إعادة صياغة حديثة له سارية في عام 2015. إن الغرض من هذا النظام في المقام الأول هو المساعدة على تحديد الدولة العضو التي ينبغي أن تكون مسؤولة عن فحص طلب لجوء معين بموجب اللائحة (الجماعة الأوروبية) 604/2013. وتحدد هذه اللائحة المعايير والآليات لتحديد الدولة العضو المسؤولة عن فحص طلب الحماية الدولية المقدم في إحدى الدول الأعضاء من قبل مواطن من بلد ثالث أو شخص عديم الجنسية (لائحة دبلن الثالثة).[884] تخدم البيانات الشخصية الواردة في نظام «يوروداك» بشكل أساسي غرض تسهيل تطبيق لائحة دبلن الثالثة.[885] يُسمح لسلطات إنفاذ القانون الوطنية واليوروبول

[877] نفس المرجع السابق.

[878] اللائحة الخاصة بنظام معلومات التأشيرات، المادة 37.

[879] نفس المرجع السابق، المادة 38 (1).

[880] نفس المرجع السابق، المادة 38 (2).

[881] نفس المرجع السابق، المادة 38 (2).

[882] انظر صفحة الويب الخاصة بالمشرف الأوروبي على حماية البيانات على موقع «يوروداك».

[883] لائحة المجلس (الجماعة الأوروبية) رقم 2725/2000 المؤرخة في 11 ديسمبر 2000 بشأن إنشاء نظام «يوروداك» لمضاهاة بصمات الأصابع من أجل التطبيق الفعال لاتفاقية دبلن، الجريدة الرسمية 316 L 2000 OJ؛ لائحة المجلس (الجماعة الأوروبية) رقم 407/2002 المؤرخة في 28 فبراير 2002 المحدّدة لقواعد معينة لتنفيذ اللائحة (الجماعة الأوروبية) رقم 2725/2000 المتعلقة بإنشاء نظام «يوروداك» لمضاهاة بصمات الأصابع من أجل التطبيق الفعال لاتفاقية دبلن، الجريدة الرسمية 62 L 2002 OJ (لوائح «يوروداك»)، اللائحة (الاتحاد الأوروبي) رقم 603/2013 الصادرة عن البرلمان الأوروبي والمجلس بتاريخ 26 يونيو 2013 بشأن إنشاء نظام «يوروداك» لمضاهاة بصمات الأصابع من أجل التطبيق الفعال للائحة (الاتحاد الأوروبي) رقم 604/2013 المؤسّسة للمعايير والآليات لتحديد الدولة العضو المسؤولة عن فحص طلب الحماية الدولية المقدّم في إحدى الدول الأعضاء من قبل مواطن من بلد ثالث أو شخص عديم الجنسية وبناءً على طلبات المقارنة مع بيانات «يوروداك» من قبل سلطات إنفاذ القانون للدول الأعضاء واليوروبول لأغراض إنفاذ القانون، والمعدّلة اللائحة (الاتحاد الأوروبي) رقم 1077/2011 المؤسّسة لوكالة أوروبية للإدارة التشغيلية لنظم تكنولوجيا المعلومات واسعة النطاق في مجال الحرية والأمن والعدالة، الجريدة الرسمية 180 L 2013 OJ، ص. 1 (لائحة «يوروداك» المعاد صياغتها).

[884] اللائحة (الاتحاد الأوروبي) رقم 604/2013 الصادرة عن البرلمان الأوروبي والمجلس في 26 يونيو 2013 المحدّدة لمعايير وآليات تحديد الدولة العضو المسؤولة عن فحص طلب الحماية الدولية المقدم في إحدى الدول الأعضاء من قبل مواطن من بلد ثالث أو شخص عديم الجنسية، الجريدة الرسمية 180 L 2013 OJ (لائحة دبلن الثالثة).

[885] لائحة «يوروداك» المعاد صياغتها، الجريدة الرسمية 180 L 2013 OJ، ص. 1، المادة 1 (1).

بمضاهاة بصمات الأصابع المرتبطة بالتحقيقات الجنائية مع البصمات الواردة في نظام «يوروداك»، ولكن فقط لغرض منع الجرائم الإرهابية أو الجرائم الجنائية الخطيرة الأخرى والكشف عنها والتحقيق فيها. ونظراً لأنه تم تصميم «يوروداك» كأداة لدعم تنفيذ سياسة اللجوء في الاتحاد الأوروبي، وليس كأداة لإنفاذ القانون، فإن سلطات إنفاذ القانون لديها إمكانية الوصول إلى قاعدة البيانات هذه فقط في حالات محددة وفي ظل ظروف محددة وشروط صارمة.[886] وعندما ينبغي استخدام البيانات لأغراض أخرى متعلقة بإنفاذ القانون، يتم تطبيق الأمر التوجيهي المتعلق بحماية البيانات الموجه للشرطة وسلطات العدالة الجنائية، في حين أن البيانات المستخدمة للغرض الرئيسي المتمثل في تسهيل تنفيذ لائحة دبلن الثالثة محمية بموجب اللائحة العامة لحماية البيانات. يُحظر القيام بأي نقل إضافي للبيانات الشخصية التي حصلت عليها دولة عضو أو اليوروبول وفقاً للائحة «يوروداك» المعاد صياغتها إلى أي دولة ثالثة أو منظمة دولية أو جهة خاصة يوجد مقرها في الاتحاد الأوروبي أو خارجه.[887]

يتكون نظام «يوروداك» من وحدة مركزية، تديرها وكالة الاتحاد الأوروبي للإدارة التشغيلية لأنظمة تكنولوجيا المعلومات واسعة النطاق في مجال الحرية والأمن والعدالة (eu-LISA)، لتخزين ومضاهاة بصمات الأصابع، ونظام لنقل البيانات الإلكترونية بين الدول الأعضاء وقاعدة البيانات المركزية. تأخذ الدول الأعضاء وتنقل بصمات أصابع كل شخص يبلغ من العمر 14 عاماً على الأقل يطلب اللجوء في أراضيها، وأيضاً بصمات كل شخص من خارج الاتحاد الأوروبي أو شخص عديم الجنسية يبلغ من العمر 14 عاماً على الأقل تم القبض عليه بسبب العبور غير المسموح به لحدودها الخارجية. هذا ويجوز للدول الأعضاء أيضاً أن تأخذ وتنقل بصمات أصابع المواطنين من خارج الاتحاد الأوروبي أو الأشخاص عديمي الجنسية الذين يتم العثور عليهم داخل أراضيها بدون ترخيص.

على الرغم من أنه يمكن لأي دولة عضو الالتجاء إلى نظام «يوروداك» وطلب مقارنات مع بيانات بصمات الأصابع، فإن الدولة العضو التي جمعت البصمات وأرسلتها إلى الوحدة المركزية وحدها لها الحق في تعديل البيانات، وذلك إما عن طريق تصحيحها أو استكمالها أو محوها.[888] وتحتفظ وكالة الاتحاد الأوروبي للإدارة التشغيلية لأنظمة تكنولوجيا المعلومات واسعة النطاق في مجال الحرية والأمن والعدالة بسجلات لجميع عمليات معالجة البيانات لمراقبة حماية البيانات ولضمان أمن البيانات.[889] وتساعد الهيئات الإشرافية الوطنية أصحاب البيانات وتقدم لهم المشورة بشأن ممارسة حقوقهم.[890] يخضع جمع بيانات البصمات ونقلها للمراجعة القضائية من قبل المحاكم الوطنية. كما تنطبق كل من لائحة حماية البيانات الخاصة بمؤسسات الاتحاد الأوروبي وإشراف المشرف[892] الأوروبي على حماية البيانات على أنشطة المعالجة الخاصة بالنظام المركزي، والتي تديرها وكالة الاتحاد الأوروبي للإدارة التشغيلية لأنظمة تكنولوجيا المعلومات واسعة النطاق في مجال الحرية والأمن والعدالة فيما يتعلق بـ»يوروداك».[893] وإذا تعرض شخص لضرر نتيجة لعملية معالجة غير مشروعة، أو من أي عمل لا يتوافق مع لائحة «يوروداك»، فيحق لذلك الشخص الحصول على تعويض من الدولة العضو المسؤولة عن الضرر.[894] ولكن يجب التأكيد على أن طالبي اللجوء هم فئة هشة معرضة للخطر بشكل خاص وغالباً ما يكونوا قد قاموا برحلات طويلة ومحفوفة بالمخاطر. وبسبب وضعهم الهش وحالة عدم الاستقرار التي يمرون بها في كثير من الأحيان أثناء النظر في طلب اللجوء الخاص بهم، فإن ممارستهم لحقوقهم، بما في ذلك الحق في التعويض، قد تكون صعبة من الناحية العملية.

لاستخدام قاعدة بيانات «يوروداك» لأغراض إنفاذ القانون، يجب على الدول الأعضاء تعيين السلطات التي سيكون لها الحق في طلب الوصول إليها، وكذلك السلطات التي ستتحقق من أن طلبات المقارنة مشروعة.[895] ويخضع وصول السلطات الوطنية واليوروبول إلى بيانات بصمات «يوروداك» لشروط صارمة للغاية. إذ يجب على السلطة الطالبة تقديم طلب إلكتروني مُعلَّل فقط بعد أن تقوم بمقارنة البيانات مع

[886] نفس المرجع السابق، المادة 1 (2).
[887] نفس المرجع السابق، المادة 35.
[888] نفس المرجع السابق، المادة 27.
[889] نفس المرجع السابق، المادة 28.
[890] نفس المرجع السابق، المادة 29.
[891] نفس المرجع السابق، المادة 29.
[892] اللائحة (الجماعة الأوروبية) رقم 45/2001 للبرلمان الأوروبي والمجلس المؤرخة في 18 ديسمبر 2000 المتعلقة بحماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية من قبل مؤسسات وهيئات الجماعة الأوروبية وحرية حركة هذه البيانات، الجريدة الرسمية 8 L 2001 0J.
[893] لائحة «يوروداك» المعاد صياغتها، الجريدة الرسمية 180 L 2013 0J، ص. 1، المادة 31.
[894] نفس المرجع السابق، المادة 37.
[895] روتس، ل. (2015)، 'لائحة يوروداك الجديدة: بصمات الأصابع كمصدر للتمييز غير الرسمي'، مجلة البلطيق للدراسات الأوروبية التابعة لجامعة تالين للتكنولوجيا، المجلد 5، رقم 2، الصفحات 129-108.

تلك الموجودة في أنظمة المعلومات الأخرى المتاحة، مثل قواعد بيانات بصمات الأصابع الوطنية و نظام معلومات التأشيرات. ويجب أن يكون هناك شاغل طاغٍ متعلق بالأمن العام يضفي على عملية المقارنة صفة التناسب. كما يجب أن تكون المقارنة ضرورية حقاً، وأن تتعلق بحالة معينة، ويجب أن تكون هناك أسباب معقولة للاعتقاد بأن المقارنة ستسهم بشكل كبير في منع أي من الجرائم الجنائية المعنية أو الكشف عنها أو التحقيق فيها، ولا سيما عندما يكون هناك اشتباه مدعوم بأدلة أن المشتبه به أو الجاني أو الضحية في جريمة إرهابية أو جريمة جنائية خطيرة أخرى يندرج ضمن فئة تخضع لجمع البصمات داخل نظام «يوروداك». هذا ويجب إجراء المقارنة فقط باستخدام بيانات بصمات الأصابع. ويجب أن يحصل اليوروبول أيضاً على تصريح من الدولة العضو التي جمعت بيانات بصمات الأصابع.

يتم الاحتفاظ بالبيانات الشخصية المخزنة في «يوروداك» والمتعلقة بطلبات اللجوء لمدة 10 سنوات من تاريخ أخذ بصمات الأصابع، ما لم يحصل صاحب البيانات على جنسية دولة عضو في الاتحاد الأوروبي. أما إذا حصل على الجنسية، فيتعين محو بياناته على الفور. ويتم تخزين البيانات المتعلقة بالأجانب الذين تم القبض عليهم بسبب عبور الحدود الخارجية غير المسموح به لمدة 18 شهراً. ويتعين محو هذه البيانات على الفور إذا تلقى صاحب البيانات تصريح إقامة أو غادر أراضي الاتحاد الأوروبي أو حصل على جنسية دولة عضو. وتظل بيانات الأشخاص الذين مُنحوا اللجوء متاحة للمقارنة في سياق منع الجرائم الإرهابية وغيرها من الجرائم الجنائية الخطيرة والكشف عنها والتحقيق فيها لمدة ثلاث سنوات.

بالإضافة إلى جميع الدول الأعضاء في الاتحاد الأوروبي، تطبق أيسلندا والنرويج وليختنشتاين وسويسرا أيضاً نظام «يوروداك» استناداً إلى اتفاقات دولية.

وقد تم إنشاء فريق تنسيق الإشراف على نظام «يوروداك» (Eurodac SCG) لضمان الإشراف على هذا النظام. وهو يتألف من ممثلين عن المشرف الأوروبي على حماية البيانات والهيئات الإشرافية الوطنية، والذين يجتمعون مرتين في السنة. و يتكون هذا الفريق من ممثلي 28 دولة عضو في الاتحاد الأوروبي ومن أيسلندا وليختنشتاين والنرويج وسويسرا.[896]

**الآفاق**

في مايو 2016، أصدرت المفوضية اقتراحاً بشأن إعادة صياغة جديدة للائحة «يوروداك»، في إطار إصلاح يهدف إلى تحسين أداء نظام اللجوء الأوروبي المشترك (CEAS).[897] إن إعادة الصياغة المقترحة هذه مهمة، لأنها ستوسع نطاق قاعدة بيانات «يوروداك» الأصلية بشكل كبير. لقد تم إنشاء نظام «يوروداك» في البداية لدعم تنفيذ نظام اللجوء الأوروبي المشترك، وذلك من خلال تقديم أدلة بصمات الأصابع حتى يتسنى تحديد الدولة العضو المسؤولة عن فحص طلب اللجوء المقدم في الاتحاد الأوروبي. وستعمل إعادة الصياغة المقترحة على توسيع نطاق قاعدة بيانات «يوروداك» لتسهيل عودة المهاجرين غير الشرعيين.[898] كما ستكون السلطات الوطنية قادرة على الرجوع إلى قاعدة البيانات لأغراض تحديد مواطني الدول الثالثة الذين يقيمون في الاتحاد الأوروبي بشكل غير نظامي، أو الذين دخلوا الاتحاد الأوروبي بشكل غير نظامي، من أجل الحصول على أدلة لمساعدة الدول الأعضاء على إعادة هؤلاء الأفراد. بالإضافة إلى ذلك، في حين أن النظام القانوني المعمول به حالياً لا يتطلب سوى جمع بصمات الأصابع وتخزينها، فإن الاقتراح يقدم مجموعة من صور وجوه الأفراد المعنيين،[899] والتي تُعد نوعاً آخر من البيانات البيومترية.

[896] انظر صفحة الويب الخاصة بالمشرف الأوروبي على حماية البيانات على موقع «يوروداك».

[897] المفوضية الأوروبية، اقتراح لائحة صادرة عن البرلمان الأوروبي والمجلس بشأن إنشاء نظام «يوروداك» لمضاهاة بصمات الأصابع من أجل التطبيق الفعال لـ[لائحة (الاتحاد الأوروبي) رقم 604/2013 المحدّدة لمعايير وآليات تحديد الدولة العضو المسؤولة عن فحص طلب الحماية الدولية المقدم في إحدى الدول الأعضاء من قبل مواطن من بلد ثالث أو شخص عديم الجنسية]، للتعرف على مواطن من بلد ثالث أو شخص عديم الجنسية مقيم بشكل غير قانوني وبناء على طلبات المقارنة مع بيانات «يوروداك» من قبل سلطات إنفاذ القانون في الدول الأعضاء واليوروبول لأغراض إنفاذ القانون (المعاد صياغتها)، النسخة النهائية 4 ،272 (2016) COM مايو 2016.

[898] انظر المذكرة التفسيرية للمقترح، ص. 3.

[899] المفوضية الأوروبية، اقتراح لائحة صادرة عن البرلمان الأوروبي والمجلس بشأن إنشاء نظام «يوروداك» لمضاهاة بصمات الأصابع من أجل التطبيق الفعال لـ[لائحة (الاتحاد الأوروبي) رقم 604/2013 المحدّدة لمعايير وآليات تحديد الدولة العضو المسؤولة عن فحص طلب الحماية الدولية المقدم في إحدى الدول الأعضاء من قبل مواطن من بلد ثالث أو شخص عديم الجنسية]، للتعرف على مواطن من بلد ثالث أو شخص عديم الجنسية مقيم بشكل غير قانوني وبناء على طلبات المقارنة مع بيانات «يوروداك» من قبل سلطات إنفاذ القانون في الدول الأعضاء واليوروبول لأغراض إنفاذ القانون (المعاد صياغتها)، النسخة النهائية 4 ،272 (2016) COM مايو 2016، المادة 2 (1).

هذا ومن شأن الاقتراح أيضاً تخفيض الحد الأدنى لسن الأطفال الذين يمكن أخذ البيانات البيومترية منهم، وذلك إلى ست سنوات [900] بدلاً من 14 سنة الذي يُعد الحد الأدنى للسن بموجب لائحة سنة 2013. إن النطاق الموسع لهذا الاقتراح يعني أنه سيشكل تدخلاً في حقوق الخصوصية وحماية البيانات لعدد أكبر من الأفراد الذين قد يتم تضمينهم في قاعدة البيانات. ولموازنة هذا التدخل، يسعى الاقتراح والتعديلات التي تقدمت بها لجنة الحريات المدنية والعدالة والشؤون الداخلية (LIBE)[901] بالبرلمان الأوروبي إلى تعزيز متطلبات حماية البيانات. ووقت صياغة هذا الدليل، كانت المناقشات حول الاقتراح جارية في كل من البرلمان والمجلس.

**نظام مراقبة الحدود الأوروبية («يوروسور»)**

تم تصميم نظام مراقبة الحدود الأوروبية («يوروسور»)[902] لتعزيز السيطرة على حدود شنغن الخارجية من خلال الكشف عن الهجرة غير النظامية والجرائم العابرة للحدود ومنعها ومكافحتها. وهو يعمل على تعزيز تبادل المعلومات والتعاون التشغيلي بين مراكز التنسيق الوطنية والوكالة الأوروبية لحرس الحدود والسواحل (فرونتيكس)، وهي وكالة الاتحاد الأوروبي المسؤولة عن تطوير وتطبيق المفهوم الجديد للإدارة المتكاملة للحدود.[903] تتجلى الأهداف العامة لنظام «يوروسور» فيما يلي:

- تقليل عدد المهاجرين غير الشرعيين الذين يدخلون الاتحاد الأوروبي دون أن يتم اكتشافهم؛
- الحد من عدد وفيات المهاجرين غير الشرعيين من خلال إنقاذ المزيد من الأرواح في البحر؛
- زيادة الأمن الداخلي للاتحاد الأوروبي ككل من خلال المساهمة في منع الجريمة العابرة للحدود.[904]

شرع نظام «يوروسور» في العمل في 2 ديسمبر 2013 في جميع الدول الأعضاء ذات الحدود الخارجية، وفي 1 ديسمبر 2014 في بقية الدول الأعضاء. وتنطبق هذه اللائحة على مراقبة الحدود الخارجية البرية والبحرية والجوية للدول الأعضاء. يتبادل نظام «يوروسور» البيانات الشخصية ويعالجها على نطاق محدود للغاية، حيث يحق للدول الأعضاء ووكالة «فرونتيكس» تبادل أرقام تعريف السفن فقط. ويتبادل نظام «يوروسور» المعلومات التشغيلية، مثل موقع الدوريات والحوادث، وكقاعدة عامة، لا يمكن أن تتضمن المعلومات المتبادلة بيانات شخصية.[905] أما في الحالات الاستثنائية التي يتم فيها تبادل البيانات الشخصية في إطار نظام «يوروسور»، فإن اللائحة تنص على أن الإطار القانوني العام للاتحاد الأوروبي بشأن حماية البيانات ينطبق على تلك البيانات بالكامل.[906]

وبالتالي، يضمن نظام «يوروسور» الحق في حماية البيانات، وذلك من خلال الإشارة إلى أن تبادل البيانات الشخصية يجب أن يستوفي المعايير والضمانات التي حددها كل من الأمر التوجيهي المتعلق بحماية البيانات الموجه للشرطة وسلطات العدالة الجنائية واللائحة العامة لحماية البيانات.[907]

---

[900] نفس المرجع السابق، المادة 2 (2).

[901] البرلمان الأوروبي، تقرير حول اقتراح لائحة صادرة عن البرلمان الأوروبي والمجلس بشأن إنشاء نظام «يورودك» لمضاهاة بصمات الأصابع من أجل التطبيق الفعال لـ[لائحة (الاتحاد الأوروبي) رقم 604/2013 المحدّدة لمعايير وآليات تحديد الدولة العضو المسؤولة عن فحص طلب الحماية الدولية المقدم في إحدى الدول الأعضاء من قبل مواطن من بلد ثالث أو شخص عديم الجنسية]، للتعرف على مواطن من بلد ثالث أو شخص عديم الجنسية مقيم بشكل غير قانوني وبناء على طلبات المقارنة مع بيانات «يورودك» من قبل سلطات إنفاذ القانون في الدول الأعضاء واليوروبول لأغراض إنفاذ القانون (المعاد صياغتها)، 9 ,00-597.620v03-PE يونيو 2017.

[902] اللائحة (الاتحاد الأوروبي) رقم 1052/2013 الصادرة عن البرلمان الأوروبي والمجلس بتاريخ 22 أكتوبر 2013 المتعلقة بإنشاء النظام الأوروبي لمراقبة الحدود («يوروسور»)، الجريدة الرسمية 295 L 2013 0J.

[903] اللائحة (الاتحاد الأوروبي) رقم 2916/1624 الصادرة عن البرلمان الأوروبي والمجلس المؤرخة في 14 سبتمبر 2016 المتعلقة بحرس الحدود و السواحل الأوروبية والمعدّلة للائحة (الاتحاد الأوروبي) 2016/399 الصادرة عن البرلمان الأوروبي والمجلس المَلغية للائحة (الجماعة الأوروبية) رقم 2007/863 الصادرة عن البرلمان الأوروبي والمجلس، ولائحة المجلس (الجماعة الأوروبية) رقم 2007/2004 وقرار المجلس EC/2005/267، الجريدة الرسمية 251 L 0J.

[904] انظر أيضاً: المفوضية الأوروبية (2008)، رسالة من المفوضية إلى البرلمان الأوروبي والمجلس واللجنة الاقتصادية والاجتماعية الأوروبية ولجنة المناطق: دراسة إنشاء نظام مراقبة الحدود الأوروبية («يوروسور»)، النسخة النهائية 68 (2008)COM، بروكسل، 13 فبراير 2008؛ المفوضية الأوروبية (2011)، تقييم الأثر المصاحب لاقتراح لائحة صادرة عن البرلمان الأوروبي والمجلس مؤسّسة للنظام الأوروبي لمراقبة الحدود («يوروسور»)، ورقة عمل طاقم الموظفين، النسخة النهائية 1536 (2011) SEC، بروكسل، 12 ديسمبر 2011، ص، 18.

[905] المفوضية الأوروبية، نظام مراقبة الحدود الأوروبية («يوروسور»): حماية حدود شنغن الخارجية - حماية حياة المهاجرين. نظام مراقبة الحدود الأوروبية («يوروسور») بإيجاز، 29 نوفمبر 2013.

[906] اللائحة 1052/2013، الحيثية 13 والمادة 13.

[907] نفس المرجع السابق، الحيثية 13 والمادة 13.

**نظام المعلومات الجمركية**

من بين أنظمة المعلومات المهمة الأخرى التي تم إنشاؤها على مستوى الاتحاد الأوروبي نظام المعلومات الجمركية (CIS).[908] ففي سياق إنشاء السوق الداخلية، تم إلغاء جميع الفحوصات والإجراءات الشكلية المتعلقة بالسلع التي يتم نقلها داخل أراضي الاتحاد الأوروبي، مما أدى إلى زيادة مخاطر الاحتيال. وقوبل هذا الخطر بتكثيف التعاون بين إدارات الجمارك في الدول الأعضاء، إن الغرض من نظام المعلومات الجمركية هو مساعدة الدول الأعضاء على منع الانتهاكات الجسيمة لقوانين الجمارك والفلاحة الوطنية وقوانين الاتحاد الأوروبي والتحقيق فيها ومقاضاة مرتكبيها. وقد تم إنشاء نظام المعلومات الجمركية من خلال صكين قانونيين اثنين، تم اعتمادهما على أسس قانونية مختلفة: تتعلق لائحة المجلس (الجماعة الأوروبية) رقم 515/97 بالتعاون بين مختلف السلطات الإدارية الوطنية لمكافحة الاحتيال في سياق الاتحاد الجمركي والسياسة الفلاحية المشتركة، بينما يهدف قرار المجلس JHA/2009/917 إلى المساعدة على منع المخالفات الجسيمة لقوانين الجمارك والتحقيق فيها ومقاضاة مرتكبيها. وهذا يعني أن نظام المعلومات الجمركية ليس معنياً فقط بإنفاذ القانون.

تشتمل المعلومات الواردة في نظام المعلومات الجمركية على البيانات الشخصية المتعلقة بالسلع، ووسائل النقل، والشركات، والأشخاص، والسلع، والنقود المحتفظ بها أو المحجوزة أو المصادرة. إن فئات البيانات التي يمكن معالجتها محدَّدة بشكل واضح، وهي تشمل الاسم والجنسية والجنس ومكان وتاريخ ازدياد الأفراد المعنيين وسبب إدراج بياناتهم في النظام ورقم تسجيل وسيلة النقل.[909] يمكن استخدام هذه المعلومات فقط لأغراض المعاينة أو الإبلاغ أو تنفيذ عمليات تفتيش معينة أو للتحليلات الاستراتيجية أو التشغيلية المتعلقة بالأشخاص المشتبه في انتهاكهم المقتضيات الجمركية.

يتم منح الوصول إلى نظام المعلومات الجمركية للسلطات الوطنية لكل من الجمارك والضرائب الفلاحةوالصحة العامة والشرطة، بالإضافة إلى اليوروبول ووكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية.

يجب أن تتوافق معالجة البيانات الشخصية مع القواعد المحدَّدة التي تنص عليها اللائحة رقم 515/97 وقرار المجلس JHA/2009/917 بالإضافة إلى مقتضيات اللائحة العامة لحماية البيانات ولائحة حماية البيانات الخاصة بمؤسسات الاتحاد الأوروبي والاتفاقية 108 المحدثة وتوصية الشرطة. إن المشرف الأوروبي على حماية البيانات مسؤول عن الإشراف على امتثال نظام المعلومات الجمركية للائحة (الجماعة الأوروبية) رقم 45/2001. وهو يعقد اجتماعاً مرة واحدة على الأقل في السنة مع جميع الهيئات الإشرافية لحماية البيانات الوطنية ذات الاختصاص فيما يتعلق بقضايا الإشراف المتعلقة بنظام المعلومات الجمركية.

**قابلية التشغيل البيني بين أنظمة معلومات الاتحاد الأوروبي**

تشكل إدارة الهجرة والإدارة المتكاملة للحدود الخارجية للاتحاد الأوروبي ومكافحة الإرهاب والجريمة العابرة للحدود تحديات مهمة وقد أصبحت معقدة بشكل متزايد في عالم تسوده العولمة. في السنوات الأخيرة، عمل الاتحاد الأوروبي على نهج شامل جديد لحماية الأمن والحفاظ عليه دون المساس بقيم الاتحاد الأوروبي وحرياته الأساسية. في هذه الجهود، يعد التبادل الفعال للمعلومات بين سلطات إنفاذ القانون الوطنية ، و بين الدول الأعضاء ووكالات الاتحاد الأوروبي ذات الصلة ، أمراً أساسياً.[910] ولأنظمة المعلومات الحالية في

---

[908] مجلس الاتحاد الأوروبي (1995)، قانون المجلس الصادر في 26 يوليو 1995 الصانع لاتفاقية استخدام تكنولوجيا المعلومات للأغراض الجمركية، الجريدة الرسمية 316 C 1995 OJ، والمُعدّل من قبل مجلس الاتحاد الأوروبي (2009)، اللائحة رقم 515/97 المؤرخة في 13 مارس 1997 بشأن المساعدة المتبادلة بين السلطات الإدارية للدول الأعضاء والتعاون بين هذه الأخيرة والمفوضية لضمان التطبيق الصحيح لقانون الجمارك والمسائل الفلاحية، قرار المجلس JHA/2009/917 المؤرخ في 30 نوفمبر 2009 بشأن استخدام تكنولوجيا المعلومات للأغراض الجمركية، الجريدة الرسمية 323 L 2009 OJ (قرار رابطة الدول المستقلة).

[909] انظر قرار رابطة الدول المستقلة، المواد 24 و25 و28.

[910] المفوضية الأوروبية (2016)، رسالة من المفوضية إلى البرلمان الأوروبي والمجلس: نظم معلومات أقوى وأذكى للحدود والأمن، النسخة النهائية 205 (2016) COM، بروكسل، 6 أبريل 2016، المفوضية الأوروبية (2016)، رسالة من المفوضية إلى البرلمان الأوروبي والمجلس الأوروبي ومجلس أوروبا: تعزيز الأمن في عالم التنقل: تحسين تبادل المعلومات في مكافحة الإرهاب وتقوية الحدود الخارجية، النسخة النهائية 602 (2016) COM، بروكسل، 14 سبتمبر 2016، المفوضية الأوروبية (2016)، اقتراح لائحة صادرة عن البرلمان الأوروبي والمجلس بشأن استخدام نظام معلومات شنغن لعودة مواطني الدول الثالثة المقيمين بشكل غير قانوني، انظر أيضاً، رسالة من المفوضية إلى البرلمان الأوروبي والمجلس الأوروبي ومجلس أوروبا: التقرير المرحلي السابع نحو اتحاد أمني فعال وحقيقي، النسخة النهائية 261 (2017) COM، بروكسل، 16 مايو 2017.

الاتحاد الأوروبي لإدارة الحدود والأمن الداخلي أهدافها، وهيكلها المؤسسي، وأصحاب البيانات والمستخدمون الخاصون بها. ويعمل الاتحاد الأوروبي على التغلب على أوجه القصور في وظائف إدارة بيانات الاتحاد الأوروبي المجزأة بين أنظمة المعلومات المختلفة مثل الجيل الثاني من نظام شنغن للمعلومات ونظام معلومات التأشيرات والنظام الأوروبي لمضاهاة بصمات الأصابع من خلال استكشاف إمكانية التشغيل البيني.[911] ويتجلى الهدف الرئيسي في ضمان حصول الشرطة والجمارك والسلطات القضائية المختصة بشكل منهجي على المعلومات اللازمة لأداء واجباتها، مع الحفاظ على التوازن فيما يتعلق بالحق في الخصوصية وحماية البيانات والحقوق الأساسية الأخرى.

إن قابلية التشغيل البيني تعني 'قدرة أنظمة المعلومات على تبادل البيانات وتمكين مشاركة المعلومات'.[912] ويجب ألا يخل هذا التبادل بالقواعد الصارمة بشأن الضرورة عند الوصول إلى البيانات واستعمالها و التي تضمنها اللائحة العامة لحماية البيانات، والأمر التوجيهي المتعلق بحماية البيانات الموجه للشرطة وسلطات العدالة الجنائية، وميثاق الاتحاد الأوروبي للحقوق الأساسية، وجميع القواعد الأخرى ذات الصلة. ويجب ألا يؤثر أي حل متكامل لإدارة البيانات على مبادئ حصر الغرض أو حماية البيانات منذ التصميم أو تلقائياً.[913]

بالإضافة إلى تحسين وظائف أنظمة المعلومات الرئيسية الثلاثة - الجيل الثاني من نظام شنغن للمعلومات، ونظام معلومات التأشيرات، والنظام الأوروبي لمضاهاة بصمات الأصابع - اقترحت المفوضية إنشاء نظام مركزي رابع لإدارة الحدود يتعامل مع مواطني الدول الثالثة: وهو نظام الدخول والخروج (EES)،[914] ومن المتوقع أن يتم تنفيذه بحلول سنة 2020. [915] كما أصدرت المفوضية اقتراحاً بشأن إنشاء نظام معلومات وتصاريح السفر الأوروبي (ETIAS)،[916] وهو نظام سيجمع المعلومات عن الأشخاص الذين يسافرون بدون تأشيرة إلى الاتحاد الأوروبي للسماح بإجراء الفحوصات المتقدمة للهجرة غير النظامية والأمنية.

[911] مجلس الاتحاد الأوروبي (2005)، برنامج لاهاي: تعزيز الحرية والأمن والعدالة في الاتحاد الأوروبي، الجريدة الرسمية 53 C 2005 OJ، المفوضية الأوروبية (2010)، رسالة من المفوضية إلى البرلمان الأوروبي والمجلس: لمحة عامة عن إدارة المعلومات في مجال الحرية والأمن والعدالة، النسخة النهائية 385 (2010) COM، المفوضية الأوروبية (2016)، رسالة من المفوضية إلى البرلمان الأوروبي والمجلس: نظم معلومات أقوى وأكثر ذكاءً للحدود والأمن، النسخة النهائية 205 (2016) COM، بروكسل، 6 أبريل 2016، المفوضية الأوروبية (2016)، قرار المفوضية الصادر في 17 يونيو 2016 بشأن إنشاء فريق الخبراء رفيع المستوى المعني بنظم المعلومات وقابلية التشغيل البيني، الجريدة الرسمية 257 C 2016 OJ.

[912] المفوضية الأوروبية (2016)، رسالة من المفوضية إلى البرلمان الأوروبي والمجلس: نظم معلومات أقوى وأذكى للحدود والأمن، النسخة النهائية 205 (2016) COM، بروكسل، 6 أبريل 2016، ص. 14.

[913] نفس المرجع السابق، الصفحتان 5-4.

[914] المفوضية الأوروبية (2016)، اقتراح لائحة صادرة عن البرلمان الأوروبي والمجلس منشئة لنظام الدخول والخروج (EES) لتسجيل بيانات الدخول والخروج وبيانات رفض الدخول لمواطني الدول الثالثة الذين يعبرون الحدود الخارجية للدول الأعضاء الاتحاد الأوروبي ومحدّدة لشروط الوصول إلى نظام الدخول والخروج لأغراض إنفاذ القانون ومعدّلة للائحة (الجماعة الأوروبية) رقم 767/2008 واللائحة (الاتحاد الأوروبي) رقم 1077/2011، النسخة النهائية 194 (2016) COM، بروكسل، 6 أبريل 2016.

[915] المفوضية الأوروبية (2016)، رسالة من المفوضية إلى البرلمان الأوروبي والمجلس: نظم معلومات أقوى وأذكى للحدود والأمن، النسخة النهائية 205 (2016) COM، بروكسل، 6 أبريل 2016، ص. 5.

[916] المفوضية الأوروبية (2016)، اقتراح لائحة صادرة عن البرلمان الأوروبي والمجلس منشئة لنظام معلومات وتصاريح السفر الأوروبي (ETIAS) ومعدّلة للوائح (الاتحاد الأوروبي) رقم 515/2014 و(الاتحاد الأوروبي) 2016/399 و (الاتحاد الأوروبي) 2016/794 و(الاتحاد الأوروبي) 2016/1624، النسخة النهائية 16 ،731 (2016) COM نوفمبر 2016.

# 9

# أنـواع معينـة من البيانـات وقواعـــد حمايـــة البيانـــات المتعلقـــة بهـــا

| الاتحاد الأوروبي | المسائل المتناولة | مجلس أوروبا |
|---|---|---|
| اللائحة العامة لحماية البيانات<br>الأمر التوجيهي المتعلق بالخصوصية والاتصالات الإلكترونية | الاتصالات الإلكترونية | الاتفاقية 108 المحدثة<br>توصية خدمات الاتصالات |
| اللائحة العامة لحماية البيانات، المادة 88 | علاقات التوظيف | الاتفاقية 108 المحدثة<br>توصية التوظيف |
| | | المحكمة الأوروبية لحقوق الإنسان، قضية «كوبلاند ضد المملكة المتحدة»، رقم 62617/00، 2007 |
| اللائحة العامة لحماية البيانات، المادة 9 (2) (ح) و(ط) | البيانات الطبية | الاتفاقية 108 المحدثة<br>توصية البيانات الطبية |
| | | المحكمة الأوروبية لحقوق الإنسان، قضية «ز ضد فنلندا»، رقم 22009/93، 1997 |
| لائحة التجارب السريرية | التجارب السريرية | |
| اللائحة العامة لحماية البيانات، المادة 6 (4) والمادة 89 | الإحصاءات | الاتفاقية 108 المحدثة<br>توصية البيانات الإحصائية |
| اللائحة (الجماعة الأوروبية) رقم 223/2009 المتعلقة بالإحصاءات الأوروبية<br>محكمة العدل التابعة للاتحاد الأوروبي، القضية C-524/06، «هوبر ضد جمهورية ألمانيا الاتحادية» [الغرفة الكبرى]، 2008 | الإحصاءات الرسمية | الاتفاقية 108 المحدثة<br>توصية البيانات الإحصائية |

| | | |
|---|---|---|
| الأمر التوجيهي EU/2014/65 المتعلق بالأسواق في الصكوك المالية<br>اللائحة (الجماعة الأوروبية) رقم 648/2012 المتعلقة بمشتقات عقود التداولات المباشرة وبالنظراء المركزيين والمستودعات التجارية<br>اللائحة (الجماعة الأوروبية) رقم 1060/2009 المتعلقة بوكالات التصنيف الائتماني<br>الأمر التوجيهي EC/2007/64 المتعلق بخدمات الدفع في السوق الداخلية | البيانات المالية | الاتفاقية 108 المحدثة<br>التوصية 90 (19) المَستخدَمة لأغراض المدفوعات وغيرها من العمليات المتعلقة بها<br>المحكمة الأوروبية لحقوق الإنسان، قضية «ميشو ضد فرنسا»، رقم 12323/11، 2012 |

في العديد من الحالات، تم اعتماد صكوك قانونية خاصة على المستوى الأوروبي لتطبيق القواعد العامة للاتفاقية 108 المحدثة أو اللائحة العامة لحماية البيانات بشكل أكثر تفصيلاً في حالات محددة.

## 1.9. الاتصالات الإلكترونية

### النقاط الرئيسية

- ترد قواعد محددة بشأن حماية البيانات في مجال الاتصالات، مع إشارة خاصة إلى خدمات الهاتف، في توصية مجلس أوروبا لسنة 1995.
- يتم تنظيم معالجة البيانات الشخصية المتعلقة بتقديم خدمات الاتصالات على مستوى الاتحاد الأوروبي في الأمر التوجيهي المتعلق بالخصوصية والاتصالات الإلكترونية.
- لا تتعلق سرية الاتصالات الإلكترونية بمحتوى الاتصال فحسب، بل أيضاً بالبيانات الوصفية، مثل المعلومات حول هوية الأشخاص الذين يقومون بالتواصل، ووقت الاتصال ومدته، وبيانات الموقع مثل المكان الذي تم إرسال البيانات منه.

لدى شبكات الاتصالات إمكانية كبيرة للقيام بالتدخل غير المبرر في المجال الشخصي للمستخدمين، حيث إنها توفر إمكانيات تقنية قوية للاستماع إلى الاتصالات التي يتم إجراؤها على هذه الشبكات وإجراء مسوحات عليها. ونتيجة لذلك، تم التوصل إلى أن لوائح خاصة لحماية البيانات ضرورية لمعالجة المخاطر المعينة على مستخدمي خدمات الاتصالات.

في سنة 1995، أصدر **مجلس أوروبا** توصية لحماية البيانات في مجال الاتصالات، مع إشارة خاصة إلى خدمات الهاتف.[917] ووفقاً لهذه التوصية، يجب أن تقتصر أغراض جمع البيانات الشخصية ومعالجتها في سياق الاتصالات على: ربط المستخدم بالشبكة، وإتاحة خدمة الاتصالات الخاصة، وإعداد الفواتير، والتحقق، وضمان التشغيل التقني الأمثل، وتطوير الشبكة و الخدمات.
هذا وتم إيلاء اهتمام خاص لاستخدام شبكات الاتصالات لإرسال الرسائل التسويقية المباشرة. كقاعدة عامة، لا يجوز توجيه رسائل التسويق المباشر إلى أي مشترك اختار صراحة عدم استلامها. ولا يجوز استخدام أجهزة الاتصال الآلي لنقل الرسائل الإعلانية المسجلة مسبقاً إلا إذا أعطى المشترك موافقة صريحة. ومن المفروض أن ينص القانون المحلي على قواعد مفصلة في هذا المجال.

في **الإطار القانوني للاتحاد الأوروبي**، بعد المحاولة الأولى في سنة 1997، تم اعتماد الأمر التوجيهي المتعلق بالخصوصية والاتصالات الإلكترونية في سنة 2002 وتم تعديله في سنة 2009، وذلك بغرض استكمال وتكييف مقتضيات الأمر التوجيهي السابق لحماية البيانات المُوجَّه إلى قطاع الاتصالات.[918]

يقتصر تطبيق الأمر التوجيهي المتعلق بالخصوصية والاتصالات الإلكترونية على خدمات الاتصال في الشبكات الإلكترونية العامة.
ويميز الأمر التوجيهي المتعلق بالخصوصية والاتصالات الإلكترونية بين ثلاث فئات رئيسية من البيانات التي تنشأ أثناء الاتصال:

- البيانات التي تشكل محتوى الرسائل المرسلة أثناء الاتصال - وهذه البيانات سرية للغاية؛
- البيانات اللازمة لإنشاء الاتصال ومواصلته - وهي ما يسمى بالبيانات الوصفية، والمشار إليها باسم «بيانات الحركة» في الأمر التوجيهي - مثل المعلومات المتعلقة بأطراف الاتصال ووقت الاتصال ومدته؛
- توجد ضمن البيانات الوصفية بيانات تتعلق تحديداً بموقع جهاز الاتصال، وهي تُسمى بيانات الموقع - وتُعد هذه البيانات في نفس الوقت بيانات حول موقع مستخدمي أجهزة الاتصال، لا سيما عندما يتعلق الأمر بمستخدمي أجهزة الاتصالات المحمولة.

---

[917] مجلس أوروبا، لجنة الوزراء (1995)، التوصية Rec(95)4 الموجّهة إلى الدول الأعضاء بشأن حماية البيانات الشخصية في مجال خدمات الاتصالات، مع إشارة خاصة إلى خدمات الهاتف، 7 فبراير 1995.

[918] الأمر التوجيهي EC/2002/58 للبرلمان الأوروبي والمجلس المؤرخ في 12 يوليو 2002 المتعلق بمعالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الإلكترونية، الجريدة الرسمية 201 L 2002 OJ (الأمر التوجيهي المتعلق بالخصوصية والاتصالات الإلكترونية) بصيغته المعدّلة بواسطة الأمر التوجيهي رقم EC/2009/136 للبرلمان الأوروبي والمجلس المؤرخ في 25 نوفمبر 2009 المعدّل للأمر التوجيهي EC/2002/22 المتعلق بالخدمة الشاملة وحقوق المستخدمين المتعلقة بشبكات وخدمات الاتصالات الإلكترونية، الأمر التوجيهي EC/2002/58 المتعلق بمعالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الإلكترونية واللائحة (الجماعة الأوروبية) رقم 2006/2004 بشأن التعاون بين السلطات الوطنية المسؤولة عن إنفاذ قوانين حماية المستهلك، الجريدة الرسمية 337 L 2009 OJ.

يمكن استخدام بيانات حركة المرور من قبل مزود الخدمة فقط للفوترة ولتقديم الخدمة من الناحية التقنية. إلا أنه يمكن الكشف عن هذه البيانات، بموافقة صاحب البيانات، إلى مراقبين آخرين يقدمون خدمات ذات قيمة مضافة تتعلق بموقع المستخدم ، مثل إعطاء معلومات حول محطة المترو أو الصيدلية التي تتواجد بقربه أو توقعات الطقس لذلك الموقع.

وفقاً للمادة 15 من الأمر التوجيهي المتعلق بالخصوصية الإلكترونية، يجب أن تفي أشكال الوصول الأخرى إلى البيانات المتعلقة بالاتصالات في الشبكات الإلكترونية بمتطلبات التدخل المبرر في الحق في حماية البيانات على النحو المنصوص عليه في المادة 8 (2) من الاتفاقية الأوروبية لحقوق الإنسان والتي أكدها ميثاق الحقوق الأساسية للاتحاد الأوروبي في المادتين 8 و52. وقد تشمل أشكال الوصول هذه الوصولَ بغرض التحقيق في الجرائم.

أدخلت تعديلات سنة 2009 على الأمر التوجيهي المتعلق بالخصوصية والاتصالات الإلكترونية[919] ما يلي:

- توسيع نطاق القيود المفروضة على إرسال رسائل البريد الإلكتروني لأغراض التسويق المباشر ليشمل خدمات الرسائل القصيرة وخدمات الرسائل متعددة الوسائط وأنواع أخرى من التطبيقات المماثلة؛ تُحظر رسائل البريد الإلكتروني التسويقية ما لم يتم الحصول على موافقة مسبقة. وبدون هذه الموافقة، يمكن التواصل فقط مع العملاء السابقين من خلال رسائل البريد الإلكتروني التسويقية، وذلك إذا كانوا قد أتاحوا عناوين بريدهم الإلكتروني ولم يعترضوا.
- إلزام الدول الأعضاء بتوفير سبل الانتصاف القضائية من انتهاكات الحظر المفروض على الاتصالات غير المرغوب فيها .[920]
- لم يعد يُسمح بتثبيت ملفات تعريف الارتباط («كوكيز»)، وهي البرمجيات التي تراقب وتسجل العمليات التي يقوم بها مستخدم الكمبيوتر، بدون موافقة المستخدم. وينبغي أن ينظم القانون الوطني بشكل أكثر تفصيلاً كيفية التعبير عن الموافقة والحصول عليها لتوفير الحماية الكافية.[921]

في حالة حدوث خرق للبيانات نتيجة للوصول غير المصرح به أو فقدان البيانات أو دمارها، يجب إبلاغ الهيئة الإشرافية المختصة على الفور. ويجب إبلاغ المشتركين عندما يكون الضرر الذي يُحتمَل أن يلحق بهم ناتجاً عن خرق البيانات.[922]

كان الأمر التوجيهي المتعلق بالاحتفاظ بالبيانات[923] يتطلب من مزودي خدمات الاتصالات الاحتفاظ بالبيانات الوصفية. ولكن تم إبطال هذا الأمر التوجيهي من قبل محكمة العدل التابعة للاتحاد الأوروبي (لمزيد من التفاصيل، انظر الجزء 3.8).

**الآفاق**

في يناير 2017، تبنت المفوضية الأوروبية اقتراحاً جديداً بشأن لائحة الخصوصية الإلكترونية لتحل محل الأمر التوجيهي القديم المتعلق بالخصوصية الإلكترونية. وسيظل الهدف هو حماية «الحقوق والحريات الأساسية للأشخاص الطبيعيين والاعتباريين في توفير واستخدام خدمات الاتصالات الإلكترونية، وعلى وجه الخصوص، الحق في احترام الحياة الخاصة والاتصالات وحماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية». في نفس الوقت، يسعى الاقتراح الجديد إلى ضمان حرية نقل بيانات الاتصالات الإلكترونية وخدمات الاتصالات الإلكترونية داخل الاتحاد.[924] ففي حين تتناول اللائحة العامة لحماية البيانات بشكل أساسي المادة 8 من ميثاق الاتحاد الأوروبي للحقوق الأساسية، تهدف اللائحة المقترحة إلى دمج المادة 7 من الميثاق في القانون الثانوي للاتحاد الأوروبي.

---

[919] الأمر التوجيهي رقم EC/2009/136 للبرلمان الأوروبي والمجلس المؤرخ في 25 نوفمبر 2009 المعدّل للأمر التوجيهي EC/2002/22 المتعلق بالخدمة الشاملة وحقوق المستخدمين المتعلقة بشبكات وخدمات الاتصالات الإلكترونية، الأمر التوجيهي EC/2002/58 المتعلق بمعالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الإلكترونية واللائحة (الجماعة الأوروبية) رقم 2006/2004 بشأن التعاون بين السلطات الوطنية المسؤولة عن إنفاذ قوانين حماية المستهلك، الجريدة الرسمية 337 L 2009 OJ.

[920] انظر الأمر التوجيهي المعدّل، المادة 13.

[921] انظر نفس المرجع السابق، المادة 5؛ انظر أيضاً الفريق العامل بموجب المادة 29 (2012)، الرأي 04/2012 بشأن الإعفاء من الموافقة على ملفات تعريف الارتباط، WP 194، بروكسل، 7 يونيو 2012.

[922] انظر أيضاً فريق عمل المادة 29 (2011)، وثيقة العمل 01/2011 بشأن إطار العمل الحالي المتعلق بخرق البيانات الشخصية في الاتحاد الأوروبي والتوصيات الخاصة بتطورات السياسة المستقبلية، WP 184، بروكسل، 5 أبريل 2011.

[923] الأمر التوجيهي EC/2006/24 للبرلمان الأوروبي والمجلس المؤرخ في 15 مارس 2006 بشأن الاحتفاظ بالبيانات التي تم إنشاؤها أو معالجتها فيما يتعلق بتوفير خدمات الاتصالات الإلكترونية المتاحة للجمهور أو شبكات الاتصالات العامة والمعدّل للأمر التوجيهي EC/2002/58، الجريدة الرسمية 105 L 2006 OJ.

[924] مقترح لائحة صادرة عن البرلمان الأوروبي والمجلس بشأن احترام الحياة الخاصة وحماية البيانات الشخصية في الاتصالات الإلكترونية ومَلغية للتوجيه EC/2002/58 (لائحة الخصوصية والاتصالات الإلكترونية) (النسخة النهائية10 (2017) COM )، المادة 1.

ستعمل اللائحة على تكييف مقتضيات الأمر التوجيهي السابق مع التكنولوجيات الجديدة وواقع السوق، وستؤسس إطاراً شاملاً ومتسقاً مع اللائحة العامة لحماية البيانات. ومن هذا المنطلق، فإن لائحة الخصوصية الإلكترونية ستكون بمثابة تقنين خاص ينضاف إلى اللائحة العامة لحماية البيانات، بحيث تكيفها مع بيانات الاتصالات الإلكترونية التي تشكل بيانات شخصية. وتغطي اللائحة الجديدة معالجة «بيانات الاتصالات الإلكترونية»، بما في ذلك محتوى الاتصالات الإلكترونية والبيانات الوصفية التي لا تكون بالضرورة بيانات شخصية. ويقتصر النطاق الإقليمي للائحة على الاتحاد الأوروبي، بما في ذلك عندما تتم معالجة البيانات التي تم الحصول عليها في الاتحاد الأوروبي خارجه، ويمتد إلى مزودي خدمات الاتصال المباشر عبر الإنترنت، وهم مزودو الخدمات الذين يقدمون المحتوى أو الخدمات أو التطبيقات عبر الإنترنت، دون مشاركة مباشرة من مشغل شبكة أو مزود خدمة الإنترنت (ISP). وتشمل الأمثلة على هؤلاء المزودين «سكايب» (المكالمات الصوتية والمرئية) و«واتساب» (المراسلة) و«غوغل» (البحث) و«سبوتيفاي» (الموسيقى) و«نتفليكس» (محتوى الفيديو). وستنطبق آليات إنفاذ اللائحة العامة لحماية البيانات على اللائحة الجديدة.

من المقرر أن يتم اعتماد لائحة الخصوصية الإلكترونية قبل 25 مايو 2018، وفي ذلك الوقت ستكون اللائحة العامة لحماية البيانات قابلة للتطبيق في جميع الدول الأعضاء البالغ عددها 28 دولة. ولكن ذلك يبقى مشروطاً بموافقة كل من البرلمان الأوروبي والمجلس.[925]

## 2.9. بيانات التوظيف

### النقاط الرئيسية

- تم تحديد قواعد محددة لحماية البيانات في علاقات التوظيف في توصية مجلس أوروبا بشأن بيانات التوظيف.
- في اللائحة العامة لحماية البيانات، يشار إلى علاقات التوظيف على وجه التحديد فقط في سياق معالجة البيانات الحساسة.
- يمكن أن تكون صلاحية الموافقة، التي يجب أن تُمنح بحرية، كأساس قانوني لمعالجة البيانات حول الموظفين، موضع شك، وذلك نظراً لاختلال التوازن الاقتصادي بين صاحب العمل والموظفين. ويجب تقييم الظروف المحيطة بالموافقة بعناية.

تخضع معالجة البيانات في سياق التوظيف للتشريعات العامة للاتحاد الأوروبي بشأن حماية البيانات الشخصية. ومع ذلك، تتعامل إحدى اللوائح[926] بشكل خاص مع حماية معالجة البيانات الشخصية من قبل المؤسسات الأوروبية في سياق التوظيف (من بين أمور أخرى). وفي اللائحة العامة لحماية البيانات، يشار إلى علاقات التوظيف على وجه التحديد في المادة 9 (2)، والتي تنص على أنه يمكن معالجة البيانات الشخصية عند تنفيذ الالتزامات أو ممارسة الحقوق المحددة للمراقب أو صاحب البيانات في مجال التوظيف.

بموجب اللائحة العامة لحماية البيانات، يجب تمكين الموظف من التمييز بوضوح بين البيانات التي يوافق على معالجتها / تخزينها والأغراض التي يتم تخزين بياناته من أجلها. ويجب أيضاً إبلاغ الموظفين بحقوقهم والمدة التي سيتم تخزين البيانات فيها، قبل منح الموافقة. وفي حالة حدوث انتهاك للبيانات الشخصية من المحتمل أن يؤدي إلى مخاطر كبيرة على حقوق وحريات الأشخاص الطبيعيين، يجب على صاحب العمل إبلاغ الموظف بهذا الانتهاك. وتسمح المادة 88 من اللائحة للدول الأعضاء بوضع قواعد أكثر تحديداً لضمان حماية حقوق الموظفين وحرياتهم فيما يتعلق ببياناتهم الشخصية في سياق التوظيف.

[925] لمزيد من المعلومات، انظر المفوضية الأوروبية (2017)، «تقترح المفوضية مستوىً عالياً من قواعد الخصوصية لجميع الاتصالات الإلكترونية وتقوم بتحديث قواعد حماية البيانات لمؤسسات الاتحاد الأوروبي»، بيان صحفي، 10 يناير 2017.

[926] اللائحة (الجماعة الأوروبية) رقم 45/2001 الصادرة عن البرلمان الأوروبي والمجلس المؤرخة في 18 ديسمبر 2000 بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية من قبل مؤسسات وهيئات الجماعة الأوروبية وحرية حركة هذه البيانات، الجريدة الرسمية L 8 OJ 2001.

مثال: في قضية «فورتن»،[927] تضمنت البيانات سجلاً لوقت العمل يحتوي على فترات العمل والراحة اليومية، والتي تشكل بيانات شخصية. يمكن أن يتطلب القانون الوطني من صاحب العمل إتاحة سجلات وقت العمل للسلطات الوطنية المسؤولة عن مراقبة ظروف العمل، ومن شأن ذلك أن يسمح بالوصول الفوري إلى البيانات الشخصية ذات الصلة. ولكن الوصول إلى تلك البيانات الشخصية ضروري لتمكين السلطة الوطنية من مراقبة التشريعات المتعلقة بظروف العمل.[928]

فيما يتعلق **بمجلس أوروبا**، صدرت توصية بيانات التوظيف في سنة 1989 ونُقحت في سنة 2015.[929] وتغطي هذه التوصية معالجة البيانات الشخصية لأغراض التوظيف في كل من القطاعين العام والخاص، يجب أن تمتثل المعالجة لمبادئ وقيود معينة، مثل مبدأ الشفافية واستشارة ممثلي الموظفين قبل وضع أنظمة المراقبة في مكان العمل. كما تنص التوصية أيضاً على أنه يجب على أصحاب العمل تطبيق تدابير وقائية، مثل استعمال تقنيات الترشيح (أي الفلاتر)، بدلاً من مراقبة استخدام الموظفين للإنترنت.

يمكن العثور على استقصاء لمشاكل حماية البيانات الأكثر شيوعاً الخاصة بسياق التوظيف في وثيقة عمل خاصة من إعداد فريق عمل المادة 29،[930] حيث قام فريق العمل بتحليل أهمية الموافقة كأساس قانوني لمعالجة بيانات التوظيف،[931] فوجد أن عدم التوازن الاقتصادي بين صاحب العمل الذي يطلب الموافقة والموظف الذي يعطي الموافقة غالباً ما يثير الشكوك حول ما إذا كانت الموافقة قد مُنحت بحرية أم لا. لذلك ينبغي النظر بعناية في الظروف التي يتم فيها الاعتماد على الموافقة كأساس قانوني لمعالجة البيانات عند تقييم صلاحية الموافقة في سياق التوظيف.

من بين مشاكل حماية البيانات الشائعة في بيئة العمل النموذجية في يومنا هذا مدى مراقبة الاتصالات الإلكترونية للموظفين بشكل شرعي داخل مكان العمل. وغالباً ما يُزعم أنه يمكن حل هذه المشكلة بسهولة عن طريق حظر الاستخدام الخاص لمرافق الاتصالات في العمل. ولكن يمكن أن يكون هذا الحظر العام غير متناسب وغير واقعي. إن حكمي المحكمة الأوروبية لحقوق الإنسان في قضيتي «كوبلاند ضد المملكة المتحدة» و«باربوليسكو ضد رومانيا» لهما أهمية خاصة في هذا السياق.

مثال: في قضية **«كوبلاند ضد المملكة المتحدة»**،[932] تمت مراقبة استخدام الهاتف والبريد الإلكتروني والإنترنت لموظفة في كلية بشكل سري للتأكد مما إذا كانت تستخدم مرافق الكلية بشكل مفرط لأغراض شخصية. ورأت المحكمة الأوروبية لحقوق الإنسان أن المكالمات الهاتفية من المباني التجارية مشمولة ضمن مفهومي الحياة الخاصة والمراسلات. ولذلك فإن هذه المكالمات ورسائل البريد الإلكتروني المرسلة من مكان العمل وكذلك المعلومات المستمدة من مراقبة استخدام الإنترنت الشخصي محمية بموجب المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان. وفي حالة المدعية، لا توجد مقتضيات تنظم الظروف التي يمكن لأصحاب العمل بموجبها مراقبة استخدام الموظفين للهاتف والبريد الإلكتروني والإنترنت. لذلك لم يكن هذا التدخل متوافقاً مع القانون. وخلصت المحكمة إلى أنه تم انتهاك المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان.

مثال: في قضية **«باربوليسكو ضد رومانيا»**،[933] تم فصل المدعي بسبب استخدامه للإنترنت في مكان عمله أثناء ساعات العمل، منتهكاً بذلك اللوائح الداخلية، علماً بأن صاحب العمل كان يراقب اتصالاته. وقد تم خلال مجريات الدعوى المحلية عرض السجلات التي تُظهر رسائل ذات طبيعة خاصة بحتة. عند استنتاج المحكمة الأوروبية لحقوق الإنسان انطباق المادة 8 في هذه القضية، لم تحدد ما إذا كانت اللوائح التقييدية الخاصة بصاحب العمل قد تركت للمدعي توقعاً معقولاً للخصوصية، لكنها ارتأت أن تعليمات رب العمل لا يمكن لها أن تحد تماماً من الحياة الاجتماعية الخاصة.

[927] محكمة العدل التابعة للاتحاد الأوروبي، القضية C-342/12، «شركة 'وورتن' للتجهيزات المنزلية المحدودة ضد هيئة ظروف العمل (ACT)»، 30 مايو 2013، الفقرة 19.
[928] نفس المرجع السابق، الفقرة 43.
[929] مجلس أوروبا، لجنة الوزراء (2015)، التوصية Rec(2015)5 الموجهة إلى الدول الأعضاء بشأن معالجة البيانات الشخصية في سياق التوظيف، أبريل 2015.
[930] فريق عمل المادة 29 (2017)، الرأي 2/2017 بشأن معالجة البيانات في العمل، WP 249، بروكسل، 8 يونيو 2017.
[931] لفريق عمل المادة 29 (2005)، وثيقة عمل حول التفسير المشترك للمادة 26(1) من الأمر التوجيهي EC/95/46 المؤرخ في 24 أكتوبر 1995، WP 114، بروكسل، 25 نوفمبر 2005.
[932] المحكمة الأوروبية لحقوق الإنسان، قضية «كوبلاند ضد المملكة المتحدة»، رقم 62617/00، 3 أبريل 2007.
[933] المحكمة الأوروبية لحقوق الإنسان، قضية «باربوليسكو ضد رومانيا» [الغرفة الكبرى]، رقم 61496/08، 5 سبتمبر 2017، الفقرة 121.

من حيث الموضوع، وجب منح الدول المتعاقدة هامشاً واسعاً للتقدير فيما يخص تقييم الحاجة إلى إنشاء إطار قانوني يحكم الظروف التي يمكن فيها لصاحب العمل تنظيم الاتصالات الإلكترونية أو الاتصالات الأخرى ذات الطبيعة غير المهنية التي يقوم بها موظفوه في مكان العمل. ومع ذلك، كان على السلطات المحلية أن تتأكد من أن قيام صاحب العمل بوضع تدابير لرصد المراسلات وغيرها من الاتصالات، بصرف النظر عن نطاق هذه التدابير ومدتها، كان مصحوباً بضمانات مناسبة وكافية ضد التجاوزات. كان كل من مبدأ التناسب والضمانات الإجرائية للوقاية من التعسف ضروريين، وقد حددت المحكمة الأوروبية لحقوق الإنسان عدداً من العوامل ذات الصلة بظروف القضية. وقد شملت هذه الظروف، من جملة أمور أخرى، نطاق المراقبة من قبل صاحب العمل ودرجة التطفل على خصوصية الموظف؛ والعواقب على الموظف؛ وما إذا كان قد تم توفير ضمانات كافية. بالإضافة إلى ذلك، توجب على السلطات المحلية ضمان وصول الموظف الذي رُصدت اتصالاته إلى سبيل انتصاف أمام هيئة قضائية من اختصاصها تحديد، على الأقل من حيث الجوهر، كيف تم الالتزام بتلك المعايير المحددة وما إذا كانت التدابير المطعون فيها قانونية.

في هذه القضية، استنتجت المحكمة الأوروبية لحقوق الإنسان أنه تم انتهاك المادة 8 لأن السلطات الوطنية لم توفر حماية كافية لحق المدعي في احترام حياته الخاصة ومراسلاته، وبالتالي فشلت في تحقيق توازن عادل بين مصالح المعنيين.

وفقاً لتوصية التوظيف لمجلس أوروبا، يجب الحصول على البيانات الشخصية التي يتم جمعها لأغراض التوظيف من الموظف الفرد مباشرة.

يتعين أن تقتصر البيانات الشخصية التي يتم جمعها لغرض التوظيف على المعلومات اللازمة لتقييم مدى ملاءمة المرشحين وإمكاناتهم المهنية.

تشير التوصية أيضاً على وجه التحديد إلى البيانات الحاملة لأحكام القيمة المتعلقة بمستوى أداء الموظفين الأفراد أو إمكاناتهم. ويتعين أن تستند البيانات الحاملة لأحكام القيمة إلى تقييمات عادلة وصادقة وألا تكون مهينة في الطريقة التي صيغت بها، وهذا أمر مطلوب بموجب مبدأي المعالجة العادلة للبيانات ودقتها.

يتمثل أحد الجوانب المحددة لقانون حماية البيانات في العلاقة بين صاحب العمل والموظف في دور ممثلي الموظفين. إذ يمكن أن يستلم هؤلاء الممثلون البيانات الشخصية للموظفين فقط بقدر ما يكون ذلك ضرورياً للسماح لهم بتمثيل مصالح الموظفين أو إذا كانت هذه البيانات ضرورية للوفاء بالالتزامات المنصوص عليها في الاتفاقات الجماعية أو الإشراف عليها.

لا يجوز معالجة البيانات الشخصية الحساسة التي يتم جمعها لأغراض التوظيف إلا في حالات معينة ووفقاً للضمانات المنصوص عليها في القانون المحلي. ولا يمكن لأصحاب العمل أن يسألوا الموظفين أو المتقدمين للوظيفة عن حالتهم الصحية أو أن يفحصوهم طبياً إلا عند الضرورة. وقد يتم ذلك من أجل: تحديد مدى ملاءمتهم للتوظيف؛ أو استيفاء متطلبات الطب الوقائي؛ أو حماية المصالح الحيوية لأصحاب البيانات أو غيرهم من الموظفين والأفراد؛ أو تمكين منح المزايا الاجتماعية؛ أو الرد على الطلبات القضائية. ولا يجوز جمع بيانات الصحة من مصادر أخرى غير الموظف المعني، إلا في حالة الحصول على موافقة صريحة ومستنيرة أو عندما ينص القانون الوطني على ذلك.

بموجب توصية التوظيف، ينبغي إبلاغ الموظفين بالغرض من معالجة بياناتهم الشخصية، ونوع البيانات الشخصية التي يتم جمعها، والجهات التي يتم إرسال البيانات إليها بانتظام، والغرض من هذه الإفصاحات وأساسها القانوني. ولا يجوز الوصول إلى الاتصالات الإلكترونية في مكان العمل إلا لأسباب أمنية أو لأسباب مشروعة أخرى، ولا يُسمح بهذا الوصول إلا بعد إبلاغ الموظفين بأن صاحب العمل يمكنه الوصول إلى هذا النوع من الاتصالات.

يجب أن يكون للموظفين الحق في الوصول إلى بيانات التوظيف الخاصة بهم وكذلك الحق في تصحيحها أو محوها. وإذا تمت معالجة البيانات الحاملة لأحكام القيمة، يجب أن يكون للموظفين، علاوة على الحقوق المذكورة، الحق في الطعن في أحكام القيمة تلك. ولكن يمكن تقييد هذه الحقوق مؤقتاً لأغراض التحقيقات الداخلية. وإذا رُفض طلب الموظف للوصول إلى بيانات التوظيف الشخصية أو تصحيحها أو محوها، فيجب أن ينص القانون الوطني على الإجراءات المناسبة للطعن في هذا الرفض.

## 3.9.بيانات الصحة

### النقاط الرئيسية

• البيانات الطبية هي بيانات حساسة وبالتالي تتمتع بحماية خاصة.

تنطبق على البيانات الشخصية المتعلقة بصحة صاحب البيانات صفة البيانات الحساسة بموجب المادة 9 (1) من اللائحة العامة لحماية البيانات وبموجب المادة 6 من الاتفاقية 108 المحدثة. وبناءً على ذلك، تخضع البيانات المتعلقة بالصحة لنظام معالجة بيانات أكثر صرامة من البيانات غير الحساسة. وتحظر اللائحة العامة لحماية البيانات معالجة «البيانات الشخصية المتعلقة بالصحة» (التي يُفهم على أنها «جميع البيانات المتعلقة بالحالة الصحية لصاحب البيانات والتي تكشف عن معلومات تتعلق بحالة الصحة البدنية أو العقلية السابقة أو الحالية أو المستقبلية لصاحب البيانات»)[934]، وكذلك البيانات الجينية والبيانات البيومترية، ما لم يكن مصرحاً بذلك بموجب المادة 9 (2). وقد تم إضافة كلا هذين النوعين من البيانات إلى قائمة «الفئات الخاصة من البيانات».[935]

مثال: في قضية «ز ضد فنلندا»،[936] ارتكب الزوج السابق للمدعية، والذي كان مصاباً بفيروس نقص المناعة البشرية، عدداً من الجرائم الجنسية. وأدين بعد ذلك بالقتل غير العمد على أساس أنه عرّض ضحاياه عن علم لخطر الإصابة بفيروس نقص المناعة البشرية. وأمرت المحكمة الوطنية بأن يظل الحكم الكامل ووثائق القضية سرية لمدة 10 سنوات على الرغم من الطلبات المقدمة من المدعية لإبقائها سرية لفترة أطول. ولكن محكمة الاستئناف رفضت هذه الطلبات، واحتوى حكمها على الاسمين الكاملين للمدعية وزوجها السابق. رأت المحكمة الأوروبية لحقوق الإنسان أن هذا التدخل لم يكن ضرورياً في مجتمع ديمقراطي، لأن حماية البيانات الطبية لها أهمية أساسية في ما يتعلق بالتمتع بالحق في احترام الحياة الخاصة والعائلية، ولا سيما عندما يتعلق الأمر بالمعلومات المتعلقة بالإصابة بفيروس نقص المناعة البشرية، بالنظر إلى وصمة العار المرتبطة بهذه الحالة في كثير من المجتمعات. لذلك، خلصت المحكمة إلى أن السماح بالوصول إلى حكم محكمة الاستئناف، الذي وصف هوية المدعية وحالتها الطبية، بعد 10 سنوات فقط من إصدار الحكم من شأنه أن ينتهك المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان.

بموجب **قانون الاتحاد الأوروبي**، تسمح المادة 9 (2) (ح) من اللائحة العامة لحماية البيانات بمعالجة البيانات الطبية حيثما كان ذلك مطلوباً لأغراض الطب الوقائي أو التشخيص الطبي أو توفير الرعاية أو العلاج أو إدارة خدمات الرعاية الصحية .ولكن لا يُسمح بإجراء هذه المعالجة إلا إذا قام بها أخصائي في مجال الرعاية الصحية يخضع لالتزام السرية المهنية، أو من قبل شخص آخر يخضع لالتزام مماثل.

بموجب **قانون مجلس أوروبا**، تطبّق توصية مجلس أوروبا بشأن البيانات الطبية لسنة 1997 مبادئ الاتفاقية 108 على معالجة البيانات في المجال الطبي بقدر أكبر من التفصيل.[937] وتتوافق القواعد المقترحة مع تلك الخاصة باللائحة العامة لحماية البيانات فيما يتعلق بالأغراض المشروعة لمعالجة البيانات الطبية، والتزامات السرية المهنية اللازمة للأشخاص الذين يستخدمون بيانات الصحة، وحقوق أصحاب البيانات في الشفافية والوصول والتصحيح والمحو. علاوة على ذلك، لا يجوز نقل البيانات الطبية التي تتم معالجتها بشكل قانوني من قبل اختصاصي الرعاية الصحية إلى سلطات إنفاذ القانون ما لم يتم توفير «ضمانات كافية لمنع الإفشاء غير المتسق مع احترام [...] الحياة الخاصة المكفول بموجب المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان».[938] كما يجب «صياغة القانون الوطني بدقة كافية وتوفير الحماية القانونية الكافية ضد التعسف».[939]

[934] اللائحة العامة لحماية البيانات، الحيثية 35.

[935] نفس المرجع السابق، المادة 2.

[936] المحكمة الأوروبية لحقوق الإنسان، قضية «ز ضد فنلندا»، رقم 22009/93، 25 فبراير 1997، الفقرتان 94 و112؛ انظر أيضاً المحكمة الأوروبية لحقوق الإنسان، قضية «م. س. ضد السويد»، رقم 20837/92، 27 أغسطس 1997؛ المحكمة الأوروبية لحقوق الإنسان، قضية «ل.ل. ضد فرنسا»، رقم 7508/02، 10 أكتوبر 2006؛ المحكمة الأوروبية لحقوق الإنسان، قضية «أ ضد فنلندا»، رقم 20511/03، 17 يوليو 2008؛ المحكمة الأوروبية لحقوق الإنسان، قضية «ك.هـ. وآخرون ضد سلوفاكيا»، رقم 32881/04، 28 أبريل 2009؛ المحكمة الأوروبية لحقوق الإنسان، قضية «شولوك ضد المملكة المتحدة»، رقم 36936/05، 2 يونيو 2009.

[937] مجلس أوروبا، لجنة الوزراء (1997)، التوصية Rec(97)5 الموجهة إلى الدول الأعضاء بشأن حماية البيانات الطبية، 13 فبراير 1997. تجدر الإشارة إلى أن هذه التوصية قيد التنقيح.

[938] المحكمة الأوروبية لحقوق الإنسان، قضية «أفيلكينا وآخرون ضد روسيا»، رقم 1585/09، 6 يونيو 2013، الفقرة 53. انظر أيضاً المحكمة الأوروبية لحقوق الإنسان، قضية «بيربوك ضد ليتوانيا»، رقم 23373/03، 25 نوفمبر 2008.

[939] المحكمة الأوروبية لحقوق الإنسان، قضية «ل.هـ. ضد لاتفيا»، رقم 52019/07، 29 أبريل 2014، الفقرة 59.

بالإضافة إلى ذلك، تتضمن توصية البيانات الطبية مقتضيات خاصة بشأن البيانات الطبية للأطفال الذين لم يولدوا بعد والأشخاص العاجزين، وبشأن معالجة البيانات الجينية. ويُعترف بالبحث العلمي صراحةً على أنه سبب للاحتفاظ بالبيانات لفترة أطول مما هو مطلوب، إلا أن ذلك يتطلب عادة إخفاء مصدر البيانات. تقترح المادة 12 من توصية البيانات الطبية لوائح مفصلة للحالات التي يحتاج فيها الباحثون إلى البيانات الشخصية وتكون فيها البيانات مخفية المصدر غير كافية.

قد يكون استعمال الأسماء المستعارة وسيلة مناسبة لتلبية الاحتياجات العلمية وفي نفس الوقت حماية مصالح المرضى المعنيين. وقد تم شرح مفهوم استعمال الاسم المستعار في سياق حماية البيانات بشكل مفصل في الجزء 2.1.1.

تنطبق توصية مجلس أوروبا لسنة 2016 بشأن البيانات الناتجة عن الاختبارات الجينية أيضاً على معالجة البيانات في المجال الطبي.[940] وتُعد هذه التوصية ذات أهمية كبيرة فيما يخص الصحة الإلكترونية (eHealth)، حيث تُستخدم تكنولوجيا المعلومات والاتصالات لتسهيل الرعاية الطبية. من بين الأمثلة على ذلك إرسال نتائج اختبار أبوة خاص بمريض ما من مقدم رعاية صحية إلى آخر. تهدف هذه التوصية إلى حماية حقوق الأشخاص الذين تتم معالجة بياناتهم الشخصية لأغراض التأمين ضد المخاطر المتعلقة بصحة الشخص أو سلامته الجسدية أو عمره أو وفاته. وتحتاج شركات التأمين إلى تبرير معالجة البيانات المتعلقة بالصحة وينبغي أن يكون التبرير متناسباً مع طبيعة وأهمية المخاطر التي يتم النظر فيها. تعتمد معالجة هذا النوع من البيانات على موافقة صاحب البيانات. وينبغي أن يكون لدى شركات التأمين أيضاً ضمانات لتخزين البيانات المتعلقة بالصحة.

إن التجارب السريرية - التي تنطوي على تقييم آثار الأدوية الجديدة على المرضى في بيئات بحثية موثقة - لها آثار كبيرة على حماية البيانات. وتخضع التجارب السريرية للمنتجات الطبية للاستخدام البشري للائحة (الاتحاد الأوروبي) رقم 536/2014 الصادرة عن البرلمان الأوروبي والمجلس بتاريخ 16 أبريل 2014 بشأن التجارب السريرية على المنتجات الطبية للاستخدام البشري، والمُلغية للأمر التوجيهي EC/2001/20 (لائحة التجارب السريرية). إن العناصر الرئيسية للائحة التجارب السريرية هي:

- إجراءات طلب مبسطة عبر بوابة الاتحاد الأوروبي؛[942]
- المواعيد النهائية لتقييم طلب التجارب السريرية؛[943]
- لجنة أخلاقيات كجزء من عملية التقييم، وفقاً لقانون الدول الأعضاء (والقانون الأوروبي المحدّد للفترات الزمنية المعنية)؛[944]
- تحسين شفافية التجارب السريرية ونتائجها.[945]

تنص اللائحة العامة لحماية البيانات بصورة محددة على أنه، لأغراض الموافقة على المشاركة في أنشطة البحث العلمي في التجارب السريرية، يتم تطبيق اللائحة (الاتحاد الأوروبي) رقم 536/2014.[946]

إن العديد من المبادرات التشريعية وغيرها من المبادرات الأخرى بشأن البيانات الشخصية في قطاع الصحة معلقة حالياً على مستوى الاتحاد الأوروبي.[947]

### سجلات الصحة الإلكترونية

تُعرَّف سجلات الصحة الإلكترونية على أنها «سجل طبي شامل، أو ما يقوم مقامه من وثائق مشابهة، للحالة الصحية الجسدية والعقلية السابقة والحالية للفرد في صيغة إلكترونية، وتوفر هذه البيانات بسهولة لأغراض العلاج الطبي ولأغراض أخرى وثيقة الصلة بهذا الغرض».[948]

---

[940] مجلس أوروبا، لجنة الوزراء (2016)، التوصية Rec(2016)8 الموجهة إلى الدول الأعضاء بشأن معالجة البيانات الشخصية المتعلقة بالصحة لأغراض التأمين، بما في ذلك البيانات الناتجة عن الاختبارات الجينية، 26 أكتوبر 2016.

[941] اللائحة (الاتحاد الأوروبي) رقم 536/2014 للبرلمان الأوروبي والمجلس المؤرخة في 16 أبريل 2014 بشأن التجارب السريرية على المنتجات الطبية للاستخدام البشري، والمَلغية للأمر التوجيهي EC/2001/20. (لائحة التجارب السريرية)، الجريدة الرسمية L 158 2014 OJ.

[942] لائحة التجارب السريرية، المادة 5 (1).

[943] نفس المرجع السابق، المادة 5 (2)-(5).

[944] نفس المرجع السابق، المادة 2، الفقرة 2 (11).

[945] نفس المرجع السابق، المادة 9 (1) والحيثية 67.

[946] اللائحة العامة لحماية البيانات، الحيثيتان 156 و161.

[947] المشرف الأوروبي على حماية البيانات (2013)، رأي المشرف الأوروبي على حماية البيانات في رسالة المفوضية بشأن «خطة عمل الصحة الإلكترونية 2012-2020 - الرعاية الصحية المبتكرة للقرن الحادي والعشرين، بروكسل، 27 مارس 2013.

[948] توصية المفوضية المؤرخة في 2 يوليو 2008 بشأن قابلية التشغيل البيني عبر الحدود لأنظمة سجلات الصحة الإلكترونية، النقطة 3 (ج).

إن سجلات الصحة الإلكترونية عبارة عن نسخ إلكترونية للسيرة المرضية للمرضى وقد تتضمن بيانات سريرية تتعلق بهؤلاء الأفراد، مثل السيرة المرضية الماضية، والمشاكل والحالات، والأدوية والعلاجات، بالإضافة إلى نتائج وتقارير الفحوصات والمختبرات. يمكن للطبيب العام والصيدلي وغيرهما من مهنيي الرعاية الصحية الولوج إلى تلك الملفات الإلكترونية التي تتنوع من سجلات كاملة إلى مجرد مقتطفات أو موجزات. ويتطرق مفهوم 'الصحة الإلكترونية' أيضاً إلى تلك السجلات الصحية.

مثال: حصل السيد أ على وثيقة تأمين من الشركة ب، المؤمن. سيجمع الأخير بعض المعلومات المرتبطة بالصحة عن السيد أ مثل المشاكل الصحية أو الأمراض التي يعاني منها حالياً. وينبغي للمؤمن أن يخزن البيانات الشخصية المتعلقة بصحة السيد أ في معزل عن غيرها من البيانات، ويحتاج المؤمن أيضاً إلى تخزين البيانات الشخصية المتعلقة بالصحة بمعزل عن غيرها من البيانات الشخصية. ويعني ذلك أن المعني بتدبير ملف السيد أ وحده من سيلج إلى البيانات المتعلقة بصحة السيد أ.

ومع ذلك، تثير الملفات الصحية الإلكترونية بعضاً من المسائل المتعلقة بحماية البيانات مثل قابلية الولوج إليها والتخزين اللائق بها وولوج صاحبها إليها.

بالإضافة إلى السجلات الصحية الإلكترونية، نشرت المفوضية الأوروبية في 10 أبريل 2014 ورقة خضراء حول الخدمات والبيانات الصحية المدعومة بالأجهزة المحمولة (mHealth)، معتبرةً أن هذه الأخيرة تُعد مجالاً ناشئاً وسريع النمو له القدرة على تغيير منظومة الرعاية الصحية وزيادة فعاليتها وجودتها. ويشمل المصطلح المذكور الممارسة الصحية العامة والطبية التي تدعمها الأجهزة النقالة مثل الهواتف النقالة وأجهزة مراقبة حالة المرضى وأجهزة المساعدة الرقمية الشخصية وغيرها من الأجهزة اللاسلكية، بالإضافة إلى التطبيقات (على سبيل المثال، تطبيقات الصحة الجيدة) التي بإمكانها الاتصال بالأجهزة الطبية أو أجهزة الاستشعار.[949]

ويُحدّد الكتاب الأخضر المخاطر التي تهدد الحق في حماية البيانات الشخصية التي قد تترتب عن تطوير الخدمات والبيانات الصحية المدعومة بالأجهزة المحمولة، وتنص على أنه نظراً إلى الطبيعة الحساسة للبيانات الصحية، ينبغي أن يحتوي التطوير على ضمانات أمنية محددة ومناسبة لصالح بيانات المريض مثل التشفير وآليات مناسبة للتحقق من هوية المريض للتخفيف من حدة الأخطار الأمنية. ويُعد الامتثال لقواعد حماية البيانات الشخصية، بما في ذلك الالتزام بتزويد المعني بالبيانات بالمعلومات ذات الصلة، وأمن البيانات ومبدأ المعالجة المشروعة للبيانات الشخصية، أمراً بالغ الأهمية لبناء الثقة في حلول الخدمات والبيانات الصحية المدعومة بالأجهزة المحمولة.[950]

تحقيقاً لتلك الغاية، تمت صياغة مدونة لقواعد السلوك من قبل الفاعلين في ذلك المجال، اعتماداً على إسهامات مجموعة واسعة من الجهات المعنية تضم ممثلين ذوي خبرة في حماية البيانات والتنظيم الذاتي والمشترك وتكنولوجيا المعلومات والاتصالات والرعاية الصحية.[951] في الوقت الذي صيغ فيه الدليل، كان مشروع مدونة قواعد السلوك قد قُدم إلى فريق عمل المادة 29 لإبداء تعليقاته عليه،وينتظر الموافقة الرسمية عليه.

[949] المفوضية الأوروبية (2014)، ورقة خضراء حول الخدمات والبيانات الصحية المدعومة بالأجهزة المحمولة («mHealth»)، النسخة النهائية219 (2014)COM ، بروكسيل، 10 أبريل 2014.

[950] نفس المرجع السابق، ص. 8.

[951] مشروع مدونة قواعد السلوك بشأن تطبيقات الخدمات والبيانات الصحية المدعومة بالأجهزة المحمولة، 07 يونيو 2016.

## 4.9. معالجة البيانات لأغراض البحث والإحصاء

### النقاط الرئيسية

- لا يجوز استخدام البيانات التي جُمعت لأغراض الإحصاء أو البحث العلمي أو التاريخي لأي غرض آخر.
- يجوز استخدام البيانات التي جُمعت بصفة مشروعة لاحقا لأغراض الإحصاء أو البحث العلمي أو التاريخي، شريطة وجود الضمانات الكافية. تحقيقاً لذلك الغرض، يمكن اللجوء إلى إخفاء مصدر البيانات أو استخدام اسم مستعار للبيانات لتوفير تلك الضمانات قبل إرسال البيانات إلى أطراف ثالثة.

يسمح **قانون الاتحاد الأوروبي** بمعالجة البيانات لأغراض الإحصاء أو البحث العلمي أو التاريخي، شريطة وجود الضمانات المناسبة لحقوق أصحاب البيانات وحرياتهم، وقد تشمل تلك الضمانات استخدام اسم مستعار للبيانات.[952] وقد ينص قانون الاتحاد الأوروبي أو القانون الوطني على استثناءات معينة تتعلق بحقوق أصحاب البيانات إذا كان من المحتمل أن تحول تلك الحقوق دون تحقيق الغرض الشرعي للبحث، أو تضر به إضراراً خطيراً.[953] ويمكن استنباط الاستثناءات من حق صاحب البيانات في الولوج والحق في التصحيح والحق في تقييد المعالجة والحق في الاعتراض.

ومع العلم أن البيانات التي جمعها المراقب بصفة قانونية لأي غرض من الأغراض يجوز إعادة استخدامها من طرف ذلك المراقب لأغراض الإحصاء أو البحث العلمي أو التاريخي، إلا أنه يجب إخفاء مصدر تلك البيانات أو إخضاعها لتدابير مثل استخدام اسم مستعار للبيانات، حسب السياق، قبل إرسالها إلى طرف ثالث لأغراض الإحصاء أو البحث العلمي أو التاريخي، إلا في حالة توفر موافقة صاحب البيانات أو وجود تنصيص محدد حول هذه النقطة في التشريع الوطني. وتظل البيانات المحمية باسم مستعار خاضعة للائحة العامة لحماية البيانات، خلافاً للبيانات المجهولة المصدر.[954]

لهذا فإن اللائحة تولي مجال الدراسة والبحث معاملةً خاصة فيما يتعلق بقواعد حماية البيانات العامة، وذلك تفادياً للتضييق على تطور البحوث وامتثالاً لهدف تحقيق فضاء البحوث الأوروبي، كما هو منصوص عليه في المادة 179 من المعاهدة المنظمة لعمل الاتحاد الأوروبي، حيث تنص على التفسير الواسع لمعالجة البيانات الشخصية لأغراض البحث العلمي، بما في ذلك تطوير التكنولوجيا وتطبيقها والبحث الأساسي والبحث التطبيقي والبحث الممول من قبل القطاع الخاص. وتقر أيضاً بأهمية جمع البيانات في سجلات لأغراض البحث والصعوبة الممكنة في التحديد الكامل للغرض اللاحق لمعالجة البيانات الشخصية لأغراض البحث العلمي وقت جمع البيانات.[955] لهذا السبب، تجيز اللائحة معالجة البيانات لتلك الأغراض، دون موافقة صاحب البيانات، شريطة توفر الضمانات المناسبة.

من الأمثلة الهامة عن استخدام البيانات لأغراض الإحصاء إعداد الإحصاءات الرسمية والتي تحصل عليها مكاتب الإحصاءات الوطنية ومكاتب الإحصاءات التابعة للاتحاد الأوروبي وفقاً للقوانين الوطنية وقوانين الاتحاد الأوروبي بشأن الإحصاءات الرسمية.

واستناداً إلى تلك القوانين، عادة ما يلتزم المواطنون والمؤسسات التجارية بالكشف عن البيانات للسلطات الإحصائية المعنية. ويلتزم المسؤولون العاملون في مكاتب الإحصاء بالتزامات السرية المهنية الخاصة التي يجب الامتثال لها امتثالاً لائقاً، نظراً لأهميتها البالغة في إرساء القدر الكبير من الثقة التي ينبغي أن يشعر بها المواطن حين تصبح بياناته متاحة للسلطات الإحصائية.[956]

تتضمن اللائحة (الجماعة الأوروبية) رقم 223/2009 المتعلقة بالإحصاءات الأوروبية (اللائحة المتعلقة بالإحصاءات الأوروبية) قواعد أساسية لحماية البيانات في سياق الإحصاءات الرسمية ولذلك يجوز احتسابها أيضاً ذات صلة بالمقتضيات المتعلقة بالإحصاءات الرسمية التي يتم إعدادها

[952] اللائحة العامة لحماية البيانات، المادة 89 (1).
[953] نفس المرجع السابق، المادة 89 (2).
[954] نفس المرجع السابق، الحيثية 26.
[955] نفس المرجع السابق، الحيثيات 33 و157 و159.
[956] نفس المرجع السابق، المادة 90.

على الصعيد الوطني.[957] وتواصل اللائحة العمل بالمبدأ القائل بأن النشاط الإحصائي الرسمي يحتاج إلى أساس قانوني واضح بما فيه الكفاية.[958]

مثال: في قضية **«هوبر ضد جمهورية ألمانيا الاتحادية»**،[959] اشتكى رجل أعمال نمساوي كان قد انتقل إلى ألمانيا من أن جمع وتخزين البيانات الشخصية للمواطنين الأجانب من قبل السلطات الألمانية في سجل موحد (AZR) ولو لأغراض إحصائية قد انتهك حقوقه بمقتضى الأمر التوجيهي الخاص بحماية البيانات. باعتبارها أن الأمر التوجيهي 95/46 يهدف إلى ضمان مستوىً متكافئ من حماية البيانات في جميع الدول الأعضاء، قضت محكمة العدل التابعة للاتحاد الأوروبي بأنه لضمان مستوىً عالٍ من الحماية في الاتحاد الأوروبي، لا يمكن لمفهوم الضرورة الوارد في المادة 7 (ه) أن يكون له معنىً مختلفاً بين الدول الأعضاء. ولذلك يُعد مفهوماً له معناه المستقل في قانون الاتحاد الأوروبي، ويجب تفسيره بما يجسد تماماً غاية الأمر التوجيهي 95/46. وقضت المحكمة الأوروبية بأن السجل الألماني لم يتوافق مع شرط الضرورة بموجب المادة 7 (ه)، مسجلةً أن المعلومات المجهولة المصدر هي وحدها التي ينبغي المطالبة بها لأغراض الإحصاء.

في سياق **مجلس أوروبا**، يمكن إجراء المزيد من معالجة البيانات لأغراض الإحصاء أو البحث العلمي أو التاريخي حينما يكون ذلك من أجل المصلحة العامة ، ويجب أن يخضع للضمانات المناسبة.[960] ويجوز أيضاً تقييد حقوق أصحاب البيانات عند معالجة البيانات لأغراض الإحصاء، شريطة انعدام خطر يمكن التعرف عليه من شأنه أن ينتهك حقوقهم وحرياتهم.[961]

تشمل التوصية المتعلقة بالبيانات الإحصائية الصادرة في 1997 أداء النشاط الإحصائي في القطاعين العام والخاص.[962]

لا يجوز استخدام البيانات التي جمعها المراقب لأغراض الإحصاء لأي غرض آخر. وتكون البيانات التي جُمعت لأغراض غير إحصائية متاحة لمزيد من الاستخدام الإحصائي. وتسمح التوصية المتعلقة بالبيانات الإحصائية أيضاً بنقل البيانات إلى أطراف ثالثة، شريطة أن يكون ذلك لأغراض الإحصاء فحسب. في تلك الحالات، ينبغي للأطراف أن توافق على نطاق الاستخدام الإضافي الشرعي للإحصاءات وتحدده كتابة. ونظراً إلى أن ذلك لا يمكن له أن يحل محل موافقة صاحب البيانات - عند الاقتضاء - يجب النص على ضمانات مناسبة في القانون الوطني للتقليل من أخطار سوء استخدام البيانات الشخصية مثل الالتزام بإخفاء مصدر البيانات أو استخدام اسم مستعار للبيانات قبل الكشف عنها.

يجب أن يلتزم مهنيو البحث الإحصائي بالتزامات السرية المهنية الخاصة بموجب القانون الوطني، كما هو الشأن دائماً فيما يخص الإحصاءات الرسمية. ويجب أن ينصرف ذلك أيضاً على المستجوِبين وغيرهم من جامعي البيانات الشخصية في حال تم توظيفهم من أجل جمع بيانات من أصحاب البيانات أنفسهم أو غيرهم من الأشخاص.

إذا كان القانون لا يجيز الاستطلاع الإحصائي باستخدام البيانات الشخصية، قد يتوجب على أصحاب البيانات الموافقة على استخدام بياناتهم لجعله شرعياً، أو قد يحتاجون إلى منحهم فرصة للاعتراض. إذا قام المستجوِبون بجمع البيانات لأغراض الإحصاء، يجب إخبارهم إخباراً واضحاً بما إذا كان التزويد بالبيانات إجبارياً أم لا بموجب القانون الوطني.

عندما يتعذر القيام باستطلاع إحصائي باستخدام بيانات مجهولة المصدر، وتكون البيانات الشخصية ضرورية، يجب إخفاء مصدر البيانات التي جُمعت لذلك الغرض في أسرع وقت ممكن. ولا يجب أن تمكن نتائج الاستطلاع الإحصائي، على الأقل، من تحديد هوية أي أصحاب بيانات، ما لم يكن من الواضح أن ذلك لا يمثل أي خطر.

بعد الانتهاء من الاستطلاع الإحصائي، ينبغي إما حذف البيانات الشخصية المستخدمة وإما إخفاء مصدرها. في حالات مثل هذه، تنصح التوصية المتعلقة بالبيانات الإحصائية بوجوب تخزين بيانات تحديد الهوية بمعزل عن غيرها من البيانات الشخصية. ويعني ذلك، على سبيل المثال، أن مفتاح التشفير أو القائمة المتضمنة لمرادفات تحديد الهوية يجب تخزينها بمعزل عن غيرها من البيانات.

[957] اللائحة (الجماعة الأوروبية) رقم 223/2009 الصادرة عن البرلمان الأوروبي والمجلس في 11 مارس 2009 بشأن الإحصاءات الأوروبية والملغية للائحة (EC, Euratom) رقم 1101/2008 الصادرة عن البرلمان الأوروبي والمجلس بشأن إرسال البيانات الخاضعة للسرية الإحصائية إلى مكتب الإحصاءات التابع للجماعات الأوروبية، لائحة المجلس (الجماعة الأوروبية) رقم 322/97 بشأن إحصاءات الجماعة، وقرار المجلس 89/382/EEC، اليوراتوم، الذي يؤسس لجنة بشأن البرامج الإحصائية للجماعات الأوروبية، الجريدة الرسمية L 87 2009 OJ، كما هو معدل باللائحة (الاتحاد الأوروبي) رقم 2015/759 الصادرة عن البرلمان الأوروبي والمجلس 29 أبريل 2015 المعدل للائحة (الجماعة الأوروبية) رقم 223/2009 بشأن الإحصاءات الأوروبية، الجريدة الرسمية L 123 2015 OJ.

[958] سيتم تناول ذلك المبدأ بمزيد من التفصيل في مدونة المكتب الإحصائي للجماعات الأوروبية لقواعد الممارسة التي تقدم، وفقاً للمادة 11 من اللائحة المتعلقة بالإحصاءات الأوروبية، إرشادات أخلاقية بشأن كيفية القيام بالإحصاءات الرسمية، بما في ذلك من استخدام منصف للبيانات الشخصية.

[959] محكمة العدل التابعة للاتحاد الأوروبي، القضية C-524/06، «هاينتز هوبر ضد جمهورية ألمانيا الاتحادية» [الغرفة الكبرى]، 16 ديسمبر 2008؛ إطلع خصوصاً على الفقرة 68.

[960] الاتفاقية المحدثة 108، المادة 5 (4) (ب).

[961] نفس المرجع السابق، المادة 11 (2).

[962] مجلس أوروبا، اللجنة الوزارية (1997)، التوصية 18 Rec(97) الموجهة إلى الدول الأعضاء بشأن حماية البيانات التي تُجمع وتُعالج لأغراض الإحصاء، 30 سبتمبر 1997.

## 5.9. البيانات المالية

### النقاط الرئيسية

- على الرغم من أن البيانات المالية لا تُعد بيانات حساسة بمقتضى الاتفاقية المحدثة 108 أو اللائحة العامة لحماية البيانات، إلا أن معالجتها تتطلب ضمانات خاصة لضمان صحة البيانات وأمنها.
- تحتاج أنظمة الدفع الإلكترونية خصوصاً إلى حماية مدمجة للبيانات ، أي حماية الخصوصية أو البيانات منذ التصميم وتلقائياً.
- قد تنشأ مشاكل خاصة تتعلق بحماية البيانات في ذلك المجال لسبب الحاجة إلى وجود آليات التحقق من الهوية المناسبة.

مثال: في قضية **«ميشو ضد فرنسا»**،[963] طعن المدعي، وهو محام فرنسي، في التزامه بموجب القانون الفرنسي بالإبلاغ عن الشبهات المتعلقة بأنشطة غسل الأموال المحتملة من قبل موكليه. ولاحظت المحكمة الأوروبية لحقوق الإنسان أن إلزام المحامين بشرط إبلاغ السلطات الإدارية بمعلومات تتعلق بشخص آخر، والتي كانوا قد حصلوا عليها من خلال المبادلات المهنية، شكل تدخلاً في حق المحامين في احترام مراسلاتهم وحياتهم الخاصة بموجب المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان، لأن ذلك المفهوم شمل أنشطة ذات طبيعة مهنية أو تجارية. مع ذلك، لم يخالف التدخل القانون وسعى إلى تحقيق هدف شرعي، وهو منع حدوث الاضطرابات والجرائم. ونظراً إلى أن المحامين لا يخضعون للالتزام بالإبلاغ عن النشاط المشبوه إلا في ظروف محددة جداً، قضت المحكمة الأوروبية بأن ذلك الالتزام كان متناسباً واستنتجت عدم انتهاك المادة 8.

مثال: في قضية **«م. ن. وآخرون ضد سان مارينو»**،[964] أبرم المدعي، وهو مواطن إيطالي، اتفاقاً ائتمانياً مع شركة كانت قيد التحقيق. ويعني ذلك أن الشركة خضعت لتفتيش نسخ من الوثائق (الإلكترونية) وحجزها. وقدم المدعي شكوىً إلى محكمة سان مارينو، مدعياً عدم وجود صلة بينه وبين الجرائم المزعومة. ومع ذلك، حكمت المحكمة بعدم قبول شكواه، لأنه لم يكن «طرفاً معنياً». وقضت المحكمة الأوروبية لحقوق الإنسان بأن المدعي كان في موقف غير مؤات إلى حد بعيد فيما يتعلق بالحماية القضائية مقارنة بـ»طرف معني»، ومع ذلك كانت بياناته ما تزال خاضعة لعمليات التفتيش والحجز. ولذلك قضت المحكمة بانتهاك المادة 8.

مثال: في قضية **«ج. س. ب. ضد سويسرا»**،[965] أُرسلت بيانات الحساب المصرفي الذي يملكه المدعي إلى السلطات الضريبية الأمريكية استناداً إلى اتفاق التعاون الإداري بين سويسرا والولايات المتحدة. وقضت المحكمة الأوروبية لحقوق الإنسان بأن ذلك الإرسال لم ينتهك المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان لأن التدخل في حق المدعي في الخصوصية نص عليه القانون وسعى إلى تحقيق هدف مشروع، وكان متناسباً مع المصلحة العامة المعنية.

أُعد تطبيق الإطار القانوني العام لحماية البيانات (كما هو محدد في الاتفاقية 108) على سياق المدفوعات من قبل **مجلس أوروبا** في التوصية Rec(90)19 لسنة 1990.[966] وتوضح التوصية مدى الجمع والاستخدام المشروعين للبيانات في سياق المدفوعات، لا سيما بوسيلة بطاقات الدفع. وتزود أيضاً المشرعين الوطنيين بتوصيات مفصلة بشأن قواعد الكشف عن بيانات الدفع للأطراف الثالثة وآجال الاحتفاظ بالبيانات والشفافية وأمن البيانات وتدفقات البيانات عبر الحدود والإشراف وسبل الانتصاف. وكوّن مجلس أوروبا أيضاً رأياً عن نقل البيانات الضريبية،[967] والذي يقدم التوصيات والمسائل التي تجب مراعاتها عند تناول نقل البيانات الضريبية.

تجيز المحكمة الأوروبية لحقوق الإنسان إرسال البيانات المالية - لا سيما بيانات الحساب المصرفي للفرد - بموجب المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان، إذا كان منصوص عليه بموجب القانون ويسعى إلى تحقيق هدف مشروع ومتناسب مع المصلحة العامة المعنية.[968]

[963] المحكمة الأوروبية لحقوق الإنسان، «ميشود ضد فرنسا»، القضية رقم 12323/11، 06 ديسمبر 2012. اطلع أيضاً على المحكمة الأوروبية لحقوق الإنسان، «نيميتز ضد ألمانيا»، القضية رقم 13710/88، 16 ديسمبر 1992، الفقرة 29 والمحكمة الأوروبية لحقوق الإنسان، «هالفورد ضد المملكة المتحدة»، القضية رقم 20605/92، 25 يونيو 1997، الفقرة 42.

[964] المحكمة الأوروبية لحقوق الإنسان، «م. ن. وآخرون ضد سان مارينو»، القضية 28005/12، 07 يوليو 2015.

[965] المحكمة الأوروبية لحقوق الإنسان، «ج. س. ب. ضد سويسرا»، القضية رقم 28601/11، 22 ديسمبر 2015.

[966] مجلس أوروبا، اللجنة الوزارية (1990)، التوصية رقم R(90)19 بشأن حماية البيانات الشخصية المستخدمة للدفع وما يرتبط به من عمليات أخرى، 13 سبتمبر 1990.

[967] مجلس أوروبا، اللجنة الاستشارية للاتفاقية 108 (2014)، الرأي المتعلق الأثر على حماية البيانات الناشئ عن آليات المبادلات الآلية للبيانات بين الدول لأغراض إدارية وضريبية، 04 يونيو 2014.

[968] المحكمة الأوروبية لحقوق الإنسان، «ج. س. ب. ضد سويسرا»، القضية رقم 28601/11، 22 ديسمبر 2015.

من ناحية قانون **الاتحاد الأوروبي**، يجب أن تمتثل أنظمة الدفع الإلكترونية التي تنطوي على معالجة البيانات الشخصية للائحة العامة لحماية البيانات. لذلك، يجب أن تضمن تلك الأنظمة حماية البيانات منذ التصميم وتلقائياً. وتلزم حماية البيانات منذ التصميم المراقب باتخاذ التدابير التقنية والتنظيمية المناسبة لتنفيذ مبادئ حماية البيانات. ويُقصد بحماية البيانات تلقائياً أنه يجب على المراقب أن يضمن أن البيانات الشخصية التي تُعد ضرورية لغرض معين وحدها ما يمكن معالجته تلقائياً (اطلع على الجزء 4.4). وفيما يتعلق بالبيانات المالية، قضت محكمة العدل التابعة للاتحاد الأوروبي بأن البيانات الضريبية التي نُقلت قد تمثل بيانات شخصية.[969] وأصدر فريق عمل المادة 29 المبادئ التوجيهية ذات الصلة والتي تهم الدول الأعضاء، بما في ذلك معايير لضمان الامتثال لقواعد حماية البيانات عند التبادل التلقائي للبيانات الشخصية لأغراض ضريبية بوسائل آلية.[970] بالإضافة إلى ذلك، سَن عدد من الصكوك القانونية لتنظيم الأسواق المالية وأنشطة مؤسسات الائتمان وشركات الاستثمار.[971] وتساعد صكوك قانونية أخرى على مكافحة تداولات المطلعين من الداخل والتلاعب بالأسواق.[972] وفيما يلي المجالات الرئيسية التي لها أثر على حماية البيانات:

- الاحتفاظ بسجلات عن المعاملات المالية؛
- ونقل البيانات الشخصية إلى بلدان ثالثة؛
- وتسجيل المحادثات الهاتفية أو الاتصالات الإلكترونية، بما في ذلك صلاحية السلطات المختصة لطلب سجلات المكالمات الهاتفية وحركة البيانات؛
- والكشف عن المعلومات الشخصية، بما في ذلك نشر العقوبات؛
- والصلاحيات الإشرافية والتحقيقية للسلطات المختصة، بما في ذلك عمليات التفتيش في عين المكان ودخول المباني الخاصة لحجز الوثائق؛
- وآليات الإبلاغ عن الخروقات، أي مخططات الإبلاغ عن المخالفات؛
- والتعاون بين السلطات المختصة التابعة للدول الأعضاء والهيئة الأوروبية للأوراق المالية والأسواق (ESMA).

وتم تناول مسائل أخرى في هذه المجالات تناولاً محدداً، بما في ذلك جمع البيانات عن الوضع المالي لأصحاب البيانات[973] أو الدفع عبر الحدود عن طريق التحويلات المصرفية، ما يفضي حتماً إلى تدفقات البيانات الشخصية.[974]

---

[969] محكمة العدل التابعة للاتحاد الأوروبي، القضية C-201/14، «سمارانداً بارا وآخرون ضد الصندوق الوطني للتأمين الصحي وآخرين»، 01 أكتوبر 2015، الفقرة 29.

[970] فريق عمل المادة 29 بشأن حماية البيانات (2015)، بيان فريق عمل المادة 29 بشأن المبادلات الآلية بين الدول لأغراض ضريبية، WP 230/14 EN.

[971] الأمر التوجيهي EU/2014/65 الصادر عن البرلمان الأوروبي والمجلس في 15 مايو 2014 بشأن أسواق الصكوك المالية والمعدل للأمرين التوجيهيين EC/2002/92 وEU/2011/61، الجريدة الرسمية 173 L 2014 OJ؛ لائحة (الاتحاد الأوروبي) رقم 600/2014 الصادرة عن البرلمان الأوروبي والمجلس في 15 مايو 2014 بشأن أسواق الصكوك المالية والمعدل للائحة (الاتحاد الأوروبي) رقم 648/2012، الجريدة الرسمية 173 L 2014 OJ؛ الأمر التوجيهي EU/2013/36 الصادر عن البرلمان الأوروبي والمجلس في 26 يونيو 2013 بشأن الولوج إلى نشاط مؤسسات الائتمان والإشراف الاحترازي على مؤسسات الائتمان وشركات الاستثمار والمعدل للأمر التوجيهي EC/2002/87 والملغي للأمرين التوجيهيين EC/2006/48 وEC/2006/49، الجريدة الرسمية 176 L 2013 OJ.

[972] لائحة (الاتحاد الأوروبي) رقم 596/2014 الصادرة عن البرلمان الأوروبي والمجلس في 16 أبريل 2014 بشأن إساءة استغلال السوق (اللائحة المتعلقة بإساءة استغلال السوق) والملغية للأمر التوجيهي EC/2003/06 الصادرة عن البرلمان الأوروبي والمجلس وللأوامر التوجيهية الصادرة عن المفوضية EC/2003/124 وEC/2003/125 وEC/2004/72، الجريدة الرسمية 173 L 2014 OJ.

[973] اللائحة (الجماعة الأوروبية) رقم 1060/2009 الصادرة عن البرلمان الأوروبي والمجلس في 16 سبتمبر 2009 بشأن وكالات تقدير الجدارة الائتمانية، الجريدة الرسمية L 2009 OJ 302 والمعدل حديثاً بالأمر التوجيهي EU/2014/51 الصادر عن البرلمان الأوروبي والمجلس في 16 أبريل 2014 والمعدل للأمرين التوجيهيين EC/2003/71 وEC/2009/138 واللوائح (الجماعة الأوروبية) رقم 1060/2009 و(الاتحاد الأوروبي) رقم 1094/2010 و(الاتحاد الأوروبي) رقم 1095/2010 فيما يتعلق بصلاحيات الهيئة الإشرافية الأوروبية (الهيئة الأوروبية للتأمين ومعاشات التقاعد المهنية) والهيئة الإشرافية الأوروبية (الهيئة الأوروبية للأوراق المالية والأسواق)، الجريدة الرسمية 153 L 2014 OJ؛ اللائحة (الاتحاد الأوروبي) رقم 462/2013 الصادرة عن البرلمان الأوروبي والمجلس في 21 مايو 2013 والمعدل للائحة (الجماعة الأوروبية) رقم 1060/2009 بشأن وكالات تقدير الجدارة الائتمانية، الجريدة الرسمية 2013 OJ 146 L.

[974] الأمر التوجيهي EC/2007/64 الصادر عن البرلمان الأوروبي والمجلس في 13 نوفمبر 2007 بشأن خدمات الدفع في السوق الداخلية والمعدل للأوامر التوجيهية EC/97/7 وEC/2002/65 وEC/2005/60 وEC/2006/48 والملغي للأمر التوجيهي EC/97/5، الجريدة الرسمية 319 L 2007 OJ، كما هو معدل بالأمر التوجيهي EC/2009/111 الصادر عن البرلمان الأوروبي والمجلس في 16 سبتمبر 2009 والمعدل للأوامر التوجيهية EC/2006/48 وEC/2006/49 وEC/2007/64 فيما يتعلق بالمصارف التابعة للمؤسسات المركزية، وبعض عناصر الأموال الخاصة، والتعرضات الكبيرة لتذبذبات السوق، والترتيبات الإشرافية، وإدارة الأزمات، الجريدة الرسمية 302 L 2009 OJ.

# 10

# التحديـــات الحديثـــة في حمايـــة البيانـــات الشخصيـــة

يتميز العصر الرقمي أو عصر تكنولوجيا المعلومات بشيوع استخدام الحواسيب والإنترنت والتكنولوجيات الرقمية وينطوي على جمع كميات ضخمة من البيانات ومعالجتها، بما في ذلك البيانات الشخصية. ويعني جمع البيانات الشخصية ومعالجتها في اقتصاد العولمة تزايد أعداد تدفقات البيانات عبر الحدود. ويمكن لتلك المعالجة أن تجلب فوائد هامة وواضحة في الحياة اليومية: تيسر محركات البحث الولوج إلى كميات كبيرة من المعلومات والمعارف وتمكن خدمات شبكات التواصل الاجتماعي الناس في جميع أنحاء العالم من التواصل والتعبير عن آرائهم وحشد الدعم للقضايا الاجتماعية والبيئية والسياسية، في حين يستفيد المستهلكون والشركات من تقنيات التسويق الفعالة والكفؤة التي تعزز الاقتصاد. وتُعد التكنولوجيا ومعالجة البيانات الشخصية أيضاً أدوات لا يمكن للسلطات الحكومية الاستغناء عنها في مكافحتها للجرائم والإرهاب. وعلى غرار ذلك، فإن البيانات الضخمة - جمع كميات كبيرة من المعلومات وتخزينها وتحليلها لتحديد الأنماط والتنبؤ بالسلوك - «يمكن أن يكون مصدراً ذا قيمة كبيرة للمجتمع ويحسن الإنتاجية وأداء القطاع العام والمشاركة الاجتماعية»،[975]

على الرغم من مزاياه الكثيرة، يفرض العصر الرقمي أيضاً تحديات على الخصوصية وحماية البيانات، نظراً إلى جمع كميات ضخمة من المعلومات الشخصية ومعالجتها بطرق تزداد تعقداً وغموضاً. وأدى التقدم التكنولوجي إلى تطوير مجموعات من البيانات الضخمة التي يسهل تدقيقها وإخضاعها لمزيد من التحليل للبحث عن أنماط ما أو لاعتماد قرارات تستند إلى الخوارزميات، ما يكسب معارف متبصرة لم يسبق لها مثيل في السلوك البشري والحياة الخاصة.[976]

تُعد التكنولوجيات الجديدة قوية وبإمكانها أن تكون خطيرة على وجه الخصوص إن وقعت بين أياد غير آمنة. وتُعد السلطات الحكومية القائمة بأنشطة المراقبة الجماعية التي قد تستخدم تلك التكنولوجيات مثالاً على الأثر الهام الذي قد تحدثه تلك التكنولوجيات على حقوق الأفراد. في 2013، أثارت تسريبات إدوارد سنودن بشأن تشغيل برامج مراقبة الإنترنت والهاتف واسعة النطاق من قبل وكالات الاستخبارات في بعض الدول مخاوف كبيرة بخصوص الأخطار التي تسببها أنشطة المراقبة للخصوصية والحكم الديموقراطي وحرية التعبير. وقد تمس المراقبة الجماعية والتكنولوجيات التي تسمح بالتخزين والمعالجة المعولمين للمعلومات الشخصية والولوج إلى البيانات بالجملة بجوهر الحق في الخصوصية.[977] بالإضافة إلى ذلك، قد يكون لها أثراً سيئاً على الثقافة السياسية وأثراً مخيفاً على الديمقراطية والإبداع والابتكار.[978] إن مجرد الخوف من أن الدولة قد تستمر في تعقب سلوك المواطنين وأفعالهم وتحليلها يمكن له أن يثنيهم عن التعبير عن آرائهم في قضايا معينة وينشأ عنه الاحتياط والحذر،[979] وحثت تلك التحديات عدداً من السلطات العامة ومراكز البحوث ومنظمات المجتمع المدني على تحليل

[975] مجلس أوروبا، اللجنة الاستشارية للاتفاقية 108، الأوامر التوجيهية بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية في عالم البيانات الضخمة، T-PD (2017)01، ستراسبورغ، 23 يناير 2017.

[976] البرلمان الأوروبي (2017)، القرار المتعلق بآثار البيانات الضخمة على الحقوق الأساسية: الخصوصية وحماية البيانات وعدم التمييز والأمن وإنفاذ القانون (2017)0076_TA-PROV_P8، ستراسبورغ، 14 مارس 2017.

[977] إطلع على الأمم المتحدة، الجمعية العمومية، تقرير المقرر الخاص المعني بتعزيز حقوق الإنسان والحريات الأساسية وحمايتها مع التصدي للإرهاب، بين إميرسون، 23 A/69/397، سبتمبر 2014، الفقرة 59. إطلع أيضاً على المحكمة الأوروبية لحقوق الإنسان، صحيفة الوقائع بشأن المراقبة الجماعية، يوليو 2017.

[978] المشرف الأوروبي على حماية البيانات (2015)، مواجهة تحديات البيانات الضخمة، الرأي 7/2015، بروكسيل، 19 نوفمبر 2015.

[979] إطلع خصوصاً على محكمة العدل التابعة للاتحاد الأوروبي، القضيتان المضمومتان C-293/12 وC-594/12، «الحقوق الرقمية أيرلندا» ضد وزير المواصلات والموارد البحرية والطبيعية وآخرين وحكومة ولاية كيرنتن وآخرين» [الغرفة الكبرى]، 08 أبريل 2014، الفقرة 37.

الآثار الممكنة للتكنولوجيات الجديدة على المجتمع. في 2015، أطلق المشرف الأوروبي على حماية البيانات عدة مبادرات هدفت إلى تقييم أثر البيانات الضخمة وإنترنت الأشياء على الأخلاقيات وأنشأت، على وجه الخصوص، فريقاً استشارياً معنياً بالأخلاقيات يهدف إلى تحفيز «نقاش مفتوح ومستنير عن الأخلاقيات الرقمية، والذي يمكن الاتحاد الأوروبي من جني فوائد التكنولوجيا على المجتمع والاقتصاد ويعزز في الآن ذاته حقوق الأفراد وحرياتهم، لا سيما حقوقهم في الخصوصية وحماية البيانات.[980]

تُعد معالجة البيانات الشخصية أيضاً أداة قوية في أيدي الشركات ويمكن لها في الوقت الحاضر أن تكشف عن معلومات مفصلة عن صحة الشخص أو حالته المالية، وهي المعلومات التي تستخدمها الشركات لاحقاً لاتخاذ قرارات هامة تخص الأفراد مثل أقساط التأمين الصحي التي ستُطبق عليهم أو على جدارتهم الائتمانية. وقد يكون أيضاً لتقنيات معالجة البيانات أثراً على العمليات الديمقراطية، عند استخدامها من قبل السياسيين والشركات للتأثير على الانتخابات - على سبيل المثال، من خلال «الاستهداف الفئوي» لاتصالات الناخبين. بعبارة أخرى، في حين كان يُنظر إلى الخصوصية في بادئ الأمر على أنها حق حماية الأفراد من التدخل غير المبرر للسلطات العامة ،فإنها في العصر الحديث، قد تكون مهددة من قبل قدرات القطاع الخاص. ويطرح ذلك أسئلة عن استخدام التكنولوجيا والتحليل التنبئي في اتخاذ القرارات التي تؤثر في حياة الأفراد اليومية ويعزز الحاجة إلى ضمان احترام أي معالجة للبيانات الشخصية لمقتضيات الحقوق الأساسية.

ترتبط حماية البيانات ارتباطاً جوهرياً بالتغير التكنولوجي والاجتماعي والسياسي ولذلك سيستحيل وضع قائمة بالتحديات مستقبلاً. ويبحث هذا الفصل في مجالات مختارة تتعلق بالبيانات الضخمة وشبكات التواصل الاجتماعي عبر الإنترنت والسوق الأوروبية الرقمية الموحدة. إنه ليس تقييماً شاملاً لتلك المجالات من وجهة نظر حماية البيانات، وإنما يسلط الضوء بدلاً عن ذلك على العديد من التفاعلات المحتملة بين الأنشطة البشرية الجديدة والمراجعة وبين حماية البيانات.

## 1.10. البيانات الضخمة والخوارزميات والذكاء الاصطناعي

### النقاط الرئيسية

- تعمل الابتكارات المربكة في مجال تكنولوجيا المعلومات والاتصالات على تشكيل نمط حياة جديد حيث ترتبط العلاقات الاجتماعية والأعمال التجارية والخدمات العامة والخاصة ارتباطاً رقمياً، ما يولد كمية كبيرة من البيانات تزداد باستمرار، ويكون الكثير منها بيانات شخصية.
- يزداد اشتغال الحكومات والمقاولات والمواطنين في اقتصاد يعتمد على البيانات، والذي أصبحت فيه البيانات نفسها موجودات قيمة.
- يحيل مفهوم البيانات الضخمة على كل من البيانات والدراسات التحليلية المتعلقة بها.
- تقع البيانات الشخصية المعالجة من خلال الدراسات التحليلية للبيانات الضخمة ضمن تشريعات الاتحاد الأوروبي ومجلس أوروبا.
- تقتصر الاستثناءات المتعلقة بقواعد حماية البيانات وبحقوقها على حقوق مختارة وحالات معينة حيث يكون إنفاذ حق ما مستحيلاً أو يتطلب جهوداً غير متناسبة من قبل المراقبين.
- يُحظر عموماً اتخاذ القرارت آلياً حظراً تاماً، باستثناء حالات معينة.
- يُعد وعي الأفراد وممارستهم للمراقبة أمرين أساسيين لضمان إنفاذ القانون.

في عالمنا الذي يزداد رقمنة، يترك كل نشاط أثراً رقمياً يمكن جمعه ومعالجته وتقييمه أو تحليله. بوجود تكنولوجيات المعلومات والاتصالات الجديدة، يتم جمع المزيد والمزيد من البيانات وتسجيلها.[981] إلى وقت قريب، لم تكن أي تكنولوجيا قادرة على تحليل هاته الكمية من البيانات أو تقييمها أو استخلاص استنتاجات مفيدة. وكانت البيانات ببساطة أكثر من أن يتم تقييمها وأكثر تعقيداً وأكثر رداءة من حيث التنظيم وأكثر سرعة من حيث الحركة من أن يتم تحديد الاتجاهات والعادات.

[980] المشرف الأوروبي على حماية البيانات، القرار الصادر في 03 ديسمبر 2015 والمؤسس لفريق استشاري خارجي معني بالأبعاد الأخلاقية لحماية البيانات ("الفريق الاستشاري المعني بالأخلاقيات")، 03 ديسمبر 20015، الحيثية 5.

[981] المفوضية الأوروبية، رسالة من المفوضية إلى البرلمان الأوروبي ومجلس أوروبا واللجنة الأوروبية الاقتصادية والاجتماعية ولجنة المناطق من أجل اقتصاد بيانات مزدهر، النسخة النهائية442 (2014)COM ، بروكسيل، 02 يوليو 2014.

## 1.1.10. تعريف البيانات الضخمة والخوارزميات والذكاء الاصطناعي

**البيانات الضخمة**

يُعد مصطلح «البيانات الضخمة» كلمة طنانة قد تحيل على عدة مفاهيم، اعتماداً على السياق. وعادة ما يشمل «القدرة التكنولوجية المتنامية على جمع المعارف الجديدة والتنبئية ومعالجتها واستخلاصها من بيانات تتسم بضخامة كميتها وسرعتها وتنوعها».[982] ولذلك يشمل مفهوم البيانات الضخمة سواء البيانات نفسها والدراسات التحليلية المرتبطة بها.

تتنوع **مصادر** البيانات وتشمل الأشخاص وبياناتهم الشخصية والآلات وأجهزة الاستشعار والمعلومات المناخية وصور الأقمار الصناعية والصور والفيديوهات الرقمية أو إشارات نظام تحديد المواقع العالمي. ومع ذلك، فإن قدراً كبيراً من البيانات والمعلومات يُعد بيانات شخصية - سواء كان ذلك اسماً أو صورة فوتوغرافية أو عنوان بريد إلكتروني أو بيانات مصرفية أو بيانات التعقب التي يزودها نظام تحديد المواقع العالمي أو المنشورات على مواقع شبكات التواصل الاجتماعي أو المعلومات الطبية أو عنوان بروتوكول الإنترنت الخاص بالحاسوب.[983]

تحيل البيانات الضخمة أيضاً إلى **معالجة** كميات البيانات والمعلومات المتاحة وتحليلها وتقييمها، أي إلى الحصول على معلومات مفيدة لأغراض تحليل البيانات الضخمة. ويعني ذلك أن البيانات والمعلومات التي جُمعت قد تُستخدم لأغراض غير تلك الأغراض المقصودة منها أصلاً، مثل الاتجاهات الإحصائية أو المزيد من الخدمات المصممة تصميماً خاصاً مثل الإعلانات. في الواقع، حينما تعمل التكنولوجيات حقاً على جمع البيانات الضخمة ومعالجتها وتقييمها، يمكن الجمع بين أي نوع من المعلومات وإعادة تقييمها: المعاملات المالية أو الجدارة الائتمانية أو العلاج الطبي أو الاستهلاك الخاص أو النشاط المهني أو التعقب والطرق المستخدمة أو استخدام الإنترنت أو البطاقات الإلكترونية والهواتف الذكية أو مراقبة الفيديو أو الاتصالات. ويجلب تحليل البيانات الضخمة بعداً كمياً جديداً للبيانات يمكن تقييمه واستخدامه آنياً على سبيل المثال لتقديم الخدمات المصممة خصيصاً للمستهلكين.

**الخوارزميات والذكاء الاصطناعي**

يشير الذكاء الاصطناعي (AI) إلى ذكاء الآلات التي تتصرف بصفتها «ذوات ذكية»، إذ يمكن لبعض الأجهزة، بصفتها ذوات ذكية، وبدعم من البرمجيات، أن تدرك بيئتها المحيطة وتتصرف وفقاً للخوارزميات. ويُطبق مصطلح الذكاء الاصطناعي عندما تحاكي الآلة الوظائف «المعرفية» - مثل التعلم وحل المشاكل - التي تكون عادة مرتبطة بالأشخاص الطبيعيين.[984] ولكي تحاكي اتخاذ القرارات، تستخدم التكنولوجيات الحديثة والبرمجيات الخوارزميات التي تستخدمها الأجهزة لاتخاذ «قرارات آلية». ويُستحسن وصف الخوارزمية بإجراء تدريجي للحساب ومعالجة البيانات والتقييم والتعليل واتخاذ القرارات الآليين.

وعلى غرار الدراسات التحليلية المرتبطة بالبيانات الضخمة، يتطلب الذكاء الاصطناعي واتخاذ القرارات الآلية الذي ينتجه جمع كميات كبيرة من البيانات ومعالجتها. ويمكن أن تصدر تلك البيانات عن الجهاز نفسه (حرارة المكابح أو الوقود وغير ذلك) أو عن البيئة المحيطة. ويُعد التنميط، على سبيل المثال، عملية قد تعتمد على اتخاذ القرارات الآلية وفقاً للأنماط أو العوامل المحددة مسبقاً.

---

[982] مجلس أوروبا، اللجنة الاستشارية للاتفاقية 108، المبادئ التوجيهية بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية في عالم البيانات الضخمة، 23 يناير 2017، في ص. 2؛ المفوضية الأوروبية، رسالة من المفوضية الأوروبية إلى البرلمان الأوروبي ومجلس أوروبا والمجلس الأوروبي الاقتصادي والاجتماعي ولجنة المناطق من أجل اقتصاد بيانات مزدهر، النسخة النهائية442 (2014)COM ، بروكسيل، 02 يوليو 2014، في ص. 4؛ الاتحاد الدولي للاتصالات (2015)، التوصية Y.3600، البيانات الضخمة - المقتضيات والقدرات المؤسسة على الحوسبة السحابية.

[983] صحيفة القوائم لمفوضية الاتحاد الأوروبي بشأن إصلاحات الاتحاد الأوروبي في مجال حماية البيانات والبيانات الضخمة؛ مجلس أوروبا، اللجنة الاستشارية للاتفاقية 108، المبادئ التوجيهية بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية في عالم البيانات الضخمة، 23 يناير 2017، في ص. 2.

[984] ستيوارت راسل وبيتر نورفيغ، الذكاء الاصطناعي: مقاربة حديثة (الطبعة الثانية)، 2003، دار النشر «أبر سادل ريفر»، نيوجيرسي: برنتيس هول، ص. 27، 58-32، 972-968؛ ستيوارت راسل وبيتر نورفيغ، الذكاء الاصطناعي: مقاربة حديثة (الطبعة الثالثة)، 2009، دار النشر «أبر سادل ريفر»، نيوجيرسي: برنتيس هول، ص. 2.

مثال: التنميط والإعلانات المستهدفة

ينطوي التنميط المستند إلى البيانات الضخمة على البحث عن أنماط تتجسد فيها «خصائص نوع من الشخصية» - على سبيل المثال، عندما تقترح شركات التسوق الإلكتروني منتجات «قد تنال إعجابك أيضاً» استناداً إلى معلومات جُمعت من المنتجات التي وُضعت سابقاً في عربة التسوق الخاصة بالعميل. كلما ازدادت البيانات، يزداد وضوح تنوعها. ويُعد الهاتف الذكي، على سبيل المثال، استبياناً قوياً يملأه الأفراد مع كل استعمال سواء عن وعي أو دون وعي.

تستخدم السيكوغرافيا الحديثة - وهي علم دراسة الشخصيات - طريقة السمات الشخصية الخمسة (the OCEAN method) التي يُستند إليها لتحديد أنواع الشخصيات التي يُتعامل معها. وتتعلق الأبعاد 'الخمسة الكبرى' للشخصية بالانفتاح (مدى انفتاح الشخص على التجارب) والضمير المهني (مدى قرب الشخص من الكمال) والانبساط (مدى كون الشخص اجتماعياً) والوفاق (مدى قبول الشخص) والعصابية (مدى هشاشة الشخص). وتحدد هذه المعلومات نمط الشخص المعني وحاجاته ومخاوفه وكيفية تصرفه وغير ذلك. ويتم حينها استكمالها بغيرها من المعلومات المتعلقة بالشخص، يتم الحصول عليها من أي مصادر متاحة مثل وسطاء البيانات أو شبكات التواصل الاجتماعي (بما في ذلك نقرات «الإعجاب» التي حظيت بها المنشورات والصور الفوتوغرافية المنشورة) أو الموسيقى التي يُستمع إليها عبر الإنترنت أو بيانات التعقب ونظام تحديد المواقع العالمي.

وتُقارن لاحقاً كمية الملفات الشخصية التي أُنشئت من خلال تقنيات تحليل البيانات الضخمة لتحديد أنماط مشابهة ولتفسير مجموعات من الشخصيات. ونتيجة لذلك، يتم قلب المعلومات المتعلقة بسلوك بعض الشخصيات ومواقفها. وبالولوج إلى البيانات الضخمة واستخدامها، يتم قلب اختبار الشخصية بمعلومات تتعلق بالسلوك والموقف تُستخدم الآن لوصف شخصية الفرد. وبامتلاك المعلومات التي جُمع بينها والمتعلقة بـنقرات «الإعجاب» في شبكات التواصل الاجتماعي أو بيانات التعقب أو الموسيقى المُستمع إليها أو الأفلام التي شوهدت، قد تبرز صورة واضحة عن شخصية الفرد تسمح للمؤسسات التجارية بإرسال إعلانات و/أو معلومات مصممة خصيصاً لـ»شخصية» ذلك الفرد. والأهم من ذلك كله هو أنه يمكن معالجة تلك المعلومات معالجةً آنية.[985]

## 2.1.10. التوفيق بين مزايا البيانات الضخمة وأخطارها

يمكن لتقنيات المعالجة الحديثة تناول كميات كبيرة من البيانات واستيراد بيانات جديدة بسرعة وإتاحة معالجة آنية للمعلومات من حيث مدة الاستجابة القصيرة (حتى في حالة الطلبات المعقدة) وإتاحة إمكانية الطلبات المتعددة والمتزامنة، ويمكن لها تحليل أنواع مختلفة من المعلومات (الصور الفوتوغرافية أو النصوص أو الأعداد). تمكن تلك الابتكارات التكنولوجية من تنظيم كميات البيانات والمعلومات ومعالجتها وتقييمها آنياً.[986] وبالزيادة المطردة لكمية البيانات المتاحة والتي تم تحليلها، أصبح الآن من الممكن تحقيق النتائج التي كان سيستحيل تحقيقها بتحليل أصغر نطاقاً. وساعدت البيانات الضخمة على تطوير مجال جديد من الأعمال التجارية حيث قد تنشأ خدمات جديدة تُقدم للمؤسسات التجارية والمستهلكين على حد سواء. ويمكن لقيمة البيانات الشخصية لمواطني الاتحاد الأوروبي أن تنمو إلى ما يقارب واحد تريليون يورو سنوياً بحلول 2020. [987] لذلك، قد تتيح البيانات الضخمة **فرصاً** جديدة ناشئة عن تقييم كمية البيانات لاكتساب رؤى اجتماعية أو اقتصادية أو علمية يمكن لها أن تفيد الأفراد والمؤسسات التجارية والحكومات على حد سواء.[988]

---

[985] تقيم تقنيات المعالجة والبرمجيات الجديدة المعلومات المتعلقة بما ينال إعجاب الشخص وتدرس وقت التسوق عبر الإنترنت أو الإضافات إلى عربة التسوق عبر الإنترنت آنياً وتقترح «منتجات» قد تثير الاهتمام استناداً إلى المعلومات التي جُمعت.

[986] مازال تطوير برمجيات لمعالجة البيانات الضخمة في مرحلة مبكرة. ومع ذلك، تم حديثاً تطوير البرامج التحليلية، لا سيما لتحليل البيانات والمعلومات الضخمة المتعلقة بأنشطة الأفراد تحليلاً آنياً. وأتاحت إمكانية تحليل البيانات الضخمة ومعالجتها بطريقة منظمة وسائل جديدة للتنميط والإعلانات المستهدفة. المفوضية الأوروبية، رسالة من المفوضية إلى البرلمان الأوروبي ومجلس أوروبا واللجنة الأوربية الاقتصادية والاجتماعية ولجنة المناطق من أجل اقتصاد بيانات مزدهر، النسخة النهائية442 (2014)COM ، بروكسيل، 02 يوليو 2014؛ صحيفة الوقائع لمفوضية الاتحاد الأوروبي بشأن إصلاحات الاتحاد الأوروبي في مجال حماية البيانات والبيانات الضخمة ومجلس أوروبا، المبادئ التوجيهية بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية في عالم البيانات الضخمة، 23 يناير 2017، في ص. 2.

[987] صحيفة الوقائع لمفوضية الاتحاد الأوروبي بشأن إصلاحات الاتحاد الأوروبي في مجال حماية البيانات والبيانات الضخمة.

[988] المؤتمر الدولي للمفوضين المعنيين بحماية البيانات والخصوصية (2014)، قرار بشأن البيانات الضخمة والمفوضية الأوروبية، رسالة من المفوضية إلى البرلمان الأوروبي ومجلس أوروبا واللجنة الأوروبية الاقتصادية والاجتماعية ولجنة المناطق من أجل اقتصاد بيانات مزدهر، النسخة النهائية442 (2014)COM ، بروكسيل، 02 يوليو 2014، في ص. 2؛ صحيفة الوقائع لمفوضية الاتحاد الأوروبي بشأن إصلاحات الاتحاد الأوروبي في مجال حماية البيانات والبيانات الضخمة ومجلس أوروبا، المبادئ التوجيهية بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية في عالم البيانات الضخمة، 23 يناير 2017، في ص. 1.

ويمكن للدراسات التحليلية للبيانات الضخمة أن تكشف عن أنماط بين مختلف المصادر ومجموعات البيانات، ما يسمح باكتساب رؤى مفيدة في مجالات مثل العلم والطب. ويصدق ذلك، على سبيل المثال، في مجالات مثل الصحة أو الأمن الغذائي أو أنظمة النقل الذكية أو الكفاءة الطاقية أو التخطيط العمراني. ويمكن استخدام التحليل الآني للمعلومات لتحسين الأنظمة التي تم تنفيذها.

وفي مجال الأبحاث، يمكن اكتساب رؤى مفيدة جديدة بالجمع بين كميات كبيرة من البيانات والتقييمات الإحصائية، لا سيما في التخصصات التي تم فيها تقييم قدر كبير من البيانات، إلى اليوم، يدوياً فحسب. ويمكن تطوير علاجات جديدة مصممة لكي تلائم كل مريض على حدة استناداً إلى المقارنات بكمية المعلومات المتاحة. وتأمل الشركات في أن يمكنها تحليل البيانات الضخمة من اكتساب ميزة تنافسية وتحقيق مدخرات ممكنة وخلق مجالات جديدة من الأعمال التجارية من خلال خدمة العملاء المباشرة والفردية. وتأمل الوكالات الحكومية في تحقيق تحسينات في مجال العدالة الجنائية. وتقر استراتيجية المفوضية لإنشاء سوق رقمية موحدة لأوروبا بإمكانية التكنولوجيات التي تعتمد على البيانات والخدمات والبيانات الضخمة لتحفيز النمو الاقتصادي والابتكار والرقمنة في الاتحاد الأوروبي.[989]

ومع ذلك، تنطوي البيانات الضخمة على **أخطار** ترتبط عموماً بـ»خصائصها الثلاثة»: حجم البيانات المعالجة وسرعتها وتنوعها. ويحيل الحجم على كمية البيانات المعالجة، ويحيل التنوع على عدد البيانات وتنوعها، في حين تحيل السرعة على سرعة معالجة البيانات. وتنشأ اعتبارات محددة لحماية البيانات خصوصاً عندما يُستخدم تحليل البيانات على مجموعات كبيرة من البيانات لاستخلاص معارف تنبئية جديدة لأغراض اتخاذ القرارات المتعلقة بالأفراد و/أو المجموعات.[990] وتم إبراز الأخطار التي تهدد حماية البيانات والخصوصية فيما يتعلق بالبيانات الضخمة في آراء المشرف الأوروبي على حماية البيانات وفريق عمل المادة 29 وقرارات البرلمان الأوروبي ووثائق سياسات مجلس أوروبا.[991]

قد تشمل الأخطار سوء تناول البيانات الضخمة من قبل أولئك الذين يستطيعون الولوج إلى إجمالي المعلومات من خلال التلاعب أو التمييز أو قمع الأفراد أو جماعات محددة في المجتمع.[992] عندما تُجمع كميات البيانات الشخصية عن السلوك الفردي وتُعالج وتُقيم، فإن استغلالها قد يفضي إلى انتهاكات جسيمة للحقوق والحريات الأساسية تتجاوز الحق في الخصوصية. ولا يمكن قياس مدى تأثر الخصوصية والبيانات الشخصية قياساً مضبوطاً. وحدد البرلمان الأوروبي انعدام منهجية لتقييم الأثر الإجمالي للبيانات الضخمة تقييماً مستنداً إلى الأدلة، لكن ثمة أدلة تبرهن على أن الدراسات التحليلية للبيانات الضخمة قد يكون لها أثر أفقي هام سواءً في القطاع العام أو القطاع الخاص.[993]

وتتضمن اللائحة العامة لحماية البيانات مقتضيات بشأن الحق في عدم التعرض لاتخاذ القرارات الآلي، بما في ذلك التنميط.[994] وتُثار مسألة الخصوصية عندما تتطلب ممارسة الحق في الاعتراض تدخلاً بشرياً، ما يسمح لأصحاب البيانات بالتعبير عن آرائهم والاعتراض على القرار.[995] ويمكن لذلك أن يفضي إلى بروز تحديات فيما يخص ضمان مستوىً كاف من حماية البيانات الشخصية إذا استحال، على سبيل المثال، أي تدخل بشري أو عندما تكون الخوارزميات معقدة جداً وتكون كمية البيانات ذات الصلة أكبر من أن تُقدم للأفراد تبريرات لقرارات معينة و/أو معلومات مسبقة للحصول على موافقتهم. وهناك مثال على استخدام الذكاء الاصطناعي في اتخاذ القرار بشكل آلي نجده في التطورات الأخيرة التي عرفتها طلبات القروض العقارية أو عمليات الاستقدام لملء الشواغر (التوظيفات)، حيث تُرفض الطلبات استناداً إلى عدم استيفاء مقدمي الطلبات للمقاييس والعوامل المحددة مسبقاً.

---

[989] قرار البرلمان الأوروبي الصادر في 14 مارس 2017 بشأن آثار البيانات الضخمة على الحقوق الأساسية: الخصوصية وحماية البيانات وعدم التمييز والأمن وإنفاذ القانون (2016/2225 (INI)).

[990] مجلس أوروبا، اللجنة الاستشارية للاتفاقية 108، المبادئ التوجيهية بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية في عالم البيانات الضخمة، 23 يناير 2017، في ص. 2.

[991] إطلع، على سبيل المثال، على المشرف الأوروبي على حماية البيانات (2015)، التحدي لتحديات البيانات الضخمة، الرأي 7/2015، 19 نوفمبر 2015؛ المشرف الأوروبي على حماية البيانات (2016)، الإنفاذ المنسجم للحقوق الأساسية في عصر البيانات الضخمة، الرأي 8/2016، 23 سبتمبر 2016؛ البرلمان الأوروبي (2016)، القرار المتعلق بآثار البيانات الضخمة على الحقوق الأساسية: الخصوصية وحماية البيانات وعدم التمييز والأمن وإنفاذ القانون، 0076(2017)P8_TA، ستراسبورغ، 14 مارس 2017؛ مجلس أوروبا، اللجنة الاستشارية للاتفاقية 108، المبادئ التوجيهية بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية في عالم البيانات الضخمة، 01(2017)T-PD، ستراسبورغ، 23 يناير 2017.

[992] المؤتمر الدولي للمفوضين المعنيين بالخصوصية وحماية البيانات (2014)، القرار المتعلق بالبيانات الضخمة.

[993] قرار البرلمان الأوروبي الصادر في 14 مارس 2017 بشأن آثار البيانات الضخمة على الحقوق الأساسية: الخصوصية وحماية البيانات وعدم التمييز والأمن وإنفاذ القانون (2016/2225 (INI)).

[994] اللائحة العامة لحماية البيانات، المادة 22.

[995] نفس المرجع السابق، المادة 22 (3).

## 3.1.10. مسائل متعلقة بحماية البيانات

فيما يخص حماية البيانات، تتعلق المسائل الرئيسية بحجم وتنوع البيانات الشخصية التي تُعالج، من ناحية، والمعالجة ونتائجها، من ناحية أخرى. إن إدخال خوارزميات وبرمجيات معقدة لتحويل البيانات الضخمة إلى وسيلة لاتخاذ القرارات هو أمر يؤثر على الأفراد والجماعات خصوصاً، لا سيما في حالات التنميط أو التوسيم، وهو ما يثير في نهاية المطاف إشكاليات كثيرة تتعلق بحماية البيانات.

**تحديد هوية المراقبين والمعالجين ومسؤوليتهم**

ويطرح الذكاء الاصطناعي والبيانات الضخمة أسئلة عديدة تتعلق بتحديد هوية المراقبين والمعالجين ومسؤوليتهم: عندما تُجمع تلك الكمية من البيانات وتُعالج، من يكون مالك تلك البيانات؟ وعندما تُعالج البيانات بآلات وبرمجيات ذكية، من يكون المراقب؟ وما هي المسؤوليات المحددة لكل فاعل في المعالجة؟ وما هي الأغراض التي قد تستدعي استخدام البيانات الضخمة؟

ستصبح إشكالية المسؤولية في سياق الذكاء الاصطناعي أشد صعوبة حينما يتخذ الذكاء الاصطناعي قراراً يستند إلى معالجة البيانات التي طورها بنفسه. وتقدم اللائحة العامة لحماية البيانات إطاراً قانونياً يخص مسؤولية مراقب البيانات ومعالج البيانات. وتؤدي المعالجة غير المشروعة للبيانات الشخصية إلى نشوء مسؤولية مراقب البيانات ومعالج البيانات. ويثير الذكاء الاصطناعي واتخاذ القرارات آلياً تساؤلات حول العاتق الذي تقع عليه مسؤولية الانتهاكات التي تمس خصوصية أصحاب البيانات في الحالات التي يتعذر فيها نسب تلك المسؤولية على وجه اليقين، نظراً لكمية البيانات التي عولجت ومدى تشابكها. وعندما يُعد الذكاء الاصطناعي والخوارزميات منتجات، فإن ذلك يثير سؤالاً حول المسؤولية الشخصية التي تنظمها اللائحة العامة لحماية البيانات ون المسؤولية عن المنتج التي لا تنظمها اللائحة.[998] ويقتضي ذلك قواعد بشأن المسؤولية عن سد الفجوة بين المسؤولية الشخصية والمسؤولية عن المنتج فيما يخص الروبوتات والذكاء الاصطناعي، بما في ذلك اتخاذ القرارات آلياً، على سبيل المثال.[999]

**التأثير على مبادئ حماية البيانات**

تتحدى طبيعة البيانات الضخمة الموصوفة سلفاً وتحليلها واستخدامها تطبيق بعض من المبادئ التقليدية والأساسية لقانون حماية البيانات الأوروبي.[1000] وتتعلق تلك التحديات أساساً بمبادئ المشروعية وتقليل البيانات وحصر الغرض والشفافية.

يقتضي مبدأ تقليل البيانات أن تكون البيانات الشخصية ملائمة وذات صلة ومقتصرة على ما هو ضروري للأغراض التي استدعت معالجتها. ومع ذلك، قد يكون نموذج الأعمال الخاص بالبيانات الضخمة نقيض تقليل البيانات، نظراً إلى أنه يتطلب المزيد والمزيد من البيانات لأغراض غير محددة في غالب الأحيان.

وينطبق الأمر نفسه على مبدأ حصر الغرض الذي يقتضي وجوب معالجة البيانات لأهداف محددة وعدم استخدام البيانات لأغراض لا تتوافق مع الغرض الأولي من جمعها، ما لم تكن تلك المعالجة قائمة على أساس قانوني - على سبيل المثال، لا الحصر، موافقة المعني بالبيانات. (إطلع على الجزء 1.1.4)

أخيراً، تتحدى البيانات الضخمة مبدأ صحة البيانات لأن تطبيقات البيانات الضخمة تميل إلى جمع البيانات من مصادر متنوعة دون وجود إمكانية التحقق من صحة البيانات التي جُمعت و/أو الحفاظ عليها.[1001]

---

998 مجلس أوروبا، اللجنة الاستشارية للاتفاقية 108، المبادئ التوجيهية بشأن حماية الأفراد فيما يتعلق بحماية البيانات الشخصية في عالم البيانات الضخمة، 23 يناير 2017، في ص. 2.

997 اللائحة العامة لحماية البيانات، المواد 79-77 والمادة 82.

998 البرلمان الأوروبي، قواعد القانون المدني الأوروبي في مجال الروبوتات، المديرية العامة للسياسات الداخلية، (أكتوبر 2016)، ص. 14.

999 خطاب روبيرتو فيولا في الحلقة الدراسية الإعلامية بشأن قانون الروبوتات الأوروبي في البرلمان الأوروبي، (خطاب 16 فبراير 2017)؛ إعلان البرلمان الأوروبي بشأن الطلب الموجه إلى المفوضية لاقتراح قواعد المسؤولية المدنية الخاصة بالروبوتات والذكاء الاصطناعي.

1000 مجلس أوروبا، المبادئ التوجيهية بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية في عالم البيانات الضخمة، 01 (2017) T-PD، ستراسبورغ، 23 يناير 2017.

1001 المشرف الأوروبي على حماية البيانات (2016)، الإنفاذ المنسجم للحقوق الأساسية في عصر البيانات الضخمة، الرأي 8/2016، 23 سبتمبر 2013، ص. 8.

**قواعد وحقوق محددة**

تظل القاعدة العامة أن البيانات الشخصية التي تتم معالجتها من خلال الدراسات التحليلية للبيانات الضخمة تقع ضمن نطاق تشريعات حماية البيانات. ومع ذلك، تم إدراج قواعد واستثناءات محددة في حالات محددة تتعلق بالمعالجة المعقدة للبيانات باستخدام الخوارزميات في قانون الاتحاد الأوروبي وقانون مجلس أوروبا.

في قانون مجلس أوروبا، تمنح الاتفاقية المحدثة 108 حقوقاً جديدة لصاحب البيانات للسماح بمراقبة أكثر فعالية لبياناته الشخصية في عصر البيانات الضخمة. وينطبق هذا تحديداً، على سبيل المثال، على المادة 9 (1)(أ) و(ج) و(د) من الاتفاقية المحدثة المتعلقة بالحق في عدم التعرض لقرار يؤثر عليه تأثيراً هاماً يكون قائماً فقط على معالجة آلية للبيانات دون مراعاة أرائه؛ حق صاحب البيانات، بناءً على طلبه، في معرفة المنطق الذي تستند إليه معالجة البيانات حينما تُطبق عليه نتائج تلك المعالجة بالإضافة إلى حق الاعتراض. وتُعد مقتضيات أخرى من الاتفاقية المحدثة 108 ولا سيما تلك المتعلقة بالشفافية والالتزامات الإضافية عناصر مكملة لآلية الحماية التي أنشأتها الاتفاقية 108 للتصدي للتحديات الرقمية.

وفي قانون الاتحاد الأوروبي، إلى جانب الحالات التي أُدرجت في المادة 23 من اللائحة العامة لحماية البيانات، يجب ضمان **الشفافية** لجميع عمليات معالجة البيانات الشخصية، فهي مهمة على وجه خاص فيما يتعلق بخدمات الإنترنت وغيرها من عمليات المعالجة الآلية والمعقدة للبيانات، كاستخدام الخوارزميات لاتخاذ القرارات. وفي هذا الصدد، يجب أن تمكن خصائص أنظمة معالجة البيانات أصحاب البيانات من فهم ما يحدث لبياناتهم فهماً حقيقياً. لكي تضمن معالجة عادلة وشفافة، تقتضي اللائحة العامة لحماية البيانات من المراقب أن يزود صاحب البيانات بمعلومات مفيدة عن المنطق الذي ينطوي عليه اتخاذ القرارات الآلي، بما في ذلك التنميط.[1002] وفي توصيتها المتعلقة بحماية الحق في حرية التعبير والحق في الحياة الخاصة وتعزيزهما، في شأن حيادية الشبكات، أوصت اللجنة الوزارية لمجلس أوروبا بأن يقوم مزودو خدمات الإنترنت «بتزويد المستخدمين بمعلومات واضحة وتامة ومتاحة للعامة فيما يخص أي ممارسات تتعلق بإدارة استخدام الإنترنت قد تؤثر على ولوج المستخدم إلى المحتويات والتطبيقات والخدمات وتوزيعها»[1003] وينبغي للتقارير التي تصدرها السلطات المختصة في الدول الأعضاء عن الممارسات المتعلقة بإدارة استخدام الإنترنت أن يتم إعدادها بطريقة صريحة وشفافة وتنبغي إتاحتها مجاناً لعامة الناس.[1004]

يجب على مراقبي البيانات **إخبار** أصحاب البيانات - سواءً عندما تُجمع البيانات منهم أو لا- ليس فقط **بمعلومات** محددة عن البيانات التي تم جمعها والمعالجة المتوخاة منها (إطلع على الجزء 1.1.6.) وإنما أيضاً، حيثما كان ذلك مناسباً، بوجود عمليات اتخاذ القرار الآلي، مع تزويدهم ب»بمعلومات مفيدة عن المنطق الذي تنطوي عليه تلك العمليات»،[1005] وأهدافها وعواقبها المحتملة. وتوضح اللائحة العامة لحماية البيانات أيضاً (فقط في الحالات التي لم يتم فيها الحصول على البيانات الشخصية من صاحب البيانات) أن المراقب لا يكون ملزماً بتزويد صاحب البيانات بتلك المعلومات عندما «يتعذر التزويد بتلك المعلومات أو ينطوي على مجهود غير متناسب».[1006] ومع ذلك، وكما يشدد عليها فريق عمل المادة 29 في مبادئه التوجيهية بشأن اتخاذ القرارات الفردية والآلية والتنميط لأغراض اللائحة 2016/679، فإن تعقد المعالجة لا ينبغي، في حد ذاته، أن يمنع المراقب من تزويد صاحب البيانات بتفسيرات واضحة عن الدراسات التحليلية والأهداف المستخدمة في معالجة البيانات.[1007]

لا تشتمل حقوق أصحاب البيانات في **الولوج** إلى بياناتهم الشخصية و**تصحيحها** و**محوها** بالإضافة إلى حقهم في تقييد المعالجة على إعفاء مماثل. ومع ذلك، قد يُلغى التزام مراقب البيانات بإشعار صاحب البيانات بأي تصحيح لبياناته الشخصية أو محوها (إطلع على الجزء 4.1.6) عندما «يتعذر ذلك الإشعار أو ينطوي على مجهود غير متناسب».[1008]

يحق أيضاً لأصحاب البيانات **الاعتراض**، طبقاً للمادة 21 من اللائحة العامة لحماية البيانات (إطلع على الجزء 6.1.6)، على أي معالجة لبياناتهم الشخصية، بما في ذلك في حالات القيام بدراسات تحليلية للبيانات الضخمة. في حين قد يُعفى مراقبو البيانات من ذلك الالتزام إذا

---

[1002] اللائحة العامة لحماية البيانات، المادة 13 (2) (و).

[1003] مجلس أوروبا، اللجنة الوزارية (2016)، توصية CM/R(2016)1 اللجنة الوزارية الموجهة إلى الدول الأعضاء بشأن حماية وتعزيز الحق في حرية التعبير والحق في الحياة الخاصة فيما يتعلق بحيادية الشبكة، 13 يناير 2016، الفقرة 1.5.

[1004] نفس المرجع السابق، الفقرة 2.5.

[1005] اللائحة العامة لحماية البيانات، 13 (2) و و14 (2) ز.

[1006] نفس المرجع السابق، المادة 14 (5) ب.

[1007] فريق عمل المادة 29، المبادئ التوجيهية بشأن اتخاذ القرارات الفردي والآلي والتنميط لأغراض اللائحة 2016/679، اجتماع فريق العمل رقم 251، 03 أكتوبر 2017، ص. 14.

[1008] اللائحة العامة لحماية البيانات، المادة 19.

[1009] نفس المرجع السابق، المادة 89 (2) و(3).

استطاعوا إثبات وجود مصالح شرعية غالبة، قد لا يتمتعون بذلك الإعفاء فيما يخص المعالجة لأغراض التسويق المباشر.

قد يثير مراقبو البيانات استثناءات متعلقة بتلك الحقوق عند معالجة البيانات الشخصية لأغراض الأرشفة للمصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو لأغراض إحصائية.[1009]

وفيما يتعلق **بالتنميط واتخاذ القرارات الآلية**، أدخلت اللائحة العامة لحماية البيانات قواعد محددة، حيث تنص المادة 22 (1) على أن صاحب البيانات «يحق له عدم التعرض لقرار قائم على المعالجة الآلية فحسب، حين ينتج عن القرار آثاراً قانونية تتعلق به». ووفقاً لما أبرزته المبادئ التوجيهية لفريق عمل المادة 29، تنص تلك المادة على حظر عام على اتخاذ القرارات آلياً بالكامل.[1010] وقد لا يُعفى مراقبو البيانات من ذلك الحظر إلا في الحالات الثلاث التالية: عندما يكون القرار: 1) ضرورياً لتنفيذ العقد بين صاحب البيانات والمراقب أو 2) مسموحاً به بموجب قانون الاتحاد الأوروبي أو القانون الوطني أو 3) قائماً على موافقة صريحة.[1011]

**المراقبة الفردية**

يتطلب تشعب الدراسات التحليلية للبيانات الضخمة وانعدام الشفافية حولها إعادة النظر في الأفكار المتعلقة بالمراقبة الفردية للبيانات الشخصية. وينبغي لذلك أن يُصمم تصميماً يتلاءم مع السياق الاجتماعي والتكنولوجي، مع مراعاة افتقار الأفراد إلى المعرفة. ولذلك، ينبغي أن يتبنى مفهوم حماية البيانات في سياق البيانات الضخمة فكرة أوسع حول مراقبة استخدام البيانات، وأن تتطور المراقبة الفردية وفقاً لها إلى عملية أكثر تعقداً لتقييمات الآثار العديدة للأخطار المتعلقة باستخدام البيانات.[1012]

إن جودة تطبيق للبيانات الضخمة يعتمد على مدى قدرته على توقع رغبات وسلوكات الأفراد الخاضعين للاختبار (أو المستهلكين). ويتم تنقيح النماذج التنبئية الحالية والقائمة على الدراسات التحليلية للبيانات الضخمة على نحو مستمر. ولا تشمل التطورات الأخيرة استخدام البيانات لتصنيف الشخصيات (أي السلوك والمواقف) فحسب، وإنما أيضاً تحليل السلوك من خلال تحليل الأنماط الصوتية وشدة كتابة الرسائل أو حرارة الجسم. وعلى سبيل المثال، يمكن استخدام جميع تلك المعلومات آنياً على ضوء المعرفة المستمدة من تقييمات البيانات الضخمة لتقييم الجدارة الائتمانية خلال اجتماع مع ممثل عن مؤسسة مصرفية. ولا يُجرى التقييم استناداً إلى جدارة الفرد الذي يطلب القرض، وإنما إلى الخصائص السلوكية المستمدة من تحليل معلومات البيانات الضخمة وتقييمها، أي المرشح الذي يتحدث بصوت قوي أو صوت مفر أو لغته الجسدية أو حرارة الجسم.

قد لا يمثل التنميط والإعلانات المستهدفة مشكلة بالضرورة إذا كان الأفراد **واعين** باستهدافهم من قبل الإعلانات المَفصلة على المقاس. ويصبح التنميط مشكلة حينما يُستخدم للتلاعب بالأفراد، أي للبحث عن شخصيات أو مجموعات معينة من الناس للقيام بحملات سياسية. على سبيل المثال، يمكن مخاطبة مجموعات من الناخبين المترددين عن طريق رسائل سياسية مصممة لتناسب «شخصيتهم» ومواقفهم. وثمة مسألة أخرى وهي استخدام ذلك التنميط لحرمان أفراد بعينهم من الحصول على السلع والخدمات. من بين الضمانات التي قد تزود بالحماية من سوء استخدام البيانات الضخمة والمعلومات الشخصية استخدام اسم مستعار للبيانات (اطلع على الجزء 1.1.2).[1013] وعندما يتم بالفعل إخفاء مصدر البيانات الشخصية، أي عندما لا توجد معلومات تترك آثاراً تتعلق بأصحاب البيانات، لا تندرج تلك الحالات ضمن نطاق اللائحة العامة لحماية البيانات. وتمثل مسألة موافقة أصحاب البيانات والأفراد في ميدان معالجة البيانات الضخمة بدورها تحدياً لقانون حماية البيانات. ويشمل ذلك الموافقة على استهداف الإعلانات المَفصلة على المقاس والتنميط، والتي يمكن تبريرها بأسباب تتعلق بـ«تجربة العميل»، والموافقة على استخدام كميات من البيانات الضخمة لتنقيح الأدوات التحليلية القائمة على المعلومات وتطويرها. ويثير الوعي بمعالجة البيانات الضخمة، أو انعدامه، عدة أسئلة تتعلق بالوسيلة التي يمكن لأصحاب البيانات أن يمارسوا بها حقوقهم، نظراً إلى أن معالجة البيانات الضخمةقد تعتمد على كل من المعلومات المستخدمة لاسم مستعار والمعلومات المخفاة المصدر الخاضعة للخوارزميات. في حين تندرج البيانات المستخدمة لاسم مستعار ضمن نطاق اللائحة العامة لحماية البيانات، لا تنطبق اللائحة على البيانات المخفاة المصدر. ويُعد وعي الأفراد بمعالجة بياناتهم الشخصية، ومراقبتهم الفردية لها، أمراً في غاية الأهمية في مجال الدراسات التحليلية للبيانات الضخمة: دونهما، لن يكوِّنوا فكرة واضحة عمن يكون مراقب البيانات أو معالج البيانات، ما يمنعهم من ممارسة حقوقهم ممارسة فعالة.

---

[1010] فريق عمل المادة 29، المبادئ التوجيهية بشأن اتخاذ القرارات الفردي والآلي والتنميط لأغراض اللائحة 2016/679، اجتماع فريق العمل رقم 251، 03 أكتوبر 2017، ص. 9.

[1011] اللائحة العامة لحماية البيانات، المادة 22 (2).

[1012] مجلس أوروبا، اللجنة الاستشارية للاتفاقية 108، المبادئ التوجيهية بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية في عالم البيانات الضخمة، 01(2017)T-PD، ستراسبورغ، 23 يناير 2017.

[1013] نفس المرجع السابق، ص. 2.

# 2.10. إنترنت الجيل 2.0 و3.0: شبكات التواصل الاجتماعي و«إنترنت الأشياء»

## النقاط الرئيسية

- إن «خدمات شبكات التواصل الاجتماعي» (SNS) عبارة عن منصات تواصل على الإنترنت تمكن الأفراد من الانضمام إلى - أو حتى إنشاء - شبكات يرتادها مستخدمون يحملون أفكاراً ورؤى مشتركة.
- تتجلى «إنترنت الأشياء» في ربط الأشياء (من أجهزة وأدوات وغيرها) بالإنترنت زيادة على الربط البيني بين تلك الأشياء مع بعضها بعضاً.
- إن موافقة أصحاب البيانات تمثل الأرضية القانونية الأكثر شيوعاً لمعالجة البيانات بصفة مشروعة من جانب مراقبي البيانات داخل شبكات التواصل الاجتماعي.
- تتم حماية مستخدمي شبكات التواصل الاجتماعي عموماً بموجب «الإعفاء المنزلي» ، إلا أن هذا الاستثناء يمكن أن يسقط في سياقات معينة.
- إن مقدمي خدمات شبكات التواصل الاجتماعي ليسوا محميين بموجب «الإعفاء المنزلي».
- يُعتبر إعمال الخصوصية منذ التصميم وتلقائياً مسألة حاسمة في ضمان أمن البيانات في هذا المجال.

## 1.2.10. تعريف إنترنت الجيل 2.0 و3.0

**خدمات شبكات التواصل الاجتماعي**

في البداية، كان يُنظر إلى الإنترنت على أنها شبكة لربط ما بين الحواسيب ولإرسال الرسائل ذات قدرات محدودة لتبادل البيانات وذات مواقع إلكترونية كانت بالكاد تتيح للأفراد إمكانية مشاهدة المحتوى مشاهدة سلبية.[1014] وفي عصر إنترنت الجيل 2.0، حُولت الإنترنت إلى منتدىً يتفاعل فيه المستخدمون ويتعاونون ويولدون المدخلات. ويتميز هذا العصر بالنجاح المبهر لخدمات شبكات التواصل الاجتماعي وشيوع استخدامها وهي التي أصبحت اليوم جزءاً أساسياً من الحياة اليومية لملايين الناس.

يجوز تعريف خدمات شبكات التواصل الاجتماعي (SNS) أو «وسائل التواصل الاجتماعي» تعريفاً واسعاً بـ«منصات التواصل عبر الإنترنت التي تمكن الأفراد من إنشاء شبكات من المستخدمين ذوي التفكير المتشابه أو الانضمام إليها».[1015] ولإنشاء شبكة أو الانضمام إليها، يُطلب من الأفراد تقديم بيانات شخصية وإنشاء ملفاتهم الشخصية. وتمكن خدمات شبكات التواصل الاجتماعي الأفراد من توليد «المحتوى» الرقمي الذي تتعدد أشكاله وأوجهه من صور فوتوغرافية وفيديوهات إلى روابط الجرائد والمنشورات الشخصية للتعبير عن آرائهم. ومن خلال منصات التواصل عبر الإنترنتهذه، يستطيع المستخدمون التواصل مع العديد من المستخدمين الآخرين، والأهم من ذلك أن معظم خدمات شبكة التواصل الاجتماعي لا تتطلب أي رسوم للتسجيل. فبدلاً عن مطالبة المستخدمين بالدفع للانضمام إلى الشبكة، يكسب مزودو خدمات شبكات التواصل الاجتماعي معظم مداخيلهم من الإعلانات المستهدفة. ويمكن للمعلنين أن يستفيدوا استفادة عظيمة من المعلومات الشخصية التي يُكشف عنها يومياً على تلك المواقع، ذلك أن امتلاك المعلنين لمعلومات عن سن المستخدم وجنسه وموقعه الجغرافي واهتماماته يسمح لهم باستهداف الأشخاص «المرغوب فيهم» بإعلاناتهم.

وقد اعتمدت لجنة وزراء مجلس أوروبا توصية بشأن حماية حقوق الإنسان فيما يتعلق بخدمات شبكات التواصل الاجتماعي،[1016] والتي تتناول في جزء منها حماية البيانات، وتم استكمالها في 2018 بتوصية أخرى بشأن أدوار وسطاء الإنترنت ومسؤولياتهم.[1017]

[1014] المفوضية الأوروبية (2016)، تطوير إنترنت الأشياء في أوروبا، النسخة النهائية110 (SWD(2016.

[1015] فريق عمل المادة 29 (2009)، الرأي 5/2009 بشأن شبكات التواصل الاجتماعي الإلكترونية، اجتماع فريق العمل رقم 163، 12 يونيو 2009، ص. 4.

[1016] مجلس أوروبا، اللجنة الوزارية، التوصية CM/Rec(2012)4 الصادرة عن اللجنة الوزارية والموجهة إلى الدول الأعضاء بشأن حماية حقوق الإنسان فيما يتعلق بخدمات شبكات التواصل الاجتماعي، 04 أبريل 2012.

[1017] مجلس أوروبا، اللجنة الوزارية، التوصية CM/Rec(2018)2 الصادرة عن اللجنة الوزارية والموجهة إلى الدول الأعضاء بشأن أدوار وسطاء الإنترنت ومسؤولياتهم، 07 مارس 2018.

مثال: الآنسة نورا تغمرها السعادة لأن شريكها عرض عليها الزواج، وهي ترغب في أن تزف هذا النبأ السعيد إلى أصدقائها وعائلتها وتقرر كتابة منشور عاطفي على شبكة التواصل الاجتماعي للتعبير عن فرحها ولتغيير حالتها الاجتماعية إلى «مخطوبة». في الأيام التالية، عندما تسجل نورا الدخول إلى حسابها، ترى إعلانات عن متاجر فساتين الزفاف والزهور. فلماذا الأمر كذلك؟

عند إنشاء إعلان على «الفيسبوك»، اختارت الشركات التي تبيع فساتين الزفاف والزهور مقاييس معينة حتى تتمكن من استهداف أشخاص مثل نورا. وبحكم أن ملف نورا الشخصي يدل على أنها أنثى ومخطوبة وتعيش في باريس على مقربة من المنطقة التي تقع فيها متاجر الفساتين والزهور التي وضعت الإعلانات، فإن نورا حتماً ستصلها تلك الإعلانات.

**إنترنت الأشياء**

تمثل إنترنت الأشياء (IoT) الخطوة التالية في تطور الإنترنت: عصر إنترنت الجيل 3.0. باستخدام إنترنت الأشياء، يمكن للأجهزة أن تتفاعل مع أجهزة أخرى أو تتصل بها من خلال الإنترنت. ويسمح ذلك للأشياء والأشخاص بأن يكونوا متصلين فيما بينهم من خلال شبكات التواصل والإخبار عن حالتهم و/أو عن حالة البيئة المحيطة.[1018] وفرضت إنترنت الأشياء والأجهزة المتصلة نفسها واقعاً بالفعل ويُتوقع أن تنمو نمواً كبيراً في السنوات القليلة القادمة عبر صنع وتطوير أجهزة ستفضي إلى إنشاء مدن ذكية وبناء مساكن ذكية وتأسيس شركات ذكية.

مثال: يمكن لإنترنت الأشياء أن تكون مفيدة للرعاية الصحية على نحو خاص. وصنعت الشركات بالفعل أجهزة وأجهزة استشعار وتطبيقات تسمح بمراقبة حالة صحة المريض. ومن خلال استعمال زر إنذار قابل للارتداء وأجهزة الاستشعار اللاسلكية الأخرى الموضوعة في جميع أنحاء المسكن، يمكن تعقب الروتين اليومي للأشخاص المسنين الذين يعيشون بمفردهم وإطلاق إنذارات إذا تم اكتشاف اضطرابات خطيرة في جدولهم الزمني اليومي. على سبيل المثال، يشيع استخدام الأشخاص المسنين لأجهزة استشعار السقوط. وقد تكتشف هذه الأجهزة حالات السقوط اكتشافاً دقيقاً وتشعر طبيب الفرد و/أو عائلته بها.

مثال: تُعد مدينة برشلونة أحد أشهر الأمثلة عن المدن الذكية وتحرص المدينة منذ 2012 على تفعيل التكنولوجيات المبتكرة، رامية إلى إيجاد نظام ذكي للمواصلات العامة وإدارة النفايات ومواقف السيارات وإضاءة الشوارع. ولتحسين إدارة النفايات، على سبيل المثال، تستخدم المدينة صناديق القمامة الذكية، حيث يُمكّن ذلك من مراقبة مستويات النفايات لتحسين طرق جمعها. وعندما تكون صناديق القمامة شبه ممتلئة، ترسل إشارات عن طريق شبكات الاتصالات المحمولة إلى التطبيق البرمجي المستخدم من قبل شركة إدارة النفايات. ويمكن للشركة بذلك أن تخطط للطريق الأفضل لجمع النفايات وتحدد الأولويات و/أو تقوم فقط بترتيب عمليات شحن صناديق القمامة التي تحتاج فعلاً إلى تفريغها.

## 2.2.10. التوفيق بين الفوائد والأخطار

يدل الانتشار الواسع والنجاح الهائل لخدمات شبكات التواصل الاجتماعي في العقد الماضي على أن لها **فوائد هامة**. على سبيل المثال، تُعد الإعلانات المستهدفة (كما هو موصوف في المثال الذي سقناه سلفاً) طريقة مبتكرة بصفة خاصة لكي تستهدف الشركات جمهورها، ما يتيح لهم سوقاً أكثر تحديداً. وقد يكون أيضاً من مصلحة المستهلكين أن تُعرض عليهم إعلانات أكثر ملاءمة وإثارة للاهتمام. لكن الأمر الأكثر أهمية هو أن خدمات التشبيك ووسائل التواصل الاجتماعي قد يكون لها أثر إيجابي على المجتمع وعلى إحداث التغيير، فهي تمكن المستخدمين من التواصل والتفاعل وتنظيم المجموعات والأحداث المتعلقة بالمسائل التي تؤثر فيهم.

[1018] المفوضية الأوروبية، وثيقة عمل موظفي المفوضية، تطوير إنترنت الأشياء في أوروبا، 19 ،110 (2016)SWD أبريل 2016.

على غرار وسائل التواصل الاجتماعي، يُتوقع أن تجلب إنترنت الأشياء فوائد هامة للاقتصاد وتُعد جزءاً من استراتيجية الاتحاد الأوروبي لإقامة سوق رقمية موحدة. في الاتحاد الأوروبي، تفيد التقديرات أن عدد اتصالات إنترنت الأشياء سيرتفع في 2020 إلى ستة مليارات. ويُتوقع من انتشار الاتصال أن يجلب فوائد اقتصادية هامة من خلال تطوير خدمات وتطبيقات مبتكرة ورعاية صحية أفضل وفهم أوفى لحاجات المستهلكين مع زيادة الكفاءة في الخدمة.

وفي الآن نفسه، ونظراً إلى الكم الهائل من المعلومات الشخصية الناشئة عن مستخدمي وسائل التواصل الاجتماعي والتي تُعالج لاحقاً من قبل مشغلي الخدمة، تصاحب انتشار خدمات شبكات التواصل الاجتماعي **مخاوف متزايدة** بشأن الطرق التي يمكن بها حماية الخصوصية والبيانات الشخصية. وقد تهدد خدمات شبكات التواصل الاجتماعي الحق في الحياة الخاصة والحق في حرية التعبير. وقد تشمل تلك التهديدات: «انعدام الضمانات القانونية والإجرائية المحيطة بالعمليات التي يمكن لها أن تؤدي إلى إقصاء المستخدمين؛ والحماية غير الكافية للأطفال والشباب من المحتوى أو السلوكات الضارة؛ وعدم احترام حقوق الآخرين؛ وانعدام الإعدادات التلقائية المراعية للخصوصية؛ وانعدام الشفافية بشأن الأغراض التي تستدعي جمع البيانات ومعالجتها».[1019] وسعى قانون حماية البيانات الأوروبي إلى الاستجابة لتحديات حماية البيانات والخصوصية التي جلبتها وسائل التواصل الاجتماعي. وتُعد مبادئ مثل الموافقة وحماية البيانات والخصوصية منذ التصميم وتلقائياً وحقوق الأفراد ذات أهمية خاصة في سياق وسائل التواصل الاجتماعي وخدمات شبكات التواصل.

في سياق إنترنت الأشياء، ينطوي الحجم الهائل من البيانات الشخصية الذي يتولد عن مختلف الأجهزة المتصلة فيما بينها على أخطار على حماية البيانات والخصوصية. في حين تُعد الشفافية مبدأ هاماً من قانون حماية البيانات الأوروبي، ونظراً إلى كثرة الأجهزة المتصلة لا يتضح دائماً من يكون باستطاعته جمع البيانات التي تم جمعها عن أجهزة إنترنت الأشياء والولوج إليها واستخدامها.[1020] ومع ذلك، بموجب قانوني الاتحاد الأوروبي ومجلس أوروبا، يقضي مبدأ الشفافية بإلزام المراقبين بإبقاء أصحاب البيانات على اطلاع على كيف يتم استخدام بياناتهم بلغة واضحة وبسيطة. ويجب إيضاح الأخطار والقواعد والضمانات والحقوق المرتبطة بمعالجة بياناتهم الشخصية للأفراد المعنيين. ويمكن أيضاً لأجهزة إنترنت الأشياء المتصلة وعمليات المعالجة الكثيرة والبيانات المعنية أن تمثل تحدياً لمقتضى الموافقة الواضحة والمستنيرة على معالجة البيانات – عندما تكون تلك المعالجة قائمة على الموافقة. وغالباً ما يفتقر الأفراد إلى فهم الأداء التقني لتلك المعالجة وبالتالي عواقب موافقتهم.

ويمثل الأمن مصدر قلق كبير آخر نظراً إلى كون الأجهزة المتصلة معرضة بصفة خاصة للأخطار الأمنية. وللأجهزة المتصلة مستويات متفاوتة من الأمن. ونظراً إلى أن الأجهزة المتصلة تشتغل خارج البنية التحتية القياسية لتكنولوجيا المعلومات، فإنها قد تفتقر إلى القدرة على المعالجة الكافية وسعة التخزين الكافية لاستضافة البرمجيات الأمنية أو توظيف تقنيات مثل التشفير أو استخدام اسم مستعار للبيانات أو إخفاء مصدر البيانات لحماية المعلومات الشخصية للمستخدمين.

مثال: في ألمانيا، قرر المنظمون فرض حظر على لعبة متصلة بالإنترنت عقب مخاوف شديدة إزاء أثر اللعبة على احترام الحياة الخاصة للأطفال. واعتقد المنظمون أن الدمية المتصلة بالإنترنت المسماة كايلا تمثل فعلاً جهاز تجسس مخبأ. وتشتغل الدمية بإرسال الأسئلة الصوتية للطفل الذي يلعب بها إلى تطبيق مثبت على جهاز رقمي يحولها إلى نص ويبحث في الإنترنت عن الأجوبة. ويرسل التطبيق بعد ذلك إجابة إلى الدمية التي تعبر عنها للطفل. ومن خلال تلك الدمية، يمكن تسجيل اتصالات الطفل والأشخاص الكبار بالقرب منها وإرسالها إلى التطبيق. ولولا اعتماد مصنعي الدمية لتدابير أمنية كافية، لكان بمقدور أي كان استخدام الدمية للاستماع إلى المحادثات.

[1019] مجلس أوروبا، التوصية Rec(2012)4 الموجهة إلى الدول الأعضاء بشأن حماية حقوق الإنسان فيما يتعلق بخدمات شبكات التواصل الاجتماعي، 04 أبريل 2012.
[1020] المشرف الأوروبي على حماية البيانات (2017)، فهم إنترنت الأشياء.

## 3.2.10. مسائل متعلقة بحماية البيانات

**الموافقة**

في أوروبا، لا تكون معالجة البيانات الشخصية مشروعة إلا إذا أجازها قانون حماية البيانات الأوروبي. فيما يخص مزودي خدمات شبكات التواصل الاجتماعي، تقدم موافقة أصحاب البيانات على العموم أساساً مشروعاً لمعالجة البيانات. ويجب أن تُمنح الموافقة بطريقة حرة ومحددة ومستنيرة وصريحة (اطلع على الجزء 1.1.4.)،[1021] ويُقصد بـ'طريقة حرة' أساساً أنه يجب أن تكون لأصحاب البيانات القدرة على ممارسة اختيار حقيقي وصادق. وتكون الموافقة 'محددة' و'مستنيرة' عندما تكون مفهومة وتحيل صراحة وبدقة إلى النطاق التام للمعالجة وأغراضها وعواقبها. وفي سياق وسائل التواصل الاجتماعي، يمكن التشكيك فيما إذا كانت الموافقة حرة ومحددة ومستنيرة فيما يتصل بكل أنواع المعالجات التي يقوم بها مشغل خدمات شبكات التواصل الاجتماعي والأطراف الثالثة.

مثال: للانضمام إلى خدمات شبكات التواصل الاجتماعي والولوج إليها، غالباً ما يجب على الأفراد الموافقة على أنواع مختلفة من معالجة بياناتهم الشخصية وغالباً ما يكون ذلك دون تزويد الأفراد بالمواصفات الضرورية أو الخيارات البديلة ومن بين الأمثلة عن ذلك الحاجة إلى الموافقة على تلقي الإعلانات السلوكية للتسجيل في خدمة شبكة التواصل الاجتماعي. وكما يشير فريق عمل المادة 29 في رأيه عن تعريف الموافقة، «بالنظر إلى الأهمية التي اكتسبتها بعض شبكات التواصل الاجتماعي، ستقبل بعض الفئات من المستخدمين (مثل المراهقين) تلقي الإعلانات السلوكية حتى تتفادى خطر الإقصاء جزئياً من التفاعلات الاجتماعية. وينبغي وضع المستخدم في موقف يسمح له بمنح موافقة حرة ومحددة على تلقي الإعلانات السلوكية بغض النظر عن ولوجه إلى خدمة شبكة التواصل الاجتماعي.»[1022]

بموجب اللائحة العامة لحماية البيانات، لا يمكن مبدئياً معالجة البيانات الشخصية للأطفال الذين تقل أعمارهم عن 16 سنة استناداً إلى موافقتهم.[1023] وإذا كانت الموافقة على المعالجة ضرورية، فيتعين على والد الطفل أو الوصي عليه منح تلك الموافقة. ويستحق الأطفال حماية خاصة نظراً إلى أنهم قد يكونون أقل وعياً بالأخطار والعواقب التي تنطوي عليها معالجة البيانات. ويُعد ذلك في غاية الأهمية في سياق وسائل التواصل الاجتماعي لكون الأطفال أكثر عرضة للآثار السيئة التي قد ينطوي عليها استخدام تلك الوسائل مثل التنمر السيبراني أو المطاردة الإلكترونية أو سرقة الهوية.

**الأمن وحماية البيانات/الخصوصية منذ التصميم وتلقائياً**

تنطوي معالجة البيانات الشخصية على أخطار أمنية متأصلة نظراً إلى وجود احتمال دائم لحدوث خرق أمني يؤدي بالبيانات الشخصية التي تُعالج إلى تغييرها أو ضياعها أو دمارها العرضي أو غير المشروع أو الولوج إليها أو الكشف عنها بصفة غير مرخصة. وبموجب قانون حماية البيانات الأوروبي، يُشترط على المراقبين والمعالجين تنفيذ تدابير تقنية وإجرائية مناسبة لمنع أي تدخل غير مرخص في عمليات معالجة البيانات. ويتعين أيضاً على مزودي خدمات شبكات التواصل الاجتماعي الذين تطالهم قواعد حماية البيانات الأوروبية الامتثال لذلك الالتزام.

تقتضي مبادئ حماية البيانات/الخصوصية منذ التصميم وتلقائياً من المراقبين أن يحافظوا على الأمن في تصميم منتجاتهم وأن يطبقوا تلقائياً الإعدادات المناسبة لحماية البيانات والخصوصية. ويعني ذلك أنه عندما يقرر الشخص الانضمام إلى شبكة اجتماعية، قد لا يتيح مزود الخدمة بصورة تلقائية جميع المعلومات المتعلقة بمستخدم الخدمة الجديد لصالح كافة مستخدمي تلك الخدمة. فعند الانضمام إلى الخدمة، ينبغي الحرص على ألا تسمح إعدادات حماية البيانات والخصوصية التلقائية بإتاحة المعلومات إلا لجهات الاتصال التي يختارها الفرد. ولا ينبغي أن يمتد الولوج إلى أشخاص ليسوا في تلك القائمة إلا بعد أن يتخذ المستخدم إجراءً لتغيير إعدادات حماية البيانات والخصوصية يدوياً. وقد يكون لذلك أيضاً أثراً في الحالات التي يحدث فيها خرق للبيانات رغماً عن وجود التدابير الأمنية. وفي تلك الحالات يتعين على المزودين إشعار المستخدمين المتأثرين عندما يُحتمل أن ينشأ عن ذلك خطر شديد على حقوق صاحب البيانات وحرياته.[1024]

[1021] اللائحة العامة لحماية البيانات، المادتان 4 و7؛ الاتفاقية المحدّثة 108، المادة 5.

[1022] فريق عمل المادة 29 (2011)، الرأي 15/2011 بشأن تعريف الموافقة، اجتماع فريق العمل رقم 187، 13 يوليو 2011، ص. 18.

[1023] اطلع على اللائحة العامة لحماية البيانات، المادة 8. قد تنص الدول الأعضاء في الاتحاد الأوروبي بموجب القانون على سن أقل شريطة ألا يكون ذلك أقل من 13 سنة.

[1024] نفس المرجع السابق، المادة 34.

تُعد حماية البيانات/الخصوصية منذ التصميم وتلقائياً ذات أهمية بالغة في سياق خدمات شبكة التواصل الاجتماعي لأنه بالإضافة إلى الأخطار التي ينطوي عليها الولوج غير المرخص في أغلب أنواع المعالجة، تثير مشاركة المعلومات الشخصية في وسائل التواصل الاجتماعي مزيداً من الأخطار الأمنية. وتُعزى غالباً تلك الأخطار الأمنية إلى جهل الأفراد بهوية الأشخاص الذين قد يلجون إلى معلوماتهم و كيفية استخدامهم لها. وفي ظل شيوع استخدام وسائل التواصل الاجتماعي، ارتفع عدد حوادث سرقة الهوية وضحاياها.

مثال: تُعد سرقة الهوية ظاهرة يحصل بها الشخص على معلومات أو بيانات أو وثائق تعود إلى شخص آخر (الضحية) ويستخدم تلك المعلومات لاحقاً لانتحال شخصية الضحية للحصول على سلع أو خدمات باسم الضحية. لنأخذ بول، على سبيل المثال، الذي يملك حساباً على أحد مواقع التواصل الاجتماعي ويشتغل معلماً ويُعد عضواً نشطاً في مجتمعه المحلي وهو غير متحفظ ولا ينتابه قلق خاص بشأن إعدادات حماية البيانات والخصوصية الخاصة بحسابه على موقع التواصل الاجتماعي. ويملك قائمة طويلة بجهات الاتصال تشتمل أحياناً على أشخاص لا يعرفهم بالضرورة على مستوى شخصي. ونظراً إلى اشتغاله في مدرسة كبيرة وشعبيته الكبيرة في تدريبه لفريق كرة القدم التابع للمدرسة، يظن أن هؤلاء الأشخاص هم على الأرجح آباء التلاميذ الذين يدرسون بالمدرسة أو أصدقاء المدرسة. ويُعرض عنوان البريد الإلكتروني لبول وذكرى ميلاده في حسابه في موقع التواصل الاجتماعي. علاوة على ذلك، ينشر بول بانتظام صوراً فوتوغرافية لكلبه طوبي مصحوبة بعبارات مثل «أنا وكلبي طوبي في حصة الركض الصباحية». لم يدرك بول أنه من بين الأسئلة المتعلقة بالأمن الأكثر شيوعاً لحماية بريده الإلكتروني أو حسابه على الهاتف المحمول هو سؤال «ما اسم حيوانك الأليف؟». وباستخدام المعلومات المتاحة في ملف بول الشخصي في موقع التواصل الاجتماعي، نجح نيك بسهولة في اختراق حسابات بول.

**حقوق الأفراد**

يجب على مزودي خدمات شبكات التواصل الاجتماعي احترام حقوق الأفراد (اطلع على الجزء 1.6)، بما في ذلك حق الفرد في إخباره بغرض المعالجة وكيف يجوز استخدام البيانات الشخصية لأغراض التسويق المباشر. ويجب أيضاً تمتيع الأفراد بالحق في الولوج إلى البيانات الشخصية التي أنشأوها في منصات شبكات التواصل الاجتماعي وطلب حذفها، حتى عندما يوافق الأشخاص على معالجة البيانات الشخصية وتحميل المعلومات على الإنترنت، ينبغي لهم أن يكونوا قادرين على المطالبة بـ»الحق في النسيان» إن لم يرغبوا في الحصول على خدمات شبكات التواصل الاجتماعي بعد ذلك. وتمكن أيضاً إمكانية نقل البيانات المستخدمين من الحصول على نسخة من البيانات الشخصية التي أتاحوها لمزود خدمات شبكات التواصل الاجتماعي في صيغة منظمة وشائعة الاستخدام ومقروءة آلياً، ومن نقل بياناتهم من مزود خدمات شبكات التواصل الاجتماعي إلى آخر.[1025]

**المراقبون**

من بين الأسئلة الصعبة التي تُثار غالباً في سياق وسائل التواصل الاجتماعي السؤال المتعلق بمن يكون المراقب، أو بعبارة أخرى: من يكون الشخص الذي يتحمل التزام ومسؤولية الامتثال لقواعد حماية البيانات؟ ويُعد مزودو خدمات شبكة التواصل الاجتماعي مراقبين بموجب قانون حماية البيانات الأوروبي، ويتضح ذلك بالنظر إلى التعريف الواسع لـ»لمراقب» وتحديد مزودي تلك الخدمات لغرض ووسائل معالجة البيانات التي يشاركها الأفراد. فبموجب قانون الاتحاد الأوروبي، إذا كان المراقبون يعرضون خدمات على أصحاب البيانات في الاتحاد الأوروبي، فإنهم يكونون مطالبين بالامتثال لمقتضيات اللائحة العامة لحماية البيانات حتى لو لم يتم تأسيس هيئاتهم داخل الاتحاد الأوروبي.

ومع ذلك، هل يمكن أيضاً احتساب مستخدمي خدمات شبكات التواصل الاجتماعي مراقبين؟ عندما يعالج الأفراد البيانات الشخصية «أثناء نشاط شخصي أو منزلي محض»، لا تُطبق قواعد حماية البيانات. ويُعرف ذلك في قانون حماية البيانات الأوروبي بـ»الاستثناء المنزلي». غير أنه في بعض الحالات لا يشمل الاستثناء المنزلي مستخدم خدمة شبكات التواصل الاجتماعي. يُذكر أن المستخدمين يتداولون معلوماتهم الشخصية طوعاً على الإنترنت، مع العلم أن المعلومات التي يتقاسمونها مع الآخرين غالباً ما تشتمل على معلومات شخصية لأناس آخرين.

[1025] اللائحة العامة لحماية البيانات، المادة 21.

مثال: يملك بول حساباً على أحد منصات شبكات التواصل الاجتماعي المشهورة جداً ويسعى إلى أن يصبح ممثلاً ويستخدم حسابه لنشر صور فوتوغرافية وفيديوهات ومنشورات يشرح فيها شغفه للفن. وتُعد الشعبية ذات أهمية لمستقبله؛ ولذلك قرر أنه لا ينبغي إتاحة ملفه الشخصي لقائمة جهات الاتصال القريبة منه فحسب وإنما أيضاً لجميع مستخدمي الإنترنت سواء كانوا أعضاء في الشبكة أم لا. هل يستطيع بول نشر صوره الفوتوغرافية وفيديوهاته التي التقطها وقام بتصويرها بصحبة صديقته سارة دون موافقتها؟ بصفتها معلمة في مدرسة ابتدائية، تسعى سارة إلى النأي بحياتها الخاصة عن مشغلها وتلاميذها وآبائهم. لنتخيل حالة تكتشف فيها سارة، التي لا تستخدم شبكات التواصل الاجتماعي، عن طريق صديقهم المشترك نيك أن صورة فوتوغرافية التقطتها في حفلة بصحبة بول نُشرت في الإنترنت. في تلك الحالة، لن يطال قانون الاتحاد الأوروبي معالجة بيانات بول لأنها مشمولة بـ»الاستثناء المنزلي».

ومع ذلك يظل من الضروري أن يتحلى المستخدمون بالوعي وأن يدركوا أن تحميل المعلومات المتعلقة بغيرهم من الأفراد في الإنترنت دون موافقتهم قد ينطوي على انتهاك لحقوق هؤلاء الأفراد في حماية البيانات والخصوصية. وحتى عندما يُطبق الاستثناء المنزلي - على سبيل المثال، إذا كان للمستخدم ملف شخصي متاح حصراً لقائمة جهات الاتصال التي يختارها - قد يجعل نشر المعلومات الشخصية المتعلقة بالآخرين هذا المستخدم، رغم ذلك، مسؤولاً. وعلى الرغم من أن قواعد حماية البيانات لا تُطبق إذا كان الاستثناء المنزلي يُطبق، قد تنشأ مسؤولية من تطبيق غيرها من القواعد الوطنية مثل التشهير أو انتهاك الشخصية. وأخيراً، يُعد مستخدمو خدمات شبكة التواصل الاجتماعي وحدهم من تحميهم الاستثناءات المنزلية: يقع المراقبون والمعالجون الذين يتيحون وسائل تلك المعالجة الخاصة ضمن نطاق قانون حماية البيانات الأوروبي.[1026]

بإصلاح الأمر التوجيهي المتعلق بالخصوصية والاتصالات الإلكترونية، فإن قواعد حماية البيانات والخصوصية والأمن التي تُطبق على مزودي خدمات الاتصالات السلكية واللاسلكية بموجب الإطار القانوني الحالي تُطبق أيضاً على الاتصالات بين الآلات وخدمات الاتصالات الإلكترونية بما في ذلك على سبيل المثال خدمات الاتصال المباشر عبر الإنترنت (OTT).

[1026] نفس المرجع السابق، الحيثية 18.

# مراجـــع إضافيـــة

**الفصل 1**

أراسيلي مانغاس، م. (محرر) (2008)، ميثاق الحقوق الأساسية للاتحاد الأوروبي، بلباو، مؤسسة «بنك بلباو فيزكايا أرخانتاريا» (BBVA).

بركا، و. (2012)، الحق الأساسي في حماية البيانات في منطقة التوتر بين الحرية والأمن، فيينا، دار «مانشه» للنشر ومكتبة الجامعة.

دوكسي، ك. «أربعة حقوق أساسية: تحقيق التوازن، قانون خصوصية البيانات الدولي، المجلد 6، عدد 3، ص. 195-209.

غونزاليس فاستر، غ. وغيلرت، غ. (2012)، الحق الأساسي في حماية البيانات في الاتحاد الأوروبي: سعياً وراء حق غير محدد المعالم'، المجلة الدولية الخاصة بالقانون والحواسيب والتكنولوجيا، المجلد 26 (1)، ص. 73-82.

غوتويرث، س.، بولي، ي.، دي هيرت، ب.، دو تيروانج، س. ونووت، س. (محررون) (2009)، الإصلاح الجذري لحماية البيانات، مجموعة «سبرينغر».

هايمانز، ه. (2016)، الاتحاد الأوروبي كحارس للخصوصية على الانترنت - قصة المادة 16 من المعاهدة المنظمة لعمل الاتحاد الأوروبي، مجموعة «سبرينغر».

هاستينكس، ب. (2016)، «قانون الاتحاد الأوروبي لحماية البيانات: مراجعة للأمر التوجيهي EC/95/46 واللائحة العامة لحماية البيانات المقترحة».

كرانينبورغ، ه . (2015) «'غوغل' والحق في النسيان»، مجلة قانون حماية البيانات الأوروبي، المجلد 1، عدد 1، ص. 70 -79.

لينسكي، أ. (2014)، «تفكيك حماية البيانات: 'القيمة المضافة' للحق في حماية البيانات في نظام الاتحاد الأوروبي»، مجلة القانون الدولي والمقارن الفصلية، المجلد 63، عدد 3، ص. 569-597

لينسكي، أ. (2015)، أسس قانون حماية البيانات الأوروبي، أوكسفورد، مطبعة جامعة «أكسفورد».

كوكوت، ج. وسوبوطا، ك. (2013)، «الفرق بين الخصوصية وحماية البيانات في السوابق القضائية لمحكمة العدل التابعة للاتحاد الأوروبي والمحكمة الأوروبية لحقوق الإنسان، المجلد 3، عدد 4، ص. 222-228.

مجموعة الحقوق الرقمية الأوروبية، مدخل لحماية البيانات، بروكسل.

فروين، ج. وبوكورت، و. (2009)، الاتفاقية الأوروبية لحقوق الإنسان، برلين، دار «ن. ب. إنجل» للنشر.

غرابنوارتر، ك. وبابل، ك. (2012)، الاتفاقية الأوروبية لحقوق الإنسان، ميونيخ، دار «س. ه. بيك» للنشر.

هاريس، د.، أوبويل، م.، واربريك، ك. وبيتس، إ. (2009)، قانون الاتفاقية الأوروبية لحقوق الإنسان، أوكسفورد، مطبعة جامعة «أوكسفورد».

جاراس، ه. (2010)، ميثاق الحقوق الأساسية للاتحاد الأوروبي، ميونيخ، دار «س. ه. بيك» للنشر.

ماير، ج. (2011)، ميثاق الحقوق الأساسية للاتحاد الأوروبي، بادن بادن، دار «نوموس» للنشر.

موويراي، أ. (2012)، قضايا ومواد وتعليق بشأن الاتفاقية الأوروبية لحقوق الإنسان، أوكسفورد، مطبعة جامعة «أوكسفورد».

نوفاك، م.، يانوشيفسكي، ك. وهوفستاتر، ت. (2012)، كافة حقوق الإنسان للجميع - دليل فيينا حول حقوق الإنسان، أنتويرب، «إنترسانشيا ن. ف.»، دار النشر العلمية الجديد.

بيشاريل، ك. وكوترون، ل. (2010)، ميثاق الحقوق الأساسية للاتحاد الأوروبي والاتفاقية الأوروبية لحقوق الإنسان، بروكسل، دار «إميل بروبلان» للنشر.

سيميتيس، س. (1997)، الأمر التوجيهي الخاص بحماية البيانات للاتحاد الأوروبي- جمود أو تحفيز؟ - المجلة القانونية الأسبوعية الجديدة، عدد 5، ص. 281-288.

وارن، س. وبراندیس، ل. (1890)، «الحق في الخصوصية»، مجلة هارفرد للقانون، المجلد 4، عدد 5، ص. 193-220.

وايت، ر. وأوفي، ك. (2010)، الاتفاقية الأوروبية لحقوق الإنسان، أوكسفورد، مطبعة جامعة «أكسفورد».

**الفصل 2**

أكويستي، أ.، وغروس ر. (2009)، «التنبؤ بأرقام الضمان الاجتماعي من البيانات العامة»، أشغال الأكاديمية الوطنية للعلوم، 7 يوليو 2009.

كاري، ب. (2009)، حماية البيانات: دليل عملي حول القانون بالمملكة المتحدة والاتحاد الأوروبي، أوكسفورد، مطبعة جامعة «أوكسفورد».

ديلغادو، ل. (2008)، الحق في الخصوصية وحماية البيانات في الاتحاد الأوروبي، مدريد، دار «ديكينسون س. ل» للنشر.

دي مونتيجوي، ي. -أ.، هيدالغو، ك. أ.، فيرليسين، م.، وبلونديل ف. د. (2013)، «متميزة وسط الحشد: حدود خصوصية التنقل البشري»، تقارير «نيتشر» العلمية، المجلد 3، 2013.

ديسجينس-باساناو، غ. (2012)، حماية البيانات ذات الطابع الشخصي، باريس، دار «لكسيسنيكسيس» للنشر.

دي مارتينو، أ. (2005)، حماية البيانات في القانون الأوروبي، بادن بادن، دار «نوموس» للنشر.

غونزاليس فاستر، غ. (2014)، بروز حماية البيانات كحق أساسي في الاتحاد الأوروبي، مجموعة «سبرينغر».

مورغان، ر. وبوردمان، ر. (2012)، استراتيجية حماية البيانات: تفعيل الامتثال لحماية البيانات، لندن، دار «سويت & ماكسويل» للنشر.

أوم، ب. (2010)، «وعود الخصوصية المنكوثة: الاستجابة للفشل المفاجئ لإخفاء الهوية»، مجلة جامعة كاليفورنيا للقانون، المجلد 57، عدد 6، ص. 1701-1777.

سمراتي، ب. وسويني، ل. (1998)، «حماية الخصوصية عند الإفصاح عن المعلومات: إخفاء الهوية- k (k-Anonymity) وإنفاذها من خلال التعميم والقمع»، التقرير التقني SRI-CSL-98-04.

سويني، ل. (2002)، «إخفاء الهوية-k: نموذج لحماية الخصوصية»، المجلة الدولية لعدم اليقين والغموض والأنظمة القائمة على المعرفة، المجلد 10، عدد 5، ص. 557-570.

تينيفلد، م.، باتشنر، ب، وبيتري، ت.(2012)، مدخل لقانون حماية البيانات: حماية البيانات وحرية المعلومات من منظور أوروبي، ميونيخ، دار «أولدنبورغ» للنشر.

مكتب المفوض المعلومات بالمملكة المتحدة (2012)، إخفاء الهوية: إدارة مخاطر حماية البيانات. مدونة قواعد الممارسات.

**الفصول من 3 إلى 6**

بروهان، أ. (2012)، «الأمر التوجيهيEG/95/46 بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وحرية حركة البيانات»، في غرابيتز، إ.، هيلف، م. ونيتشيم، م. (محررون)، قانون الاتحاد الأوروبي، المجلد IV، أ 30، ميونيخ، دار «س. ه. بيك» للنشر.

كوندي أورتيز، ك. (2008)، حماية البيانات الشخصية، قادس، دار «ديكنسون» للنشر.

كودراي، ل. (2010)، حماية البيانات في الاتحاد الأوروبي، ساربروكن، مطابع الجامعات الأوروبية.

كارن، ل. وكاي، ج. (2010)، «إلغاء الموافقة: «نقطة مظلمة» في قانون حماية البيانات؟»، مجلة قانون وأمن الحواسيب، المجلد 26، عدد 3، ص. 273-283.

دامان، أ. وسيميتيس، س. (1997)، الأمر التوجيهي الخاص بحماية البيانات للاتحاد الأوروبي، بادن بادن، دار «ناموس» للنشر.

دي هيرت، ب. وباباكونستانتينو، ف. (2012)، «الأمر التوجيهي الخاص بحماية بيانات الموجه للشرطة والعدالة الجنائية: تعليق وتحليل»، مجلة الحواسيب والقانون التابعة للجمعية الخاصة بالحواسيب والقانون، المجلد 22، عدد 6، ص. 1-5.

دي هيرت، ب. وباباكونستانتينو، ف. (2012)، اللائحة المقترحة الخاصة بحماية البيانات، التي تحل محل الأمر التوجيهي EC/95/46: نظام سليم من أجل حماية الأفراد»، مجلة قانون وأمن الحواسيب، المجلد 28، عدد 2، ص. 130-142.

فريتي، فديريكو (2012)، «منظور أوروبي حول الموافقة على معالجة البيانات من خلال إعادة صياغة مفهوم اختلاف حماية البيانات الأوروبية بعد معاهدة لشبونة: أخذ الحقوق على محمل الجد»، مجلة القانون الخاص الأوروبية، المجلد 20، عدد 2، ص. 473-506.

وكالة الاتحاد الأوروبي للحقوق الأساسية (2010)، حماية البيانات في الاتحاد الأوروبي: دور الهيئات الإشرافية الوطنية (تعزيز هيكل الحقوق الأساسية في الاتحاد الأوروبي II)، لوكسمبورغ، مكتب الإصدارات في الاتحاد الأوروبي (مكتب الاصدارات).

وكالة الاتحاد الأوروبي للحقوق الأساسية (2010)، تطوير مؤشرات من أجل حماية حقوق الطفل في الاتحاد الأوروبي واحترامها والنهوض بها (نسخة المؤتمر)، فيينا، وكالة الاتحاد الأوروبي للحقوق الأساسية.

وكالة الاتحاد الأوروبي للحقوق الأساسية (2011)، الوصول إلى العدالة في أوروبا: نظرة عامة على التحديات والفرص، لوكسمبورغ، مكتب الإصدارات.

هيئة المعلومات الصحية والجودة الآيرلندية (2010)، إرشادات حول تقييم أثر الخصوصية في الرعاية الصحية والاجتماعية.

كيركفارد، س.، واترز، ن.، غرينليف، غ.، بايفريف، ل. أ. ، لويد، إ. وساكسبي، س. (2011)، «بعد مرور 30 عاماً - مراجعة اتفاقية 108 الخاصة بحماية البيانات الصادرة عن مجلس أوروبا»، مجلة قانون وأمن الحواسيب، المجلد 27، عدد 3، ص. 223-231.

سيميتيس، س. (2011)، قانون حماية البيانات الاتحادي، بادن بادن، دار «ناموس» للنشر.

مكتب مفوض المعلومات بالمملكة المتحدة، تقييم أثر الخصوصية.

**الفصل 7**

المشرف الأوروبي على حماية البيانات (2014)، بيان موقف حول نقل البيانات الشخصية إلى دول ثالثة ومنظمات دولية من قبل مؤسسات وهيئات الاتحاد الأوروبي.

غوتويرث، س. بولي، ي.، دي هيرت، ب.، دي تيروانج، س. ونووت، س. (2009)، الإصلاح الجذري لحماية البيانات، برلين، مجموعة «سبرينغر».

كونر، ك. (2007)، قانون حماية البيانات الأوروبي، أوكسفورد، مطبعة جامعة «أوكسفورد».

كونر، ك. (2013)، اللائحة الخاصة بتدفق البيانات عبر الحدود وقانون خصوصية البيانات، أوكسفورد، مطبعة جامعة «أوكسفورد».

فريق عمل المادة 29 (2005)، ورقة عمل حول التفسير المشترك للمادة 26 (1) من الأمر التوجيهي EC/95/46 بتاريخ 24أكتوبر 1995.

**الفصل 8**

بلاسي كازاغرام، ك. (2016)، الحماية العالمية للبيانات في مجال إنفاذ القانون، من منظور الاتحاد الأوروبي، لندن، دار «روتلدج» للنشر.

بويم، ف. (2012)، تبادل المعلومات وحماية البيانات في مجال الحرية والأمن والعدالة. نحو مبادئ حماية البيانات المنسقة لتبادل المعلومات على مستوى الاتحاد الأوروبي، برلين، مجموعة «سبرينغر».

اليوروبول (2012)، حماية البيانات في اليوروبول، لوكسمبورغ، مكتب الإصدارات.

وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية، حماية البيانات في وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية: نظام حسب الطلب قوي وفعال، لاهاي، وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية.

دي هيرت، ب. وباباكونستانتينو، ف. (2012)، «الأمر التوجيهي الخاص بحماية بيانات الموجه للشرطة والعدالة الجنائية: تعليق وتحليل»، مجلة الحواسيب والقانون التابعة للجمعية الخاصة بالحواسيب والقانون، المجلد 22، عدد 6، ص. 1-5.

دروور، د. إلرمان، ج. (2012)، «إطار اليوروول لحماية البيانات كمصدر قوة في محاربة الجرائم السيبرانية»، منتدى مجال البحث الأوروبي (ERA)، المجلد 13، عدد 3، ص 381-395.

غوتييريز زارزا، أ. (2015)، تبادل المعلومات وحماية البيانات في الإجراءات الجنائية العابرة للحدود في أوروبا، برلين، مجموعة «سبرينغر».

غوتويرث، س.، بولي، ي.، دي هيرت، ب. (2010)، حماية البيانات في عالم منمط، دوردريخت، مجموعة «سبرينغر».

غوتويرث، س.، بولي، ي.، دي هويت، ب. ولينز، ر. (2011)، الحواسيب والخصوصية وحماية البيانات: عنصر اختيار، دوردريخت، مجموعة «سبرينغر».

كونستادينيديس، ت. (2011)، «تدمير الديمقراطية بحجة الدفاع عنها؟ الأمر التوجيهي الخاص بالاحتفاظ بالبيانات، دولة المراقبة ومنظومتنا الدستورية»، مجلة القانون الأوروبي، المجلد 36، عدد 5، ص. 722-776.

سانتوس فارا، ج. (2013)، دور البرلمان الأوروبي في إبرام اتفاقيات عبر أطلسية بشأن نقل البيانات الشخصية بعد معاهدة لشبونة، مركز قانون العلاقات الخارجية، أوراق عمل منصة « كلير» .2013/2.

**الفصل 9**

بوليسباخ، أ.، جيجراث، س.، بولي، ي. وهاكون، ر. (2010)، قانون تكنولوجيا المعلومات الأوروبي الموجز، أمستردام، مجموعة «كلوير» للقانون الدولي.

غوتويرث، س.، لينيز، ر.، دي هيرت، ب. وبولي، ي(2012) ، حماية البيانات الأوروبية: هل هي في صحة جيدة؟ دوردريخت، مجموعة «سبرينغر».

غوتويرث، س.، بولي، ي. ودي هيرت، ب. (2010)، حماية البيانات في عالم منمط، دوردريخت، مجموعة «سبرينغر».

غوتويرث، س.، بولي، ي.، دي هيرت، ب.، ولينز، ر. (2011)، الحواسيب والخصوصية وحماية البيانات: عنصر اختيار، دوردريخت، مجموعة «سبرينغر».

كونستادينيديس، ت. (2011)، «تدمير الديمقراطية بحجة الدفاع عنها؟ الأمر التوجيهي الخاص بالاحتفاظ بالبيانات، دولة المراقبة ومنظومتنا الدستورية»، مجلة القانون الأوروبي، المجلد 36، عدد 5، ص. 722-776.

روزماري، ج.، وهاميلتون، أ. (2012)، قانون وممارسة حماية البيانات، لندن، دار «سويت & ماكسويل» للنشر.

**الفصل 10**

الإمام، خ. وألفاريز، س. (2015)، «تقييم نقدي للرأي 05/2014 لفريق عمل المادة 29 حول تقنيات إخفاء هوية البيانات»، قانون خصوصية البيانات الدولي، المجلد 5، عدد 1، ص. 73-87.

ماير-شونبيرغر، ف.، كيت، ف. (2013)، «الإشعار والموافقة في عالم البيانات الضخمة»، قانون خصوصية البيانات الدولي، المجلد 3، عدد 2، ص. 67-73.

روبشتين، إ. (2013)، «البيانات الضخمة: نهاية الخصوصية أم بداية جديدة؟»، لقانون خصوصية البيانات الدولي، المجلد 3، عدد 2، ص. 74-87.

# السوابـــق القضائيـــة

## السوابق القضائية المختارة للمحكمة الأوروبية لحقوق الإنسان

**الوصول إلى البيانات الشخصية**

قضية «غاسكين ضد المملكة المتحدة»، رقم 10454/83، 7 يوليو 1989

قضية «غوديلي ضد إيطاليا»، رقم 33783/09، 25 سبتمبر 2012

قضية «ك. ه. وآخرون ضد سلوفاكيا»، رقم 04/32881، 28 أبريل 2009

قضية «ليندر ضد السويد»، رقم 9248/81، 26 مارس 1987

قضية «م. ك. ضد فرنسا»، رقم 19522/09، 18 أبريل 2013

قضية «أودييفر ضد، فرنسا» [الغرفة الكبرى]، رقم 42326/98، 13 فبراير 2003.

**التوفيق بين حماية البيانات وحرية التعبير والحق في المعلومات**

قضية شركة «'أكسيل سبرينغر' المساهمة ضد ألمانيا» [الغرفة الكبرى]، رقم 39954/08، 7 فبراير 2012

قضية «بوهلين ضد ألمانيا»، رقم 53495/09، 19 فبراير 2015

قضية شركة «كوديرك وهاشيت فيلياكي» ضد فرنسا [الغرفة الكبرى]، رقم 40454/07، 10 نوفمبر 2015

قضية «ماغيار هيلسينكي بيزوتساغ ضد المجر» [الغرفة الكبرى]، رقم 18030/11، 8 نوفمبر 2016

قضية «مولر وآخرين ضد سويسرا»، رقم 10737/84، 24 مايو 1988

قضية شركتي «ساتاكونان ماركينابورسي» و «ساتاميديا» المحدودتين ضد فنلندا، رقم 931/13، 27 يونيو 2017

قضية «نقابة الفنانين التشكيليين النمساويين ضد النمسا»، رقم 68354/01، 25 يناير 2007

قضية «فون هانوفر ضد ألمانيا» (رقم 2)، [الغرفة الكبرى]، رقمي 08/40660 و08/60641، 7 فبراير 2012

**التوفيق بين حماية البيانات وحرية الدين**

قضية «سنان إشيك ضد تركيا»، رقم 21924/05، 2 فبراير 2010

**التحديات المتعلقة بحماية البيانات على الانترنت**

قضية «ك. ي. ضد فنلندا»، رقم 2872/02، 2 ديسمبر 2008

**موافقة صاحب البيانات**

قضية «إلبيرت ضد لاتفيا»، رقم 61243/08، 13 يناير 2015

قضية «سنان إشيك ضد تركيا»، رقم 21924/05، 2 فبراير 2010

قضية «ي. ضد تركيا»، رقم 648/10، 17 فبراير 2015

**المراسلة**

قضية «أمان ضد سويسرا» [الغرفة الكبرى]، رقم 27798/95، 16 فبراير 2000

قضية «جمعية التكامل الأوروبي وحقوق الإنسان وإكيمزييف ضد بلغاريا»، رقم 62540/00، 28 يونيو 2007

قضية «شركة 'بيرن لارسن هولدينغ' المحدودة وآخرون ضد النرويج»، رقم 24117/08، 14 مارس 2013

قضية «جماليتين جانلي ضد تركيا»، رقم 22427/04، 18 نوفمبر 2008

قضية «د. ل. ضد بلغاريا»، رقم 7472/14، 19 مايو 2016

قضية «داليا ضد فرنسا»، رقم 07/964، 2 فبراير 2010

قضية «غاسكين ضد المملكة المتحدة»، رقم 10454/83، 7 يوليو 1989

قضية «هارالامبي ضد رومانيا»، رقم 03/21737، 27 أكتوبر 2009

قضية «خليلي ضد سويسرا»، رقم 16188/07، 18 أكتوبر 2011

قضية «ليندر ضد السويد»، رقم 9248/81، 26 مارس 1987

قضية «مالون ضد المملكة المتحدة»، رقم 8691/79، 2 أغسطس 1984

قضية «روتارو ضد رومانيا» [الغرفة الكبرى]، رقم 28341/95، 4 مايو 2000

قضية «س. ومارير ضد المملكة المتحدة» [الغرفة الكبرى]، رقم 30562/04 ورقم 30566/04، 4 ديسمبر 2008

قضية «شيموفولوس ضد روسيا»، رقم 30194/09، 21 يونيو 2011

قضية «سيلفر وآخرون ضد المملكة المتحدة»، رقم5947/72 ، و6205/73، و7052/75، و7061/75 و7107/75 و7113/75، 25 مارس 1983

قضية «'ذا صنداي تايمز' ضد المملكة المتحدة»، رقم 6538/74، 26 أبريل1979

**قواعد بيانات السجل العدلي**

قضية «أيكاغير ضد فرنسا»، رقم 8806/12، 22 يونيو 2017

قضية «ب. ب. ضد فرنسا»، رقم 5335/06، 17 ديسمبر 2009

قضية «برونيه ضد فرنسا»، رقم 21010/10، 18 سبتمبر 2014

قضية «م. ك. ضد فرنسا»، رقم 19522/09، 18 أبريل 2013

قضية «م. م. ضد المملكة المتحدة»، رقم 24029/07، 13 نوفمبر 2012

**أمن البيانات**

قضية «هارالامبي ضد رومانيا»، رقم 03/21737، 27 أكتوبر 2009

قضية «ك. ه. وآخرون ضد سلوفاكيا»، رقم 04/32881، 28 أبريل 2009

**قاعدة بيانات الحمض النووي**

قضية «س. ومارير ضد المملكة المتحدة» [الغرفة الكبرى]، رقم 30562/04 ورقم 30566/04، 4 ديسمبر 2008

**بيانات نظام تحديد الموقع**

قضية «أوزون ضد ألمانيا»، رقم 35623/05، 2 سبتمبر 2010.

**البيانات المتعلقة بالصحة**

قضية «أفيلكينا وآخرون ضد روسيا»، رقم 1585/09، 6 يونيو 2013
قضية «بيريوك ضد ليتوانيا»، رقم 23373/03، 25 نوفمبر 2008
قضية «إ ضد فنلندا»، رقم 20511/03، 17 يوليو 2008
قضية «ل. ه. ضد لاتفيا»، رقم 52019/07، 29 أبريل 2014
قضية «ل. ل. ضد فرنسا»، رقم 7508/02، 10 أكتوبر 2006
قضية «م. س. ضد السويد»، رقم 20837/92، 27 أغسطس 1997
قضية «شولوك ضد المملكة المتحدة»، رقم 36936/05، 2 يونيو 2009
قضية «ي. ضد تركيا»، رقم 648/10، 17 فبراير 2015
قضية «ز ضد فنلندا»، رقم 22009/93، 25 فبراير 1997

**الهوية**

قضية «تشيوبوتارو ضد مولدوفا»، رقم 27138/04، 27 أبريل 2010
قضية «غوديلي ضد إيطاليا»، رقم 33783/09، 25 سبتمبر 2012
قضية «أوديفر ضد، فرنسا» [الغرفة الكبرى]، رقم 42326/98، 13 فبراير 2003

**المعلومات المتعلقة بالأنشطة المهنية**

قضية «'غ.س.ب.' ضد سويسرا»، رقم 28601/11، 22 ديسمبر 2015
قضية «م. ن. وآخرون ضد سان مارينو»، رقم 28005/12، 7 يوليو 2015
قضية «ميشو ضد فرنسا»، رقم 12323/11، 6 ديسمبر 2012
قضية «نييميتز ضد ألمانيا»، رقم 13710/88، 16 ديسمبر 1992

**اعتراض الاتصال**

قضية «أمان ضد سويسرا» [الغرفة الكبرى]، رقم 27798/95، 16 فبراير 2000
قضية «بريتو فيرينهو بكسيغا فيلا-نوفا ضد البرتغال»، رقم 69436/10، 1 ديسمبر 2015
قضية «كوبلاند ضد المملكة المتحدة»، رقم 62617/00، 3 أبريل 2007
قضية «هالفورد ضد المملكة المتحدة»، رقم 20605/92، 25 يونيو 1997
قضية «إيورداتشي وآخرون ضد مولدوفا»، رقم 25198/02، 10 فبراير 2009
قضية «كوب ضد سويسرا»، رقم 23224/94، 25 مارس 1998
قضية «ليبرتي وآخرون ضد المملكة المتحدة»، رقم 58243/00، 1 يوليو 2008
قضية «مالون ضد المملكة المتحدة»، رقم 8691/79، 2 أغسطس 1984
قضية «مصطفى سيزغين تانريكولو ضد تركيا»، رقم 27473/06، 18 يوليو 2017
قضية «بروتانو ضد رومانيا»، رقم 30181/05، 3 فبراير 2015
قضية «شولوك ضد المملكة المتحدة»، رقم 36936/05، 2 يونيو 2009

**التزامات الجهات المكلفة بالمسؤولية**

قضية «ب.ب. ضد فرنسا»، رقم 5335/06، 17 ديسمبر 2009
قضية «إ ضد فنلندا»، رقم 20511/03، 17 يوليو 2008
قضية «موزلي ضد المملكة المتحدة»، رقم 48009/08، 10 مايو 2011

**البيانات الشخصية**

قضية «أمان ضد سويسرا» [الغرفة الكبرى]، رقم 27798/95، 16 فبراير 2000

قضية «أوتسون ضد ألمانيا»، رقم 35623/05، 2010

قضية «بيرن لارسن هولدينغ (شركة محدودة) وآخرون ضد النرويج»، رقم 24117/08، 14 مارس 2013

**الصور**

قضية «شياكا ضد إيطاليا»، رقم 50774/99، 11 يناير 2005

قضية «فون هانوفر ضد ألمانيا»، رقم 59320/00، 24 يونيو 2004

**الحق في النسيان (حق المرء في أن يُنسى)**

قضية «سيغشدد-فيلباي وآخرون ضد السويد»، رقم 62332/00، 6 يونيو 2006

قضية «'ساتاكونان ماركينابورسو المحدودة' و'ساتاميديا المحدودة' ضد فنلندا»، رقم 931/13، 27 يونيو 2017

**الحق في الاعتراض**

قضية «لياندر ضد السويد»، رقم 9248/81، 26 مارس 1987

قضية «م.س. ضد السويد»، رقم 20837/92، 27 أغسطس 1997

قضية «موزلي ضد المملكة المتحدة»، رقم 48009/08، 10 مايو 2011

قضية «روتارو ضد رومانيا» [الغرفة الكبرى]، رقم 28341/95، 4 مايو 2000

قضية «سينان إيشيك ضد تركيا»، رقم 21924/05، 2 فبراير 2010

**الفئات الحساسة من البيانات**

قضية «برونيه ضد فرنسا»، رقم 21010/10، 18 سبتمبر 2014

قضية «إ ضد فنلندا»، رقم 20511/03، 17 يوليو 2008

قضية «ميشود ضد فرنسا»، رقم 12323/11، 6 ديسمبر 2012

قضية «س. ومارير ضد المملكة المتحدة» [الغرفة الكبرى]، رقما 30562/04 و30566/04، 4 ديسمبر 2008

**الإشراف والتنفيذ (دور مختلف الجهات الفاعلة، بما فيها الهيئات الإشرافية)**

قضية «إ ضد فنلندا»، رقم 20511/03، 17 يوليو 2008

قضية «ك.و. ضد فنلندا»، رقم 2872/02، 2 ديسمبر 2008

قضية «فون هانوفر ضد ألمانيا»، رقم 59320/00، 24 يونيو 2004

قضية «فون هانوفر ضد ألمانيا (رقم 2)» [الغرفة الكبرى]، رقما 40660/08 و60641/08، 7 فبراير 2012

**طرق المراقبة**

قضية «ألان ضد المملكة المتحدة»، رقم 48539/99، 5 نوفمبر 2002

قضية «رابطة التكامل الأوروبي وحقوق الإنسان وإيكيمزييف ضد بلغاريا»، رقم 62540/00، 28 يونيو 2007

قضية «باربوليسكو ضد رومانيا» [الغرفة الكبرى]، رقم 61496/08، 5 سبتمبر 2017

قضية «د.ل. ضد بلغاريا»، رقم 7472/14، 19 مايو 2016

قضية «دراغوييفيتش ضد كرواتيا»، رقم 68955/11، 15 يناير 2015

قضية «كارابيوغلو ضد تركيا»، رقم 30083/10، 7 يونيو 2016
قضية « كلاس وآخرون ضد ألمانيا»، رقم 5029/71، 6 سبتمبر 1978
قضية «روتارو ضد رومانيا» [الغرفة الكبرى]، رقم 28341/95، 4 مايو 2000
قضية « سزابو وفيسي ضد المجر»، رقم 37138/14، 12 يناير 2016
قضية « تايلور-سابوري ضد المملكة المتحدة»، رقم 47114/99، 22 أكتوبر 2002
قضية «أوزون ضد ألمانيا»، رقم 35623/05، 2 سبتمبر 2010
قضية «فيرزيني-كامبينكي وكراسنيانسكي ضد فرنسا»، رقم 49176/11، 16 يونيو 2016
قضية « فيتر ضد فرنسا»، رقم 59842/00، 31 مايو 2005
قضية «فوكوتا-بوجيتش ضد سويسرا»، رقم 61838/10، 18 أكتوبر 2016
قضية « رومان زخاروف ضد روسيا» [الغرفة الكبرى]، رقم 47143/06، 4 ديسمبر 2015

**المراقبة بالفيديو**

قضية «كوبكه ضد ألمانيا»، رقم 420/07، 5 أكتوبر 2010
قضية «بيك ضد المملكة المتحدة»، رقم 44647/98، 28 يناير 2003

**العينات الصوتية**

قضية «ويس ضد فرنسا»، رقم 71611/01، 20 ديسمبر 2005
قضية «ب.ج. وج.هـ. ضد المملكة المتحدة»، رقم 44787/98، 25 سبتمبر 2001

## السوابق القضائية المختارة لمحكمة العدل التابعة للاتحاد الأوروبي

**السوابق القضائية المتعلقة بالأمر التوجيهي المتعلق بحماية البيانات**

القضية C-13/16، «إدارة الشرطة الإقليمية في ريغا ضد شركة 'ريغاس ساتيكسمي' للنقل التابعة لبلدية ريغا»، 4 مايو 2017
[مبدأ المعالجة المشروعة: المصلحة المشروعة التي يسعى إليها طرف ثالث]

القضية C-398/15، «غرفة التجارة والصناعة والحرف التقليدية والفلاحة لمدينة ليتشي ضد سالفاتوري ماني»، 9 مارس 2017
[حق المرء في أن تُمحى بياناته الشخصية؛ الحق في الاعتراض على المعالجة]

القضيتان المضمومتان C-203/15 وC-698/15، «تيلي 2 السويد المحدودة ووزارة الداخلية ضد طوم واطسون وآخرين» [الغرفة الكبرى]، 21 ديسمبر 2016
[سرية الاتصالات الإلكترونية؛ مزودو خدمات الاتصالات الإلكترونية؛ الالتزام المتعلق بالاحتفاظ العام والعشوائي ببيانات المرور والموقع؛ لا يوجد استعراض مسبق من قبل محكمة أو سلطة إدارية مستقلة؛ ميثاق الحقوق الأساسية للاتحاد الأوروبي؛ التوافق مع قانون الاتحاد الأوروبي]

القضية C-582/14، «باتريك برايير ضد جمهورية ألمانيا الاتحادية»، 19 أكتوبر 2016
[تعريف 'البيانات الشخصية'؛ عناوين بروتوكول الإنترنت؛ تخزين البيانات من قبل مزود خدمات الوسائط عبر الإنترنت؛ عدم سماح التشريعات الوطنية بأخذ المصلحة المشروعة للمراقب في الاعتبار]

القضية C-362/14، «ماكسيميليان شريمز ضد مفوض حماية البيانات» [الغرفة الكبرى]، 6 أكتوبر 2015
[مبدأ المعالجة القانونية؛ الحقوق الأساسية؛ بطلان قرار «الملاذ الآمن»؛ صلاحيات الهيئات الرقابية المستقلة]

القضية C-230/14، «'فيلتيمو' (شركة محدودة) ضد الهيئة الوطنية لحماية البيانات وحرية المعلومات»، 1 أكتوبر 2015
[صلاحيات الهيئات الإشرافية الوطنية]

القضية C-201/14، «سمارانداا بارا وآخرون ضد الصندوق الوطني للتأمين الصحي وآخرين»، 1 أكتوبر 2015
[الحق في الحصول على معلومات بشأن معالجة البيانات الشخصية]

القضية C-212/13، «فرانتيسيك رانيس ضد مكتب حماية البيانات الشخصية»، 11 ديسمبر 2014
[مفهوم «معالجة البيانات» و«المراقب»]

القضية C-473/12، «المعهد المهني للوكلاء العقاريين (IPI)» ضد جيفري انغلبرت وآخرين»، 7 نوفمبر 2013
[الحق في الحصول على معلومات بشأن معالجة البيانات الشخصية]

القضية T-462/12 R، «مجموعة 'بيلكنتون' المحدودة ضد المفوضية الأوروبية»، أمر رئيس المحكمة العامة، 11 مارس 2013

القضية C-342/12، «شركة 'فورتن' للتجهيزات المنزلية المحدودة ضد هيئة ظروف العمل (ACT)»، 30 مايو 2013
[مفهوم 'البيانات الشخصية'؛ سجل وقت العمل؛ المبادئ المتعلقة بجودة البيانات ومعايير إضفاء الشرعية على معالجة البيانات؛ وصول الهيئة الوطنية المسؤولة عن مراقبة ظروف العمل؛ التزام صاحب العمل بإتاحة سجل وقت العمل للسماح بالاطلاع الفوري عليه]

القضيتان المضمومتان C-293/12 وC-594/12، «شركة 'ديجيتال رايتس آيرلاند' المحدودة ضد وزير الاتصالات والموارد البحرية والطبيعية وآخرين» و «ضد حكومة مقاطعة كارينثيان وآخرين» [الغرفة الكبرى]، 8 أبريل 2014
[انتهاك الأمر التوجيهي المتعلق بالاحتفاظ بالبيانات للقانون الأساسي للاتحاد الأوروبي؛ المعالجة المشروعة؛ حصر الغرض ومدة التخزين]

القضية C-288/12، «المفوضية الأوروبية ضد المجر» [الغرفة الكبرى]، 8 أبريل 2014
[شرعية عزل منصب المشرف الوطني على حماية البيانات]

القضيتان المضمومتان C-141/12 وC-372/12، «إ. س. ضد وزير الهجرة والاندماج واللجوء» و«وزير الهجرة والاندماج واللجوء ضد م. وس»، 17 يوليو 2014
[نطاق حق صاحب البيانات في الوصول إلى بياناته؛ حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية؛ مفهوم 'البيانات الشخصية'؛ البيانات المتعلقة بمقدم طلب تصريح الإقامة والتحليل القانوني الوارد في وثيقة إدارية تحضيرية للقرار؛ ميثاق الحقوق الأساسية للاتحاد الأوروبي]

القضية C-131/12، «'غوغل إسبانيا' (شركة المحدودة) التابعة لشركة 'غوغل' ضد الوكالة الإسبانية لحماية البيانات (APED) وماريو كوستيخا غونثاليث» [الغرفة الكبرى]، 13 مايو 2014
[التزامات مزودي محركات البحث بالامتناع، بناءً على طلب صاحب البيانات، عن إظهار البيانات الشخصية في نتائج البحث؛ انطباق الأمر التوجيهي المتعلق بحماية البيانات؛ مفهوم «معالجة البيانات»؛ معنى «المراقبون»؛ الموازنة بين حماية البيانات وحرية التعبير؛ الحق في النسيان]

القضية C-614/10، «المفوضية الأوروبية ضد جمهورية النمسا» [الغرفة الكبرى]، 16 أكتوبر 2012
[استقلالية هيئة إشرافية وطنية]

القضيتان المضمومتان C-468/10 وC-469/10، «الرابطة الوطنية لمؤسسات الائتمان المالي (ASNEF) واتحاد التجارة الإلكترونية والتسويق المباشر (FECEMD) ضد إدارة الدولة»، 24 نوفمبر 2011
[التنفيذ الصحيح للمادة 7 (و) من الأمر التوجيهي المتعلق بحماية البيانات - «المصالح المشروعة للآخرين» - في القانون الوطني]

القضية C-360/10، «الشركة البلجيكية للمؤلفين والملحنين والناشرين (SABAM) (شركة تعاونية ذات مسؤولية محدودة)» ضد 'نتلوغ' (شركة محدودة)»، 16 فبراير 2012
[التزام مزودي الشبكات الاجتماعية بمنع الاستخدام غير المشروع للأعمال الموسيقية والسمعية والبصرية من قبل مستخدمي الشبكة]

القضية C-70/10، «سكارليت إكستنديد (شركة مغفلة) ضد الشركة البلجيكية للمؤلفين والملحنين والموزعين الموسيقيين (SABAM) (شركة تعاونية ذات مسؤولية محدودة)»، 24 نوفمبر 2011
[مجتمع المعلومات؛ حقوق النشر؛ شبكة الإنترنت؛ برمجيات 'النظير للنظير' (peer-to-peer)؛ مزودو خدمات الإنترنت؛ تركيب نظام لترشيح الاتصالات الإلكترونية لمنع عمليات مشاركة الملفات التي تنتهك حقوق النشر؛ عدم وجود التزام عام برصد المعلومات المنقولة]
القضية C-543/09، «دويتشه تيليكوم (شركة عامة محدودة) ضد جمهورية ألمانيا الاتحادية»، 5 مايو 2011
[ضرورة تجديد الموافقة]

القضيتان المضمومتان C-92/09 و C-93/09 «فولكر وماركوس شيكه (شركة يحكمها القانون المدني الألماني) وهارتموت أيفرت ضد لاند هيسن» ]الغرفة الكبرى[، 9 نوفمبر 2010
[مفهوم «البيانات الشخصية»؛ تناسب الالتزام القانوني بنشر البيانات الشخصية حول المستفيدين من بعض الصناديق الفلاحية في الاتحاد الأوروبي]

القضية C-553/07، «مجلس العمدة وأعضاء مجلس بلدية روتردام ضد م.إ.إ. رايكيبور»، 7 مايو 2009
[حق صاحب البيانات في الوصول]

القضية C-518/07، «المفوضية الأوروبية ضد جمهورية ألمانيا الاتحادية» [الغرفة الكبرى]، 9 مارس 2010
[استقلالية هيئة إشراف الوطنية]

القضية C-73/07، «مسؤول حماية البيانات ضد شركة 'ساتاكونان ماركينابورسي' المحدودة وشركة 'ساتاميديا' المحدودة»، [الغرفة الكبرى]، 16 ديسمبر 2008
[مفهوم 'الأنشطة الصحفية' بالمعنى المقصود في المادة 9 من الأمر التوجيهي المتعلق بحماية البيانات]

القضية C-524/06، «هاينز هوبر ضد. جمهورية ألمانيا الاتحادية» [الغرفة الكبرى]، 16 ديسمبر 2008
[شرعية الاحتفاظ ببيانات الأجانب في سجل إحصائي]

القضية C-275/06، «منتجو الموسيقى إسبانيا (بروموسيكاي) ضد تيليفونيكا إسبانيا (شركة ذات مساهم واحد)» [الغرفة الكبرى]، 29 يناير 2008
[مفهوم «البيانات الشخصية»؛ التزام مزودي الوصول إلى الإنترنت بالكشف عن هوية مستخدمي برمجيات تبادل الملفات (KaZaA) لجمعية حماية الملكية الفكرية]

القضية C-101/01، «دعوى جنائية في حق بوديل لينغفيست»، 6 نوفمبر 2003
[فئات خاصة من البيانات الشخصية]

القضايا المضمومة C-465/00 و C-138/01 وC-139/01، «ديوان المحاسبة ضد الإذاعة النمساوية وآخرين» و«كريستا نويكوم وجوزيف لاويرمان ضد الإذاعة النمواسية»، 20 مايو 2003
[تناسبية الالتزام القانوني بنشر البيانات الشخصية حول رواتب الموظفين في فئات معينة من المؤسسات ذات الصلة بالقطاع العام]

القضية C 434/16، «بيتر نوفاك ضد مفوض حماية البيانات»، رأي المحامي العام كوكوت، 20 يوليو 2017
[مفهوم البيانات الشخصية؛ وصول الفرد إلى نص الاختبار الخاص به؛ تصحيحات الفاحص]

القضية C-291/12، «مايكل شوارز ضد مدينة بوخوم»، 17 أكتوبر 2013
[الإحالة إلى حكم أولي؛ مجال الحرية والأمن والعدالة؛ جواز السفر البيومتري؛ بصمات الأصابع؛ أساس قانوني؛ التناسب]

**السوابق القضائية المتعلقة بالأمر التوجيهي 2016/681**

الرأي 1/15 الصادر عن المحكمة [الغرفة الكبرى]، 26 يوليو 2017
[الأساس القانوني؛ مشروع اتفاق بين كندا والاتحاد الأوروبي بشأن نقل ومعالجة بيانات سجلات أسماء الركاب؛ توافق مشروع الاتفاق مع المادة 16 من المعاهدة المتعلقة بسير عمل الاتحاد الأوروبي والمادتين 7 و8 والمادة 52 (1) من ميثاق الحقوق الأساسية للاتحاد الأوروبي]

**السوابق القضائية المتعلقة بلائحة حماية البيانات الخاصة بمؤسسات الاتحاد الأوروبي**

القضية P C-615/13، «'كلاينت أورث' و'شبكة عمل مبيدات الآفات في أوروبا' (PAN Europe) ضد الهيئة الأوروبية للسلامة الغذائية (EFSA)»، المفوضية الأوروبية، 16 يوليو 2015
[الوصول إلى الوثائق]

القضية C-28/08 P، «المفوضية الأوروبية ضد شركة 'بافاريان لايجر' المحدودة» [الغرفة الكبرى]، 29 يونيو 2010
[الوصول إلى الوثائق]

**السوابق القضائية المتعلقة بالأمر التوجيهي EC/2002/58**

القضية C-536/15، «تيلي 2 (المملكة الهولندية) (شركة محدودة) وآخرون ضد هيئة المستهلكين والأسواق (AMC)»، 15 مارس 2017
[مبدأ عدم التمييز؛ إتاحة البيانات الشخصية المتعلقة بالمشتركين لأغراض توفير خدمات الاستعلام عن الأدلة المتاحة للجمهور والأدلة المتاحة للجمهور؛ موافقة المشترك؛ التمييز على أساس الدولة العضو التي تقدم فيها خدمات الاستعلام عن الأدلة المتاحة للجمهور والأدلة المتاحة للجمهور]

القضيتان المضمومتان C-203/15 و C-698/15، «أ ب ضد وكالة البريد والاتصالات السويدية» و«وزير الدولة للشؤون الداخلية ضد توم واتسون وآخرين» [الغرفة الكبرى]، 21 ديسمبر 2016
[سرية الاتصالات الإلكترونية؛ مزودو خدمات الاتصالات الإلكترونية؛ الالتزام المتعلق بالاحتفاظ العام والعشوائي ببيانات المرور والموقع؛ عدم وجود مراجعة مسبقة من قبل محكمة أو سلطة إدارية مستقلة؛ ميثاق الحقوق الأساسية للاتحاد الأوروبي؛ التوافق مع قانون الاتحاد الأوروبي]

القضية C-70/10، «سكارليت إكستنديد (شركة مغفلة) ضد الشركة البلجيكية للمؤلفين والملحنين والموزعين الموسيقيين (SABAM) (شركة تعاونية ذات مسؤولية محدودة)»، 24 نوفمبر 2011
[مجتمع المعلومات؛ حقوق النشر؛ شبكة الإنترنت؛ برمجيات «النظير للنظير»؛ مزودو خدمات الإنترنت؛ تثبيت نظام لترشيح الاتصالات الإلكترونية لمنع عمليات مشاركة الملفات التي تنتهك حقوق النشر؛ عدم وجود التزام عام برصد المعلومات المنقولة]

القضية C-461/10، «'بونيي أوديو' (شركة محدودة) وايربوكس (شركة محدودة) و'نورشتيتس فولاغسفروب' (شركة محدودة) و'بيراتفولاغيت (شركة محدودة) و'ستوريساید (شركة محدودة) ضد 'بيرفيكت كوميونيكايشن السويد' (شركة محدودة)»، 19 أبريل 2012
[حقوق النشر والحقوق الأخرى المتعلقة به؛ معالجة البيانات عبر الإنترنت؛ التعدي على حق حصري؛ الكتب الصوتية التي يتم توفيرها بواسطة خادم بروتوكول نقل الملفات (FTP) عبر الإنترنت بواسطة عنوان بروتوكول الإنترنت (IP) يوفره مزود خدمة الإنترنت؛ قرار احترازي صادر ضد مزود خدمة الإنترنت يأمره بتقديم اسم وعنوان مستخدم عنوان بروتوكيل الإنترنت]

# الفهـــــرس

## السوابق القضائية لمحكمة العدل التابعة للاتحاد الأوروبي

### السوابق القضائية للمحكمة الأوروبية لحقوق الإنسان

**السوابق القضائية للمحاكم الوطنية**

يتوفر قدر كبير من المعلومات حول وكالة الاتحاد الأوروبي للحقوق الأساسية على الإنترنت. ويمكن الوصول إليها من خلال موقع وكالة الاتحاد الأوروبي للحقوق الأساسية على : fra.europa.eu

يتوفـر مزيد من المعلومـات حول السوابـق القضائيـة للمحكمة الأوروبية لحقـوق الإنسان على موقع الويب الخاص بالمحكمة: echr.coe.int. وتمنح بوابة البحث قاعدة بيانات المحكمة الأوروبية لحقوق الإنسان (HUDOC) الوصول إلى الأحكام والقرارات باللغتين الإنجليزية و/أو الفرنسية، والترجمات إلى لغات إضافية، والملخصات القانونية، والبيانات الصحفية، وغيرها من المعلومات حول عمل المحكمة : http://hudoc.echr.coe.int.

**كيفية الحصول على منشورات مجلس أوروبا**

تنتج دار النشر «منشورات مجلس أوروبا» أعمالاً في جميع المجالات المرجعية للمنظمة، بما في ذلك حقوق الإنسان والعلوم القانونية والصحة والأخلاق والشؤون الاجتماعية والبيئة والتعليم والثقافة والرياضة والشباب والتراث المعماري. يمكن طلب الكتب والمنشورات الإلكترونية من الدليل الشامل عبر الإنترنت : http://book.coe.int/.

تتيح غرفة القراءة الافتراضية للمستخدمين الاطلاع على مقتطفات من الأعمال الرئيسية المنشورة للتو أو النصوص الكاملة لوثائق رسمية معينة دون أي تكلفة.

يمكن الحصول على معلومات عن اتفاقيات مجلس أوروبا بالإضافة إلى النصوص الكامل لها من موقع الويب الخاص بمكتب المعاهدات: http://conventions.coe.int/.

**كيف تتصل بالاتحاد الأوروبي؟**

**شخصيا**
في جميع أنحاء الاتحاد الأوروبي ، توجد المئات من مراكز معلومات Europe Direct تحت تصرفك. لمعرفة عنوان أقرب مركز، قم بزيارة الصفحة التالية: https://european-union.europa.eu/contact-eu_fr

**عن طريق الهاتف أو البريد الإلكتروني**
Europe Direct هي خدمة تجيب على أسئلتك حول الاتحاد الأوروبي. يمكنك الاتصال بهذه الخدمة:
• عن طريق الهاتف:
- عبر رقم مجاني: 11 10 9 8 7 6 800 00 (بعض المشغلين يتقاضون رسوما مقابل هذه المكالمات) ،
- الرقم القياسي التالي: 22999696 32+؛
• عن طريق البريد الإلكتروني عبر الصفحة
https://european-union.europa.eu/contact-eu_fr

**منشورات الاتحاد الأوروبي**
يمكنك تنزيل أو طلب منشورات مجانية ومدفوعة من موقع مكتبة الاتحاد الأوروبي على:
https://op.europa.eu/fr/web/general-publications/publications
يمكنك الحصول على عدة نسخ من المنشورات المجانية عن طريق الاتصال ب Europe Direct أو مركز المعلومات المحلي الخاص بك
https://european-union.europa.eu/contact-eu_fr

**قانون الاتحاد الأوروبي والوثائق ذات الصلة**
للوصول إلى المعلومات القانونية للاتحاد الأوروبي ، بما في ذلك جميع قوانين الاتحاد الأوروبي منذ عام ١٩٥٢ بجميع إصدارات اللغات الرسمية ، قم بزيارة EUR-Lex على:
https://eur-lex.europa.eu/

**البيانات المفتوحة من الاتحاد الأوروبي**
بوابة الاتحاد الأوروبي للبيانات المفتوحة
https://data.europa.eu/en
يوفر الوصول إلى مجموعات البيانات من الاتحاد الأوروبي. يمكن تنزيل البيانات وإعادة استخدامها مجانا ، لأغراض تجارية أو غير تجارية.

أدى التطور السريع لتكنولوجيا المعلومات إلى تفاقم الحاجة إلى حماية قوية للبيانات الشخصية، والتي تحميها أدوات كل من الاتحاد الأوروبي (EU) ومجلس أوروبا (CoE). إن صون هذا الحق المهم ينطوي على تحديات جديدة وهامة، حيث يوسع التقدم التكنولوجي حدود بعض المجالات مثل المراقبة واعتراض الاتصالات وتخزين البيانات. وقد تم إعداد هذا الدليل لإطلاع الممارسين القانونيين غير المتخصصين في حماية البيانات بهذا المجال الناشئ من القانون، كما يقدم لمحة عامة عن الأطر القانونية المعمول بها في الاتحاد الأوروبي ومجلس أوروبا، بالإضافة إلى شرح السوابق القضائية الرئيسية، وتلخيص الأحكام الرئيسية لكل من محكمة العدل التابعة للاتحاد الأوروبي والمحكمة الأوروبية لحقوق الإنسان. علاوة على ذلك، يقدم هذا الدليل سيناريوهات افتراضية بمثابة توضيحات عملية للقضايا المتنوعة التي تمت مواجهتها في هذا المجال الذي يعرف تطوراً متواصلاً.


**وكالة الاتحاد الأوروبي للحقوق الأساسية**

شوارزنبيرجبلاتز 11 - 1040 فيينا - النمسا

الهاتف: 43+ (1) 580 30-0 - الفاكس: 43+ (1) 580 30-699

fra.europa.eu

facebook.com/fundamentalrights

linkedin.com/company/eu-fundamental-rights-agency

twitter.com/EURightsAgency

**المحكمة الأوروبية لحقوق الانسان**

**مجلس أوروبا**

67075 ستراسبورغ سيدكس - فرنسا

الهاتف: 33+ (0) 3 88 41 20 18 - الفاكس: 33+ (0) 3 88 41 27 30

echr.coe.int - publishing@echr.coe.int - twitter.com/ECHR_CEDH

**المشرف الأوروبي على حماية البيانات**

شارع ويرتز 60 - 1047 بروكسل - بلجيكا

الهاتف: 32+ 2 283 19 00

www.edps.europa.eu - edps@edps.europa.eu - twitter.com/EU_EDPS