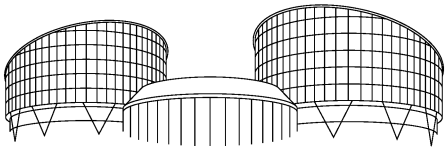

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

Le 19 novembre 2024

Séminaire judiciaire 2025

*La protection des droits de l'homme à l'ère de l'intelligence artificielle, des algorithmes et des mégadonnées (***big data***)*

Document de travail

Table des matières

Introduction 2
I. Les normes du Conseil de l'Europe et les normes européennes en matière d'intelligence artificielle : éléments de contexte 3
A. Les textes du Conseil de l'Europe 3
2. Autres textes internationaux 8
II. La jurisprudence de la Cour européenne des droits de l'homme à l'ère de l'intelligence artificielle 10
A. Liberté d'expression (article 10 de la Convention) 10
1. Nouvelles technologies 10
2. Utilisation de données à caractère personnel et de technologies de reconnaissance faciale pour l'identification de personnes exerçant leur liberté d'expression 11
3. Sécurité sur Internet et droit à l'oubli numérique 12
4. Journalisme responsable en ligne 13
5. Transferts de données et protection des sources journalistiques 15
6. Élections libres (article 3 du Protocole n° 1 à la Convention) 16
B. Droit à un procès équitable (article 6 de la Convention) 18
1. Accès à un tribunal 18
2. Audience contradictoire (communication des éléments de preuve) en matière pénale 19
3. Principe d'immédiateté dans la procédure pénale 20
4. Biais dans le système 21
5. Motivation des décisions 22
C. Interdiction de la discrimination (article 14, article 1 du Protocole n° 12 à la Convention) 23
1. Profilage racial 23
2. Biais dans le système 24
3. Données médicales sensibles et accès aux soins médicaux 24
4. Cyberviolence fondée sur le genre 25
Résumé 28
Annexe : jurisprudence 30

Introduction

« *La Cour considère que tout État qui revendique un rôle de pionnier dans l'évolution de nouvelles technologies porte la responsabilité particulière de trouver le juste équilibre en la matière* » (*S. et Marper c. Royaume-Uni* [GC], 2008, § 112).

Des progrès sans précédent ont été obtenus dans les domaines de la science et de la technologie depuis l'entrée en vigueur de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (« la Convention »). Le rythme des avancées significatives s'accélère dans le secteur des technologies de l'information et du numérique, et notamment des algorithmes et de l'intelligence artificielle (« l'IA »). L'IA, en particulier, qui n'était au départ qu'une discipline de niche dans le domaine de l'informatique, a rapidement acquis un pouvoir transformateur qui influe sur la manière dont nous interagissons avec le monde, et elle ouvre de nouvelles perspectives dans le débat sur le contenu et l'application des droits de l'homme et des libertés, et par conséquent sur la protection de ces droits et libertés.

L'écosystème juridique entourant l'IA est encore naissant, tant sur le plan de la réglementation applicable que sur celui de la jurisprudence. Ce n'est qu'en 2024 que le Conseil de l'Europe et l'Union européenne ont adopté les premiers textes juridiquement contraignants visant à établir un cadre juridique qui permette aux États de réglementer les activités menées dans le cadre du cycle de vie des systèmes d'IA et leurs effets sur les droits de l'homme. La Convention-cadre du conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit est le tout premier traité international juridiquement contraignant en la matière ; elle impose à tout État partie de garantir que les activités menées dans le cadre du cycle de vie des systèmes d'IA sont pleinement compatibles avec les droits de l'homme, la démocratie et l'état de droit. Le règlement sur l'intelligence artificielle, adopté la même année par l'Union européenne, a pour objectif d'établir un cadre juridique uniforme en vue d'assurer le développement et le déploiement responsables des systèmes d'IA tout en parant aux risques qui pourraient peser sur les valeurs protégées par l'Union européenne telles que les droits fondamentaux, la démocratie et l'état de droit. Ainsi, toute analyse menée sur l'IA et sur ses répercussions potentielles doit tenir compte de ce contexte juridique en constante évolution et de la possibilité de développements considérables dans un avenir proche.

En cette année qui marque le 75e anniversaire de la ratification de la Convention, le séminaire judiciaire, inspiré par l'actualité de ce sujet et par les réformes législatives récentes, examinera certaines des questions les plus pertinentes soulevées par le développement et par l'utilisation des systèmes d'IA, et cherchera notamment à recenser les défis et les opportunités que ces nouvelles technologies représentent pour la protection des droits de l'homme. Dans cette thématique générale, trois sous-thèmes ont été retenus dans la perspective des discussions au cours du séminaire : 1) la liberté d'expression à l'ère de l'intelligence artificielle, 2) l'intelligence artificielle et le droit à un procès équitable, et 3) les risques de discrimination liés à l'intelligence artificielle.

Le présent document de travail a pour objectif de présenter la jurisprudence de la Cour relative à certains aspects des trois thèmes de discussion sélectionnés, sans toutefois anticiper ou préjuger de quelque manière que ce soit de la manière dont la Cour tranchera telle ou telle affaire dont elle pourra être saisie et qui sera susceptible de soulever des questions relatives à l'IA.

Ce document de travail s'ouvre sur une vue d'ensemble des normes du Conseil de l'Europe en matière d'IA.

I. Les normes du Conseil de l'Europe et les normes européennes en matière d'intelligence artificielle : éléments de contexte

A. Les textes du Conseil de l'Europe

Le Conseil de l'Europe joue un rôle de premier plan dans le processus de réflexion et apporte une contribution primordiale à l'élaboration du cadre juridique dans lequel les systèmes d'IA sont appelés à évoluer. Le Conseil de l'Europe a commencé à travailler sur le thème de l'IA il y a une dizaine d'années, et il a intensifié ses efforts au cours des dernières années avec la publication, par plusieurs de ses organes et comités, de politiques, de recommandations, de déclarations, de lignes directrices et autres instruments juridiques. Le présent document de travail propose une sélection de ses publications les plus récentes en la matière (pour un aperçu des travaux réalisés jusqu'à présent ou prévus par les comités intergouvernementaux et autres entités du Conseil de l'Europe dans le domaine de l'intelligence artificielle, voir Le Conseil de l'Europe et l'intelligence artificielle).

La Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit, septembre 2024

La Convention-cadre sur l'IA a été adoptée par le Comité des Ministres du Conseil de l'Europe à Strasbourg le 17 mai 2024 et a été ouverte à la signature le 5 septembre 2024 à l'occasion de la conférence des ministres de la Justice à Vilnius (Lituanie). Elle a été signée le jour même par dix parties, dont l'Union européenne (au nom de ses vingt-sept États membres) et les États-Unis d'Amérique. Elle constitue le tout premier accord international juridiquement contraignant visant à réglementer l'ensemble du cycle de vie des systèmes d'IA et à promouvoir l'innovation responsable tout en répondant aux risques éventuels et en assurant la compatibilité de l'utilisation des systèmes d'IA avec les droits de l'homme, la démocratie et l'État de droit. Cette convention-cadre est accompagnée du rapport explicatif de la Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit, lequel, sans chercher à livrer une interprétation faisant autorité du texte de la Convention-cadre, peut faciliter la compréhension des dispositions qu'elle énonce. La Convention-cadre sur l'IA représente l'aboutissement des travaux entrepris en la matière par le Conseil de l'Europe. Il convient de noter à cet égard qu'en 2019 le Comité des Ministres du Conseil de l'Europe a instauré un Comité intergouvernemental *ad hoc* sur l'intelligence artificielle (CAHAI) et lui a assigné pour mission d'examiner la faisabilité et les éléments potentiels d'un cadre juridique pour le développement, la conception et l'application de l'IA. Dans son rapport final livré en 2021, le CAHAI a exposé les éléments potentiels d'un cadre juridique sur l'IA, fondés sur les normes du Conseil de l'Europe en matière de droits de l'homme, de démocratie et d'État de droit. Les travaux du CAHAI ont été poursuivis en 2021 par le Comité sur l'intelligence artificielle (CAI), lequel a été chargé de produire un « projet de Convention-cadre sur la conception, le développement, l'utilisation et la mise hors service des systèmes d'intelligence artificielle, fondée sur les normes du Conseil de l'Europe en matière de droits humains, de démocratie et d'état de droit, ainsi que sur d'autres normes juridiques internationales pertinentes, et propice à l'innovation ». Le CAI s'est également vu assigner la mission d'élaborer, pour la fin de l'année 2024, une « méthodologie juridiquement non contraignante pour l'évaluation des risques et de l'impact des systèmes d'IA du point de vue des droits humains, de la démocratie et de l'état de droit (méthodologie HUDERIA) » pour soutenir la mise en œuvre de la Convention-cadre sur l'IA. La méthodologie HUDERIA a pour but de fournir des évaluations détaillées des impacts potentiels et réels que la conception, le développement et l'application des systèmes d'IA pourraient avoir sur les droits de l'homme et les libertés fondamentales, la démocratie et l'état de droit. La méthodologie HUDERIA a été adoptée par le CAI le 28 novembre 2024.

L'application de l'IA dans les soins de santé et son impact sur la relation « patient-médecin », septembre 2024

Ce rapport publié par le Comité directeur du Conseil de l'Europe pour les droits humains dans les domaines de la biomédecine et de la santé (CDBIO) met l'accent sur certains principes des droits humains mentionnés dans la « Convention d'Oviedo » qui revêtent une importance particulière dans la relation thérapeutique, à savoir l'autonomie du patient, les obligations professionnelles, l'autodétermination concernant les données de santé et l'accès équitable aux soins de santé. Il entend permettre aux décideurs, aux prestataires de santé, aux professionnels de la santé et aux patients (y compris aux associations de patients) i) d'examiner comment les systèmes d'IA sont utilisés dans les soins de santé, au vu de leurs incidences sur les droits humains, et ii) de développer et de renforcer la relation thérapeutique, notamment en aidant les médecins et, le cas échéant, d'autres professionnels de la santé à promouvoir les droits consacrés dans la Convention d'Oviedo. Il traite de l'IA dans le domaine de la santé, notamment des applications utilisées par les professionnels de ce domaine et des applications utilisées par les patients eux-mêmes (applications prescrites par un médecin ou que le patient décide d'utiliser, comme les outils d'analyse des symptômes ou les logiciels de suivi des données de santé).

Lignes directrices sur la mise en œuvre responsable de systèmes d'intelligence artificielle dans le journalisme, Comité directeur sur les médias et la société de l'information (CDMSI), novembre 2023

Ces lignes directrices constituent une contribution importante à la promotion d'une sphère de communication publique fondée sur l'État de droit et respectueuse des droits humains. Elles fournissent des orientations pratiques aux destinataires concernés, en particulier les organisations des médias, mais aussi les États, les fournisseurs de technologies et les plateformes numériques qui diffusent des informations, en détaillant la manière dont les systèmes d'IA devraient être utilisés pour soutenir la production journalistique. Elles proposent certaines responsabilités pour les fournisseurs de technologie et les plateformes, ainsi que pour les États membres.

Étude sur l'impact des systèmes d'intelligence artificielle, leur potentiel de promotion de l'égalité, y compris l'égalité de genre, et les risques qu'ils peuvent entraîner en matière de non-discrimination, Commission pour l'égalité de genre (GEC) et Comité directeur sur l'anti-discrimination, la diversité et l'inclusion (CDADI), 2023

Cette étude sur l'impact des systèmes d'intelligence artificielle sur l'égalité, notamment l'égalité de genre, et la non-discrimination, enquête sur les risques de discrimination liés aux technologies algorithmiques, sur les réponses juridiques spécifiques à la discrimination algorithmique que peut proposer le Conseil de l'Europe, et sur le potentiel de ces technologies pour promouvoir l'égalité, y compris l'égalité de genre.

Les droits humains dès la conception de l'IA – une protection durable des droits humains à l'ère de l'intelligence artificielle, recommandation de la Commissaire aux droits de l'homme, mai 2023

Cette recommandation examine les principaux défis auxquels sont confrontés les États membres dans la protection et la promotion des droits humains dans le cadre de l'utilisation de l'IA. Elle encourage les États membres à évaluer les risques et les conséquences des systèmes d'IA pour les droits humains avant de les utiliser, à renforcer les garanties de transparence et à assurer un contrôle indépendant ainsi que l'accès à des recours effectifs. Elle rappelle le rôle crucial que jouent les structures nationales de protection des droits humains pour que les États membres protègent les droits humains lors de la conception, du développement et du déploiement des systèmes d'IA. Elle souligne également la nécessité de renforcer la supervision et le contrôle exercés par des institutions indépendantes, de

promouvoir la transparence des systèmes d'IA et la sensibilisation du public à leurs effets sur les droits humains, et d'explorer de manière proactive les possibilités que donne l'IA de renforcer la protection des droits humains plutôt que de l'affaiblir.

Rapport « Discours de haine et fausses informations : impact sur les conditions d'exercice des élus locaux et régionaux », Congrès des pouvoirs locaux et régionaux du Conseil de l'Europe, CG(2022)43-11final

Ce rapport explore le phénomène négatif, de plus en plus répandu, consistant à utiliser, en ligne et hors ligne, le discours de haine et les fausses informations, ainsi que les actes d'intimidation et les abus subis par les élus locaux et régionaux. Il analyse la manière dont le discours de haine, les fausses informations et les abus verbaux et physiques font partie du quotidien des élus locaux et régionaux et détaille les implications et les effets de ces pratiques sur les conditions d'exercice des élus. Il explique comment ces pratiques négatives abîment le tissu démocratique local et régional en créant un environnement politique toxique et intimidant. Enfin, ce rapport suggère une série de mesures à prendre par les autorités nationales, régionales et locales pour assurer la protection et le soutien des élus locaux et régionaux confrontés à ces phénomènes.

Justice par algorithme – Le rôle de l'intelligence artificielle dans les systèmes de police et de justice pénale, résolution 2342 (2020) de l'Assemblée parlementaire

L'Assemblée parlementaire du Conseil de l'Europe observe dans cette résolution qu'un nombre important d'applications de l'IA à l'usage des systèmes de police et de justice pénale sont utilisées dans les États membres du Conseil de l'Europe, ou que leur déploiement y est envisagé. Cette résolution fait référence en particulier aux applications permettant la reconnaissance faciale, la police prédictive, l'identification de victimes potentielles d'actes criminels, l'évaluation des risques en matière de détention provisoire, de peine prononcée et de libération conditionnelle, ou encore l'identification d'affaires non résolues qui pourraient l'être aujourd'hui grâce aux technologies modernes de criminalistique. L'Assemblée parlementaire y reconnaît que l'utilisation de l'IA dans les systèmes de police et de justice pénale présente des avantages importants lorsqu'elle est correctement réglementée et elle appelle les États membres à fonder toute réglementation future de l'IA sur des principes éthiques fondamentaux universellement admis et applicables : i) la transparence, y compris l'accessibilité et l'explicabilité, ii) la justice et l'équité, y compris la non-discrimination, iii) la prise de décision par une personne, qui en est responsable, et la mise à disposition de voies de recours, iv) la sûreté et la sécurité, et v) le respect de la vie privée et la protection des données. Elle appelle en outre les États membres à tenir un registre de toutes les applications d'IA utilisées dans le secteur public, à procéder à des évaluations d'impact transparentes des applications d'IA sur les droits de l'homme, initialement et périodiquement, à mettre en place des mécanismes de contrôle éthique efficaces et indépendants pour la mise en place et l'exploitation des systèmes d'IA, et à permettre un contrôle judiciaire.

Recommandation du Comité des Ministres aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme (CM/Rec(2020)1)

Les États membres doivent veiller à ce que toute conception, tout développement et tout déploiement en cours des systèmes algorithmiques s'effectuent dans le respect des droits de l'homme et des libertés fondamentales. Lorsque les systèmes algorithmiques sont susceptibles d'avoir un impact négatif sur les droits de l'homme d'un individu, d'un groupe particulier ou sur l'ensemble de la population, y compris sur les processus démocratiques ou l'état de droit, ces impacts engagent les obligations des États et les responsabilités du secteur privé vis-à-vis des droits humains.

Le Comité des Ministres recommande en particulier aux gouvernements des États membres : i) de revoir leurs cadres législatifs et leurs politiques, ainsi que leurs propres pratiques en matière d'acquisition, de conception, de développement et de déploiement en cours de systèmes algorithmiques, ii) de s'assurer, par le biais de cadres réglementaires et de contrôle appropriés relatifs aux systèmes algorithmiques, que les acteurs du secteur privé participant à la conception, au développement et au déploiement en cours de tels systèmes se conforment aux lois applicables et assument leurs responsabilités en matière de respect des droits de l'homme, iii) d'entreprendre des consultations, une coopération et un dialogue réguliers, inclusifs et transparents avec toutes les parties prenantes concernées, iv) de privilégier le renforcement de l'expertise des établissements publics et privés participant à l'intégration des systèmes algorithmiques dans de multiples aspects de la société, en vue de protéger efficacement les droits de l'homme, v) d'encourager la mise en œuvre de programmes d'éducation aux médias, à l'information et au numérique efficaces et adaptés, et vi) de tenir compte de l'impact environnemental du développement de services numériques à grande échelle.

Lignes directrices sur la reconnaissance faciale (T-PD(2020)03rev4)

Ces lignes directrices, adoptées par le Comité Consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel – Convention 108+ (T-PD), traitent de l'utilisation des technologies de reconnaissance faciale, y compris les technologies de reconnaissance faciale à la volée. Elles exposent que l'intégration de ces technologies dans les systèmes de surveillance existants fait courir des risques sérieux aux droits au respect de la vie privée et à la protection des données à caractère personnel, ainsi qu'à d'autres droits fondamentaux puisque leur utilisation n'impose pas toujours que les personnes dont les données biométriques sont ainsi traitées en soient informées ou y coopèrent. C'est le cas par exemple avec la possibilité d'accéder à des images numériques de personnes sur Internet. Ces lignes directrices disposent, afin de prévenir de telles atteintes, que les Parties à la Convention 108+ s'assureront que le développement et l'utilisation de la reconnaissance faciale respectent le droit à la vie privée et le droit à la protection des données personnelles, renforçant ainsi les droits de l'homme et les libertés fondamentales par la mise en œuvre des principes consacrés par la Convention 108+ dans le contexte particulier des technologies de reconnaissance faciale. Elles fournissent un ensemble de mesures de référence que les gouvernements, les développeurs en reconnaissance faciale, les fabricants, les prestataires de services et entités utilisatrices devraient suivre et appliquer pour garantir que cette technologie ne nuise pas à la dignité humaine, aux droits de l'homme et aux libertés fondamentales de toute personne, notamment au droit à la protection des données à caractère personnel.

Décoder l'intelligence artificielle : 10 mesures pour protéger les droits de l'homme, recommandation de la Commissaire aux droits de l'homme, mai 2019

Cette recommandation sur l'IA et les droits de l'homme donne des orientations pratiques sur la manière dont les effets négatifs des systèmes d'IA sur les droits de l'homme peuvent être évités ou atténués. Elle s'adresse aux États membres, mais les principes énoncés concernent quiconque a une

influence importante sur le développement, la mise en œuvre ou les effets d'un système d'IA : i) les États membres devraient établir un cadre juridique qui prévoie une procédure à suivre par les autorités publiques pour évaluer l'impact, sur les droits de l'homme, des systèmes d'IA, ii) l'utilisation des systèmes d'IA par les États devrait être régie par les normes relatives aux marchés publics, appliquées dans le cadre de procédures transparentes, auxquelles tous les acteurs concernés seraient invités à contribuer, iii) les États membres devraient faciliter la mise en œuvre effective des normes des droits de l'homme dans le secteur privé, iv) l'utilisation d'un système d'IA dans tout processus décisionnel ayant des effets concrets sur les droits des personnes doit être identifiable et transparente, v) les États membres devraient établir un cadre législatif qui permette de vérifier de manière indépendante et effective que le développement, le déploiement et l'utilisation des systèmes d'IA par les autorités publiques et les entités privées respectent les droits de l'homme, vi) il faut prévenir et atténuer les risques de discrimination en accordant une attention particulière aux groupes qui présentent un risque accru de voir leurs droits affectés par l'IA de manière disproportionnée, vii) le développement, l'apprentissage, la phase d'essai et l'utilisation de systèmes d'IA qui reposent sur le traitement de données à caractère personnel doivent garantir pleinement le droit des personnes au respect de la vie privée et familiale, viii) les États membres devraient tenir compte de l'ensemble des normes internationales relatives aux droits de l'homme qui peuvent être concernées par l'utilisation de l'IA, en veillant en particulier à la liberté d'expression, à la liberté de réunion et d'association et au droit au travail, ix) les États membres doivent établir des lignes de responsabilité claires en ce qui concerne les violations des droits de l'homme qui peuvent se produire à différentes phases du cycle de vie d'un système d'IA, et x) la connaissance et la compréhension de l'IA devraient être encouragées dans les institutions gouvernementales, les organes de contrôle indépendants, les structures nationales de protection des droits de l'homme, le système judiciaire et les services répressifs, ainsi qu'auprès du grand public.

Lignes directrices sur l'intelligence artificielle et la protection des données (T-PD(2019)01)

Ces lignes directrices, adoptées par le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, fournissent un ensemble de mesures de référence que les gouvernements, les développeurs en IA, les fabricants et les prestataires de services devraient appliquer pour éviter que les applications de l'IA ne nuisent à la dignité humaine, aux droits de l'Homme et aux libertés fondamentales de toute personne, notamment en ce qui concerne le droit à la protection des données à caractère personnel. Ces mesures sont les suivantes : i) la sauvegarde du droit à la protection des données à caractère personnel est essentielle au développement et à l'adoption d'applications reposant sur l'IA qui sont susceptibles de produire des effets sur les personnes et la société, ii) un développement de l'IA reposant sur le traitement de données à caractère personnel devrait être fondé sur les principes figurant dans la Convention 108+, iii) une approche centrée sur la prévention et la réduction des risques potentiels dus au traitement des données personnelles est un élément nécessaire à une innovation responsable dans le domaine de l'IA, iv) une vision plus large des éventuelles conséquences du traitement des données devrait être adoptée, v) les applications de l'IA doivent, à tout moment, pleinement respecter les droits des personnes concernées, et vi) les applications de l'IA devraient permettre aux personnes concernées d'exercer un contrôle significatif sur le traitement des données et leurs effets connexes tant au niveau individuel que sur la société.

Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement (CEPEJ(2018)14)

Adoptée en décembre 2018 par la Commission européenne pour l'efficacité de la justice (CEPEJ) du Conseil de l'Europe, cette Charte a été le premier texte européen à exposer des principes éthiques relatifs à l'utilisation de l'IA dans les systèmes judiciaires. Elle fournit un cadre composé de cinq

principes destinés à guider les acteurs publics et privés en charge de la conception et du déploiement d'outils et de services d'intelligence artificielle s'appuyant notamment sur le traitement des décisions juridictionnelles et des données judiciaires. Il s'agit i) du principe de respect des droits fondamentaux, qui requiert d'assurer une conception et une mise en œuvre des outils et des services d'intelligence artificielle qui soient compatibles avec les droits fondamentaux, ii) du principe de non-discrimination, qui requiert de prévenir spécifiquement la création ou le renforcement de discriminations entre individus ou groupes d'individus, iii) du principe de qualité et sécurité, qui requiert d'utiliser des sources certifiées et des données intangibles avec des modèles conçus d'une manière multidisciplinaire, dans un environnement technologique sécurisé, iv) du principe de transparence, de neutralité et d'intégrité intellectuelle, qui requiert de rendre accessibles et compréhensibles les méthodologies de traitement des données et d'autoriser les audits externes, et v) du principe de maîtrise par l'utilisateur, qui requiert de bannir une approche prescriptive et de permettre à l'usager d'être un acteur éclairé et maître de ses choix. Le CEPEJ collecte des informations sur les systèmes d'IA et d'autres outils avancés de cyberjustice appliqués dans la transformation numérique du système judiciaire (Centre de ressources sur la cyberjustice et l'IA – Commission européenne pour l'efficacité de la justice (CEPEJ) (coe.int)).

Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique (CM/Rec(2018)7)

Ces lignes directrices forment un ensemble de principes fondamentaux susceptibles d'aider les États à constituer le socle indispensable à la poursuite de l'intérêt supérieur de l'enfant dans le monde de l'environnement numérique. Elles leur recommandent en particulier : i) de réexaminer leur législation, leurs politiques et leurs pratiques, ii) de veiller à ce que cette recommandation soit traduite et diffusée aussi largement que possible auprès des autorités et des parties prenantes compétentes, iii) d'exiger des entreprises commerciales qu'elles assument leurs responsabilités au regard du respect des droits de l'enfant dans l'environnement numérique et qu'elles prennent des mesures de mise en œuvre, et de les encourager à coopérer avec les parties prenantes étatiques concernées, les organisations de la société civile et les enfants, iv) de coopérer avec le Conseil de l'Europe en vue de l'élaboration, de la mise en œuvre et du suivi de stratégies et de programmes visant à assurer le respect, la protection et la réalisation des droits de l'enfant dans l'environnement numérique, et v) d'examiner au plus tard tous les cinq ans la mise en œuvre de cette recommandation. En 2020, le Conseil de l'Europe a publié un Manuel pour les décideurs politiques sur les droits de l'enfant dans l'environnement numérique pour appuyer la mise en œuvre de cette recommandation.

2. Autres textes internationaux

Règlement sur l'intelligence artificielle, UE, 2024

Le règlement sur l'intelligence artificielle (règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828) a été formellement adopté par le Conseil européen le 21 mai 2024 et publié au Journal officiel de l'Union européenne le 12 juillet 2024. Il propose une classification des systèmes d'IA fondée sur les risques : i) les systèmes présentant des risques inacceptables, soit les systèmes d'IA qui représentent une menace considérable pour la sécurité et les droits fondamentaux (par exemple les systèmes de catégorisation biométrique, les systèmes permettant la notation sociale, les systèmes destinés à l'évaluation du risque qu'une personne commette des infractions pénales, les systèmes qui développent des bases de données de reconnaissance faciale ou les systèmes qui ont recours à des techniques de manipulation) et qui sont interdits pour cette raison, ii) les systèmes d'IA à haut risque,

qui sont strictement réglementés, iii) les systèmes d'IA à risque limité, qui sont soumis à des obligations de transparence plus légères, notamment celle de s'assurer que les utilisateurs finaux sont conscients qu'ils interagissent avec l'IA (chatbots et deepfakes par exemple), et iv) les systèmes à risque minimal, qui comprennent la majorité des applications d'IA actuellement disponibles sur le marché unique de l'UE (jeux vidéo et filtres anti-spam activés par l'IA par exemple) et qui ne sont pas réglementés.

Recommandation du Conseil sur l'intelligence artificielle, OCDE, adoptée en 2019 et amendée en 2024

Cette Recommandation vise à stimuler l'innovation et à renforcer la confiance dans l'IA en promouvant une approche responsable au service d'une IA digne de confiance, tout en garantissant le respect des droits humains et des valeurs démocratiques. Elle traite des questions de fond propres à l'IA et a vocation à définir une norme susceptible d'être mise en œuvre et suffisamment souple pour résister à l'épreuve du temps, dans un domaine en rapide mutation. Cette recommandation cherche également à établir une compréhension commune des expressions clés utilisées dans ses dispositions, telles que « système d'IA », « cycle de vie d'un système d'IA » et « acteurs de l'IA ». Elle expose les principes suivants, soulignant qu'ils sont complémentaires et devraient être considérés comme un tout : i) croissance inclusive, développement durable et bien-être, ii) respect de l'état de droit, des droits humains et des valeurs démocratiques, y compris de l'équité et de la vie privée, iii) transparence et explicabilité, iv) robustesse, sûreté et sécurité, et v) responsabilité. Le Conseil y formule également les recommandations suivantes aux fins de la coopération internationale : i) investir dans la recherche et le développement en matière d'IA, ii) favoriser l'instauration d'un écosystème inclusif propice à l'IA, iii) façonner un cadre d'action et de gouvernance interopérable favorable à l'IA, iv) renforcer les capacités humaines et préparer la transformation du marché du travail, et v) favoriser la coopération internationale au service d'une IA digne de confiance.

Recommandation sur l'éthique de l'intelligence artificielle, UNESCO, 2021

Cette Recommandation a pour objet de servir de base afin de mettre les systèmes d'IA au service de l'humanité, des individus, des sociétés, de l'environnement et des écosystèmes, ainsi que de prévenir les préjudices. Elle a également pour vocation de favoriser l'utilisation pacifique des systèmes d'IA. Elle énonce un ensemble de valeurs et de principes qui doivent être respectés par tous les acteurs du cycle de vie des systèmes d'IA et être appuyés par un cadre législatif. Les valeurs mises en avant dans cette recommandation sont les suivantes : i) respect, protection et promotion des droits de l'homme, des libertés fondamentales et de la dignité humaine, ii) un environnement et des écosystèmes qui prospèrent, iii) assurer la diversité et l'inclusion, et iv) vivre dans des sociétés pacifiques, justes et interdépendantes. Les principes énoncés sont les suivants : i) proportionnalité et innocuité, ii) sûreté et sécurité, iii) équité et non-discrimination, iv) durabilité, v) droit au respect de la vie privée et protection des données, vi) surveillance et décision humaines, vii) transparence et explicabilité, viii) responsabilité et redevabilité, ix) sensibilisation et éducation, et x) gouvernance et collaboration multipartites et adaptatives.

II. La jurisprudence de la Cour européenne des droits de l'homme à l'ère de l'intelligence artificielle

« Compte tenu du rythme élevé auquel se succèdent les innovations dans le domaine de la génétique et des technologies de l'information, la Cour ne peut écarter la possibilité que les aspects de la vie privée se rattachant aux informations génétiques fassent à l'avenir l'objet d'atteintes par des voies nouvelles, que l'on ne peut prévoir aujourd'hui avec précision » (*S. et Marper c. Royaume-Uni* [GC], 2008, § 71)

La Cour n'a pas encore eu l'occasion de se pencher sur un nombre significatif d'affaires touchant aux effets de l'IA sur la protection des droits et libertés consacrés par la Convention, ou de mesurer toute la complexité et les nuances des questions liées à l'IA. La jurisprudence constante de la Cour peut toutefois servir de point de départ lorsqu'il s'agit de rechercher si et comment les principes élaborés jusqu'à présent sont transposables et applicables aux affaires dans lesquelles l'utilisation de systèmes d'IA soulève des problématiques relatives aux droits de l'homme.

La jurisprudence présentée dans ce document de travail reflète les principes développés à ce jour par la Cour et n'a pas vocation à préjuger de la manière dont la Cour tranchera les affaires dont elle pourra être saisie et qui soulèveront des questions relatives à l'IA. La Cour statuera sur ces affaires à venir en se fondant sur leurs circonstances factuelles propres, à la lumière de la législation interne pertinente et de la pratique en vigueur dans l'État membre concerné, ainsi qu'au regard des normes européennes pertinentes telles qu'elles se présenteront au moment où elle examinera l'affaire (*Zavodnik c. Slovénie*, 2015, § 74).

A. Liberté d'expression (article 10 de la Convention)

1. Nouvelles technologies

Indissociable de la démocratie, la liberté d'expression est consacrée par un certain nombre d'instruments nationaux, européens, internationaux ou régionaux qui promeuvent ce système politique reconnu comme étant le seul à même de garantir la protection des droits de l'homme. Appelée à interpréter l'article 10 de la Convention, la Cour a déclaré que « la liberté d'expression constitue l'un des fondements [d'une société démocratique], l'une des conditions primordiales de son progrès et de l'épanouissement de chacun ». Avec l'avènement des nouvelles technologies, la Cour a reconnu que les sites Internet contribuent grandement à améliorer l'accès du public à l'actualité et à faciliter la communication de l'information, et elle a observé que la possibilité pour les individus de s'exprimer sur Internet constitue un outil sans précédent de la liberté d'expression.

Dans l'affaire *Times Newspapers Ltd c. Royaume-Uni (nos 1 et 2)*, 2009, la société requérante, qui était propriétaire et éditrice du quotidien *The Times*, alléguait que la règle de droit britannique voulant que chaque consultation d'informations diffamatoires publiées sur Internet puisse donner lieu à une action en diffamation portait atteinte de manière injustifiée et disproportionnée à sa liberté d'expression. Le journal de la requérante avait publié deux articles qui étaient prétendument diffamatoires à l'égard d'un particulier. Les deux articles en question avaient également été mis en ligne sur le site Internet du *Times*. Dans le cadre de la procédure en diffamation qui avait suivi, la société requérante avait été contrainte d'insérer dans ces deux articles archivés sur son site Internet un avertissement relatif à la procédure en cours. La Cour a observé que les sites Internet contribuent grandement à améliorer l'accès du public à l'actualité et, de manière générale, à faciliter la communication de l'information, et que la constitution d'archives sur Internet représente un aspect essentiel de ce rôle. Elle a dès lors considéré que la constitution d'archives sur Internet relève du champ d'application de l'article 10 (§ 27). Sur le fond de l'affaire, la Cour a conclu à une non-violation

de l'article 10 au motif que la condamnation de la société requérante par les juridictions internes avait constitué une restriction justifiée et proportionnée à la liberté d'expression de l'intéressée.

Dans l'affaire *Ahmet Yıldırım c. Turquie*, 2012, le requérant était propriétaire et utilisateur d'un site web sur lequel il publiait ses travaux académiques et ses points de vue dans différents domaines. Ce site avait été créé grâce au service « Google Sites », un module Google de création et d'hébergement de sites web. Dans le cadre d'une procédure pénale distincte, une mesure provisoire, ordonnant le blocage d'un site Internet au contenu jugé offensant, fut adoptée. Pendant l'exécution de cette mesure, l'accès à Google Sites fut totalement bloqué. Le requérant se trouva ainsi dans l'impossibilité d'accéder à son propre site web, et ses tentatives à cette fin se heurtèrent invariablement à la décision de blocage prononcée par le tribunal. Dans ce contexte, la Cour a affirmé qu'un blocage d'accès à Internet pouvait heurter de front le libellé même de l'article 10 de la Convention, en vertu duquel les droits reconnus dans cet article valent « sans considération de frontière » (§ 67). Au sujet de la justification des mesures de blocage, la Cour a dit que pareilles restrictions devaient s'inscrire dans un cadre légal particulièrement strict quant à la délimitation de l'interdiction et efficace quant au contrôle juridictionnel contre les éventuels abus (§ 64). Elle a conclu à une violation de l'article 10.

Dans l'affaire *Delfi AS c. Estonie* [GC], 2015, la société requérante, qui était propriétaire d'un portail d'actualités sur Internet exploité à des fins commerciales, se plaignait d'avoir été jugée responsable, par les juridictions internes, pour les commentaires diffamatoires qui avaient été déposés par les lecteurs en réaction à un article publié sur le portail d'actualités. La société requérante avait retiré les commentaires offensants environ six semaines après leur mise en ligne sur le site. La Cour, ayant examiné les griefs portés devant elle sous l'angle de l'article 10 de la Convention, a admis, tout en reconnaissant les avantages d'Internet, que ceux-ci s'accompagnent d'un certain nombre de risques dans la mesure où des propos clairement illicites, notamment des propos diffamatoires, haineux ou appelant à la violence, peuvent être diffusés comme jamais auparavant dans le monde entier, en quelques secondes, et parfois demeurer en ligne pendant fort longtemps (§ 110). Elle a également dit que les communications en ligne et leur contenu risquent bien plus que la presse de porter atteinte à l'exercice et à la jouissance des droits et libertés fondamentaux, en particulier du droit au respect de la vie privée (§ 133). Appliquant ces principes au cas d'espèce, la Cour a conclu à une non-violation de l'article 10, estimant que la sanction qui avait été imposée à la requérante dans les circonstances concrètes de l'affaire reposait sur des motifs pertinents et suffisants et qu'elle ne constituait pas une restriction disproportionnée du droit de la société requérante à la liberté d'expression (voir la section « Journalisme responsable en ligne » ci-dessous).

2. Utilisation de données à caractère personnel et de technologies de reconnaissance faciale pour l'identification de personnes exerçant leur liberté d'expression

Dans l'affaire *Catt c. Royaume-Uni*, 2019, le requérant, un manifestant pacifique, se plaignait de la conservation de ses données à caractère personnel dans une base de données de la police relative à l'extrémisme national pendant au moins six ans, soit le délai applicable avant un réexamen programmé (§ 120). La Cour a estimé que le requérant était entièrement tributaire de la diligence avec laquelle les autorités appliqueraient les garanties du code de pratique en vigueur, très souples par nature, pour veiller au caractère proportionné de la durée de conservation de ses données. Elle a souligné que l'absence de garanties qui auraient permis de supprimer les données dès que la durée de leur conservation serait devenue disproportionnée était particulièrement préoccupante lorsque des données révélant des opinions politiques, qui bénéficient d'un niveau de protection accru, étaient conservées sans limitation de durée (§§ 122-123). Elle a ainsi conclu à une violation de l'article 8.

L'affaire *Glukhin c. Russie*, 2023, portait sur l'utilisation par la police d'une technologie de reconnaissance faciale en vue d'identifier un participant à une manifestation pacifique. Le requérant s'était livré à une manifestation individuelle pacifique sans la déclarer préalablement. La police l'identifia à partir des photographies et de la vidéo publiées sur les réseaux sociaux, puis le repéra et l'arrêta alors qu'il effectuait un trajet en métro (§ 86). La Cour a estimé que la surveillance des faits ou

gestes d'un individu dans un lieu public au moyen de mécanismes de surveillance peut tomber sous le coup de l'article 8 dès lors que les données à caractère personnel ainsi collectées sont enregistrées de manière systématique ou permanente (§ 66). Elle a également précisé que les données à caractère personnel qui révèlent une opinion politique appellent un niveau de protection accru (§§ 76 et 86). Dans le contexte de la mise en place de technologies de reconnaissance faciale, elle a dit qu'il est essentiel que soient établies des règles détaillées régissant la portée et l'application des mesures qui en découlent, ainsi que des garanties solides contre les risques d'abus et d'arbitraire. Elle a ajouté que la nécessité de garanties est d'autant plus forte lorsqu'il est question du recours à une technologie de reconnaissance faciale à la volée (§ 82). La Cour a conclu, eu égard aux circonstances de l'affaire, à une violation de l'article 8.

3. Sécurité sur Internet et droit à l'oubli numérique

La notion de « droit à l'oubli » est apparue récemment dans la jurisprudence de la Cour et elle est toujours en cours d'élaboration. Malgré sa nouveauté, son application en pratique présente déjà beaucoup de particularités. De manière générale, le « droit à l'oubli » peut donner lieu en pratique à différentes mesures qui peuvent être prises par les exploitants de moteurs de recherche ou par les éditeurs de presse. Ces mesures visent soit le contenu même d'un article archivé, comme, par exemple, la suppression, la modification ou l'anonymisation d'un article, soit la limitation de l'accessibilité de l'information.

Dans l'affaire *Biancardi c. Italie*, 2021, la Cour s'est penchée sur la question de la désindexation d'informations sensibles publiées sur Internet. Le requérant, ancien rédacteur en chef d'un journal en ligne, avait été condamné au civil pour avoir conservé sur le site Internet de son journal un article relatant une bagarre dans un restaurant qui donnait des détails sur la procédure pénale ouverte à ce sujet. Les juridictions internes avaient relevé en particulier que le requérant n'avait pas désindexé les balises permettant d'accéder à l'article, de sorte que toute personne saisissant dans un moteur de recherche en ligne le nom du restaurant ou de son propriétaire pouvait accéder à des informations sensibles concernant la procédure pénale, et ce malgré la demande de retrait de l'article formulée par le propriétaire du restaurant (§§ 67-71). L'anonymat des protagonistes dans l'article en ligne n'était pas en cause dans cette affaire. La Cour a noté que l'obligation de désindexer un contenu pouvait être imposée non seulement aux fournisseurs de moteurs de recherche sur Internet, mais aussi aux administrateurs de journaux ou d'archives de presse accessibles par Internet, par exemple au requérant. Elle a estimé que le fait que des données sensibles concernant la procédure pénale ouverte contre le propriétaire du restaurant fussent restées en ligne et aisément accessibles de manière prolongée (pendant huit mois après que les personnes concernées en eurent formellement demandé le retrait) avait porté atteinte au droit du restaurateur au respect de sa réputation (§ 70). Elle a ainsi jugé que la restriction de la liberté d'expression que constituait la sanction imposée au requérant était justifiable, et elle a conclu à une non-violation de l'article 10.

Dans l'affaire *Hurbain c. Belgique* [GC], 2023, un éditeur de presse avait été condamné par les juridictions internes à anonymiser, au nom du « droit à l'oubli », une version archivée en ligne d'un article mentionnant le nom complet d'un conducteur qui avait été responsable d'un accident de la route mortel survenu de nombreuses années auparavant. La Cour s'est penchée sur la notion de « droit à l'oubli » et elle a circonscrit, au regard de la Convention, la portée des prétentions tirées de ce « droit » (§ 187). Elle a noté qu'avec le développement de la technologie et des outils de communication, un nombre croissant de personnes cherchaient à faire protéger les intérêts qu'elles tiraient de ce que l'on appelle communément le « droit à l'oubli », lequel repose sur l'intérêt d'une personne à faire effacer, modifier ou limiter l'accès à des informations passées qui affectent la perception actuelle de cette personne. Elle a précisé qu'en cherchant à faire disparaître ces informations, les intéressés voulaient éviter de se faire reprocher indéfiniment leurs actes ou leurs déclarations publiques antérieures et cela dans des contextes variables, tels que, par exemple, l'embauche ou les relations d'affaires (§§ 191-199). Elle a donc établi que son rôle consistait à arbitrer

un conflit, dans le contexte d'une publication en ligne, entre les droits du requérant tels que garantis par l'article 10 et ceux de l'automobiliste tels que garantis par l'article 8 de la Convention (§ 202). Elle a réexaminé sa jurisprudence existante et ajusté les critères à appliquer pour la mise en balance des droits découlant respectivement des articles 8 et 10 dans le contexte du maintien à disposition d'une version archivée électronique d'un article divulguant des données à caractère personnel concernant un individu (§§ 205-211). Elle a également rappelé que les communications en ligne et leur contenu risquent bien plus que la presse de porter atteinte à l'exercice et à la jouissance des droits et libertés fondamentaux, en particulier du droit au respect de la vie privée, et ce notamment en raison du rôle important que jouent les moteurs de recherche (§ 236). Appliquant ces critères aux circonstances de l'affaire portée devant elle, la Cour a estimé que les juridictions nationales avaient soigneusement réalisé une mise en balance des droits en présence conformément aux exigences de la Convention, et que l'ingérence dans l'exercice des droits du requérant tels que garantis par l'article 10 avait été réduite au strict nécessaire et qu'elle pouvait dès lors passer pour nécessaire dans une société démocratique et proportionnée. Elle a ainsi conclu à une non-violation de l'article 10.

4. Journalisme responsable en ligne

La protection accrue offerte aux « chiens de garde publics » et notamment à la presse par l'article 10 est subordonnée au respect des devoirs et responsabilités liés à la fonction de journaliste, et à l'obligation corollaire de pratiquer un « journalisme responsable ». La notion de « journalisme responsable » renvoie tant au contenu des publications qu'au comportement des journalistes, lesquels sont tenus de se conformer au droit pénal, et ce même quand il s'agit de rendre compte dans la presse de questions sérieuses d'intérêt général (*Pentikäinen c. Finlande* [GC], 2015, §§ 90-91).

Dans l'affaire *Times Newspapers Ltd c. Royaume-Uni (n^{os} 1 et 2)*, 2009 (voir la section « Nouvelles technologies » ci-dessus), la Cour a estimé que lorsqu'un journal a été informé de l'introduction d'une action en diffamation au sujet d'un article publié dans la presse écrite, l'insertion obligatoire d'un avertissement adéquat visant l'article en question dans les archives Internet où il figure ne saurait passer pour une ingérence disproportionnée dans la liberté d'expression (§ 47). Elle a affirmé que le devoir de la presse de se conformer aux principes d'un journalisme responsable en vérifiant l'exactitude des informations publiées est vraisemblablement plus rigoureux en ce qui concerne celles qui ont trait au passé – et dont la diffusion ne revêt aucun caractère d'urgence – qu'en ce qui concerne l'actualité, par nature périssable (§ 45). Elle a conclu à une non-violation de l'article 10.

Dans l'affaire *Delfi AS c. Estonie* [GC], 2015 (voir la section « Nouvelles technologies » ci-dessus), la Cour a pour la première fois été appelée à examiner un grief concernant la responsabilité éventuelle d'un portail d'actualités sur Internet pour des commentaires déposés par les internautes. Elle a dit qu'en raison de la nature particulière d'Internet, les « devoirs et responsabilités » que doit assumer un portail d'actualités sur Internet aux fins de l'article 10 peuvent dans une certaine mesure différer de ceux d'un éditeur traditionnel en ce qui concerne le contenu fourni par des tiers (§ 113). En l'espèce, elle a conclu à une non-violation de l'article 10 de la Convention, estimant que la décision des juridictions internes de tenir la société requérante pour responsable était justifiée et ne constituait pas une restriction disproportionnée du droit de l'intéressée à la liberté d'expression ; elle a considéré en particulier que les commentaires en cause présentaient un caractère extrême et qu'ils avaient été déposés en réaction à un article publié par la société requérante sur un portail d'actualités qu'elle exploitait à titre professionnel dans le cadre d'une activité commerciale, que les mesures prises par la requérante pour retirer sans délai les commentaires diffamatoires après leur publication avaient été insuffisantes, et que l'amende d'un montant de 320 € qui avait été infligée à la requérante, l'un des plus grands portails d'actualités sur Internet d'Estonie, n'était en rien excessive.

Dans l'affaire *Magyar Tartalomszolgáltatók Egyesülete et Index.hu Zrt c. Hongrie*, 2016, un organe d'autorégulation des prestataires de services de contenu sur Internet et un portail d'actualités sur Internet avaient été jugés responsables pour des commentaires grossiers et injurieux laissés par des internautes sur leurs sites web à la suite de la publication d'un avis qualifiant de trompeuses les

pratiques commerciales de deux sites web d'annonces immobilières. Les requérants se plaignaient des décisions rendues contre eux par les juridictions internes, lesquelles les avaient en effet contraints à modérer la teneur des commentaires laissés par leurs lecteurs sur leurs sites Internet, ce qui, selon eux, allait à l'encontre de l'essence même de la liberté d'expression sur Internet. La Cour a rappelé que si « en raison de la nature particulière d'Internet, les « devoirs et responsabilités » que doit assumer un portail d'actualités sur Internet aux fins de l'article 10 peuvent dans une certaine mesure différer de ceux d'un éditeur traditionnel en ce qui concerne le contenu fourni par des tiers », le fait de fournir une plateforme pour l'exercice de la liberté d'expression en permettant au public de partager des informations et des idées sur Internet doit être examiné à la lumière des principes applicables à la presse (§§ 61-62). Elle a toutefois considéré que lorsque les juridictions internes avaient tranché la question de la responsabilité des requérants, elles n'avaient pas dûment mis en balance les droits divergents en cause, à savoir d'une part celui des requérants à la liberté d'expression et d'autre part celui des sites d'annonces immobilières au respect de leur réputation commerciale. Elle a notamment souligné que les autorités internes avaient accepté telles quelles les allégations selon lesquelles les commentaires litigieux étaient illicites en ce qu'ils auraient porté atteinte à la réputation des sites web d'annonces immobilières concernés. La Cour a ainsi conclu à une violation de l'article 10 de la Convention.

Dans l'affaire *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande* [GC], 2017, des données de nature fiscale visant 1,2 million de personnes physiques avaient été publiées dans un magazine et diffusées ultérieurement au moyen d'un service de SMS. La Cour a estimé que l'existence d'un intérêt général à ce que de grandes quantités de données fiscales soient accessibles et puissent être collectées à des fins journalistiques ne signifie pas nécessairement ou automatiquement qu'il existe également un intérêt général à diffuser en masse pareilles données brutes, telles quelles, sans aucun apport analytique. Elle a précisé qu'une distinction doit être faite entre le traitement de données à des fins de journalisme et la diffusion des données brutes auxquelles les journalistes ont accès dans des conditions privilégiées (§ 175). Dans ce contexte, le fait d'empêcher que des données à caractère personnel de nature fiscale soient diffusées en masse, selon des modalités contraires à la règlementation nationale et aux règles de l'Union européenne sur la protection des données, n'était pas, en soi, une sanction, même si les limitations imposées quant à la quantité de données à publier avaient pu, en pratique, rendre les activités commerciales des sociétés requérantes moins lucratives (§ 197).

Dans l'affaire *Magyar Jeti Zrt c. Hongrie*, 2018, la responsabilité objective de la société requérante avait été engagée pour la publication d'un hyperlien vers une interview sur YouTube, dont il avait été ultérieurement jugé qu'elle renfermait un contenu diffamatoire. La société requérante soutenait que les juridictions internes avaient restreint indûment ses droits lorsqu'elles avaient jugé que la publication de cet hyperlien sur son site web engageait sa responsabilité. La Cour a souligné en particulier l'importance des hyperliens pour le bon fonctionnement d'Internet et elle a précisé qu'en tant que technique de compte rendu, les hyperliens étaient fondamentalement différents des modes de publication traditionnels. Elle a répété que le but même des hyperliens est de permettre aux internautes, en les renvoyant à d'autres pages et ressources en ligne, de naviguer d'un contenu à l'autre sur un réseau qui se caractérise par la disponibilité d'une immense quantité d'informations. Elle a ainsi estimé qu'en reliant les contenus les uns aux autres, sans toutefois maîtriser le contenu du site web auquel ils donnaient accès, les hyperliens rendaient les informations accessibles et contribuent ainsi au bon fonctionnement d'Internet (§§ 73-75). Elle a énoncé les éléments dont il convient de tenir compte, au regard de l'article 10, dans l'examen de la question de savoir s'il peut être justifié d'imputer une responsabilité à l'auteur d'un hyperlien, et elle a précisé que cette question doit faire l'objet d'un examen au cas par cas (§§ 76-77). En l'espèce, la Cour a conclu que le droit interne relatif à la responsabilité objective (stricte) pour la diffusion d'informations diffamatoires excluait toute appréciation sérieuse du respect du droit de la société requérante à la liberté d'expression, dans une situation qui appelait un contrôle minutieux par les juridictions internes. Elle a ajouté que l'imputation de cette responsabilité objective pour l'utilisation d'un hyperlien pouvait

nuire à la libre circulation des informations sur Internet, en dissuadant aussi bien ceux qui écrivent des articles que ceux qui les publient de mettre en ligne des hyperliens menant à des sites dont ils ne contrôlent pas le contenu. Elle a estimé que pareille décision était de nature à avoir un effet inhibiteur sur la liberté d'expression sur Internet (§ 83). Elle a donc considéré que, dans l'ensemble, la société requérante s'était vu imposer une restriction injustifiée de ses droits, et elle a conclu à une violation de l'article 10.

Dans l'affaire *Sanchez c. France* [GC], 2023, qui portait sur la condamnation pénale d'un homme politique pour des propos xénophobes qui avaient été postés par des tiers sur le mur de son compte Facebook personnel en période de campagne électorale, la Cour s'est penchée pour la première fois sur la question de la responsabilité des utilisateurs de réseaux sociaux à raison de commentaires postés par des tiers. La Cour a souligné en particulier que le mur Facebook du requérant ne pouvait être assimilé à un « grand portail d'actualités sur Internet exploité à titre professionnel et à des fins commerciales » ; elle a plutôt abordé cette question au regard des « devoirs et responsabilités » qui incombent aux personnalités politiques lorsqu'elles décident d'utiliser les réseaux sociaux à des fins politiques, notamment à des fins électorales, en ouvrant des forums accessibles au public sur Internet afin de recueillir leurs réactions et leurs commentaires (§ 180). Elle a fait observer dans ce contexte que le titulaire d'un compte ne pouvait revendiquer un quelconque droit à l'impunité dans l'utilisation qu'il faisait des outils numériques mis à sa disposition sur Internet et qu'il lui appartenait d'agir dans les limites de ce que l'on pouvait raisonnablement attendre de lui (§ 190). Elle a précisé sur ce dernier point que la notoriété de la personne concernée constituait un facteur pertinent : un simple particulier dont la notoriété et la représentativité sont limitées aura moins d'obligations qu'une personne ayant un mandat d'élu local et candidate à de telles fonctions, laquelle aura à son tour moins d'impératifs qu'une personnalité politique d'envergure nationale, pour qui les exigences seront nécessairement plus importantes, en raison tant du poids et de la portée de ses paroles que de sa capacité à accéder aux ressources adaptées, permettant d'intervenir efficacement sur les plateformes de médias sociaux (§ 201).

La Cour a ainsi relevé que le requérant avait utilisé son compte Facebook en sa qualité de personnalité politique et à des fins politiques, en plein contexte électoral dans lequel s'inscrivaient les commentaires litigieux (§ 189), et qu'il avait en outre toute latitude pour décider de rendre l'accès au mur de son compte Facebook public ou non. Elle a estimé que si la décision qu'il avait prise à ce titre ne pouvait, en soi, lui être reprochée, une telle option était, compte tenu du contexte local et électoral tendu qui existait à l'époque des faits, manifestement lourde de conséquences, ce que le requérant ne pouvait ignorer dans les circonstances de l'espèce (§ 193). Constatant que le requérant n'avait pas appliqué, en temps voulu, de mesures pour examiner les commentaires déjà publiés et retirer ceux qui étaient de nature clairement illicite, et que les juridictions internes avaient rendu des décisions motivées et s'étaient livrées à une appréciation raisonnable des faits (§ 199), la Cour a conclu à une non-violation de l'article 10 (§§ 209-210).

5. Transferts de données et protection des sources journalistiques

Compte tenu de l'importance vitale pour la liberté de la presse que revêt la protection des sources des journalistes et des informations susceptibles de conduire à leur identification, toute atteinte au droit à la protection de pareilles sources doit être entourée de garanties procédurales, définies par la loi, en rapport avec l'importance du principe en jeu. La Cour a également rappelé cette conclusion dans des affaires relatives aux sources en ligne et à l'interception en masse de communications.

Dans l'affaire *Comité de rédaction de Pravoye Delo et Shtekel c. Ukraine*, 2011, les requérants (le comité de rédaction et le rédacteur en chef d'un journal) avaient été jugés solidairement responsables pour le téléchargement depuis un site d'informations en ligne d'une lettre anonyme dont l'auteur présumé était un employé des services de sécurité ukrainiens et pour la publication de cette lettre. L'auteur de la lettre y alléguait que des hauts fonctionnaires du département des services de sécurité ukrainiens s'étaient livrés à la corruption et à d'autres activités délictueuses, et qu'ils entretenaient

des liens avec le crime organisé. Le journal avait cité la source de l'information et publié un commentaire rédigé par le comité de rédaction qui indiquait que les informations présentées dans la lettre pouvaient être inexactes et qui invitait les lecteurs à faire des commentaires. La Cour a rappelé que, compte tenu du rôle joué par Internet dans le cadre des activités professionnelles des médias et de son importance dans l'exercice du droit à la liberté d'expression en général, l'absence d'un cadre légal suffisant au niveau interne, permettant aux journalistes d'utiliser des informations tirées d'Internet sans crainte de s'exposer à des sanctions, entrave gravement l'exercice par la presse de sa fonction vitale de « chien de garde » (§ 64). Elle a donc conclu à une violation de l'article 10.

Dans l'affaire *Big Brother Watch et autres c. Royaume-Uni* [GC], 2021, qui portait sur l'interception en masse de communications, des services de renseignement avaient pu accéder à de gros volumes d'éléments journalistiques confidentiels de manière fortuite, en prenant accidentellement de tels éléments dans les « filets » d'une interception en masse. Les requérantes (des personnes physiques et morales) se plaignaient de la portée et de l'ampleur des programmes de surveillance électronique mis en œuvre par l'État, dont elles pensaient avoir probablement fait l'objet. La Cour a fait observer qu'à l'époque actuelle, où le numérique est de plus en plus présent, les capacités technologiques ont considérablement accru le volume des communications transitant par Internet au niveau mondial, si bien que la surveillance qui ne vise pas directement les individus est susceptible d'avoir une portée très large, tant à l'intérieur qu'à l'extérieur du territoire de l'État qui l'opère. Elle a estimé que, l'examen de communications journalistiques ou de données de communication associées par un analyste pouvant conduire à l'identification d'une source, le droit interne doit impérativement comporter des garanties solides en ce qui concerne la conservation, l'examen, l'utilisation, la transmission à des tiers et la destruction de ces éléments confidentiels. Elle a ajouté que lorsqu'il apparaît que des communications journalistiques ou des données de communication associées n'ayant pas été sélectionnées pour examen par l'utilisation délibérée d'un sélecteur ou d'un terme de recherche dont on sait qu'il est lié à un journaliste contiennent malgré tout des éléments journalistiques confidentiels, la prolongation de leur conservation et la poursuite de leur examen par un analyste ne devraient être possibles qu'à la condition d'être autorisées par un juge ou un autre organe décisionnel indépendant et impartial habilité à déterminer si ces mesures sont « justifiées par un impératif prépondérant d'intérêt public » (§ 450). La Cour a conclu d'une part à une violation des articles 8 et 10 à raison des régimes d'interception en masse et d'acquisition de données de communication, et d'autre part à une non-violation de ces deux dispositions à raison de la réception de renseignements obtenus auprès de services de renseignement étrangers.

6. Élections libres (article 3 du Protocole n° 1 à la Convention)

La Cour a souligné l'interdépendance entre le droit à des élections libres et la liberté d'expression. Des élections libres et la liberté d'expression, notamment la liberté du débat politique, constituent l'assise de tout régime démocratique. Les deux droits sont interdépendants et se renforcent l'un l'autre. Il est ainsi particulièrement important, en période préélectorale, de permettre aux opinions et aux informations de tous ordres de circuler librement ; pour autant, la nécessité d'un débat public libre et pluraliste ne se limite pas aux périodes électorales : elle existe en toutes circonstances.

Dans l'affaire *Parti communiste de Russie et autres c. Russie*, 2012, la Cour s'est penchée sur la question de savoir si l'État était tenu par une obligation positive, découlant pour lui de l'article 3 du Protocole n° 1, de faire en sorte que la couverture des élections par les médias réglementés soit objective et compatible avec l'esprit d'« élections libres », même en l'absence de preuve directe de manipulation délibérée. Elle a jugé que le système de recours en matière électorale existant en l'espèce était suffisant pour satisfaire à l'obligation positive de nature procédurale qui incombait à l'État. Quant à l'aspect matériel de l'obligation et à l'allégation selon laquelle l'État aurait dû veiller à la neutralité des médias audiovisuels, elle a estimé que des mesures avaient été prises pour garantir une certaine visibilité aux partis et aux candidats de l'opposition à la télévision et pour assurer l'indépendance éditoriale et la neutralité des médias. Ces dispositions n'avaient probablement pas

assuré une égalité de fait, mais la Cour n'a pas jugé établi que l'État avait manqué à ses obligations positives en la matière. Elle a ainsi conclu à une non-violation l'article 3 du Protocole n° 1.

En matière de publicité politique, dans l'affaire *Animal Defenders International c. Royaume-Uni* [GC], 2013, qui fait référence à l'arrêt *Bowman c. Royaume-Uni*, §§ 42-43, 1998, la Cour a rappelé que la nécessité d'un débat public libre et pluraliste ne se limite pas aux périodes électorales et qu'elle existe en toutes circonstances (§§ 106-111). Dans l'affaire *Animal Defenders International c. Royaume-Uni* [GC], 2013, la requérante, une organisation non gouvernementale, s'était vu refuser l'autorisation de diffuser à la télévision un message publicitaire dans le cadre d'une campagne sur le traitement réservé aux primates, au motif que, les objectifs de la requérante étant de nature politique, la diffusion de la publicité en question entrait dans le champ d'application de l'interdiction légale de la publicité politique. La Cour a estimé que les motifs avancés par les autorités pour justifier l'interdiction faite à la requérante de diffuser sa publicité étaient pertinents et suffisants, et que la mesure litigieuse ne pouvait donc s'analyser en une atteinte disproportionnée au droit de l'intéressée à la liberté d'expression. Elle a ainsi conclu à une non-violation de l'article 10. Dans l'affaire *Bowman c. Royaume-Uni*, 1998, la requérante avait fait l'objet de poursuites pénales pour des dépenses visant à diffuser du matériel électoral pendant la période qui précédait immédiatement le scrutin. La Cour a estimé que l'obstacle absolu ayant empêché l'intéressée de publier des informations visant à influencer des électeurs n'était pas nécessaire pour atteindre l'objectif légitime de garantir l'égalité entre les candidats (§ 47). Elle a ainsi conclu à une violation de l'article 10.

Dans l'affaire *Orlovskaya Iskra c. Russie*, 2017, l'organisation requérante s'était vu infliger une amende pour avoir publié dans son journal, au cours du mois ayant précédé des élections, des articles dont il fut jugé qu'ils relevaient de la campagne électorale sans être clairement désignés comme tels. La Cour a noté que les publications litigieuses s'inscrivaient dans l'exercice par la requérante de sa liberté de communiquer des informations ou des idées, et que le contenu de ces publications relevait de la couverture journalistique normale d'un débat politique dans la presse écrite ; elle a considéré que cela ne laissait guère de place pour des restrictions (§§ 115-116). La Cour a souligné que le rôle de « chien de garde public » de la presse ne perd pas de sa pertinence en période électorale, lorsque la presse est appelée à faciliter « la libre expression de l'opinion du peuple sur le choix du corps législatif » (§§ 129-131). Elle a ainsi conclu à une violation de l'article 10.

Dans l'affaire *Sanchez c. France* [GC], 2023 (voir la section « Journalisme responsable en ligne » ci-dessus), un homme politique avait été condamné pour des propos xénophobes qui avaient été postés par des tiers sur le mur de son compte Facebook personnel en période de campagne électorale. La Cour a rappelé qu' un simple particulier dont la notoriété et la représentativité sont limitées aura moins d'obligations qu'une personne ayant un mandat d'élu local et candidate à de telles fonctions, laquelle aura à son tour moins d'impératifs qu'une personnalité politique d'envergure nationale, pour qui les exigences seront nécessairement plus importantes, en raison tant du poids et de la portée de ses paroles que de sa capacité à accéder aux ressources adaptées, permettant d'intervenir efficacement sur les plateformes de médias sociaux (§ 201). Dans les circonstances de l'espèce, elle a conclu à une violation de l'article 10.

Dans l'affaire *Glukhin c. Russie*, 2023, (voir la section « Utilisation de données à caractère personnel et de technologies de reconnaissance faciale pour l'identification de personnes exerçant leur liberté d'expression » ci-dessus), le requérant avait été identifié au moyen d'une technologie de reconnaissance faciale après s'être livré à une manifestation individuelle. La Cour a rappelé dans ce contexte que les données à caractère personnel qui révèlent une opinion politique appellent un niveau de protection accru (§§ 76 et 86). Elle a conclu, eu égard aux circonstances de l'affaire, à une violation de l'article 8.

B. Droit à un procès équitable (article 6 de la Convention)

1. Accès à un tribunal

Se référant aux principes de la prééminence du droit et de l'interdiction de tout pouvoir arbitraire qui sous-tendent la Convention, la Cour a dit que le droit d'accès à un tribunal est un élément inhérent aux garanties consacrées par l'article 6, et qu'il n'est pas plus absolu en matière pénale qu'en matière civile. La Cour a examiné dans plusieurs affaires l'incidence des nouvelles technologies sur l'accès des particuliers à un tribunal.

Dans l'affaire *Farcaș et autres c. Roumanie* [Comité], 2018, les requérants étaient créanciers d'une société en faillite. Ils alléguaient ne pas avoir été en mesure de se tenir informés de la procédure judiciaire ou d'exercer leurs droits procéduraux au motif que les documents pertinents auraient été notifiés exclusivement par voie de publication (en version papier et en version électronique, §§ 15 et 20) dans le Bulletin des procédures de faillite, auquel ils disaient ne pas avoir accès. La Cour a noté que le tarif de la version papier du bulletin était prohibitif pour les requérants (§ 36), et que les intéressés, n'ayant pas accès à Internet (§ 39), n'avaient pas non plus pu consulter la version en ligne du bulletin. Elle a ainsi estimé qu'en l'absence d'un autre mode de notification, le droit pour les requérants d'accéder à un tribunal était devenu illusoire, et elle a conclu à une violation de l'article 6.

Dans l'affaire *Xavier Lucas c. France*, 2022, la Cour a dit que les technologies numériques (e-barreau/e-justice) pouvaient contribuer à une meilleure administration de la justice et être mises au service des droits garantis par l'article 6, et qu'elles poursuivaient donc un « but légitime » (§ 46). Elle a également estimé conforme à l'article 6 l'obligation de recourir à la présentation électronique/informatique d'un recours pour des procédures avec représentation obligatoire par avocat (§ 51). Cette affaire portait sur l'obligation de saisir la cour d'appel par voie électronique sur la plateforme e-barreau. La cour d'appel, relevant que le formulaire informatique ne permettait pas de saisir la nature de ce recours et la qualité des parties sous leurs dénominations juridiques exactes, déclara recevable le recours en annulation d'une sentence arbitrale que le requérant avait présenté sur papier. Cependant, la Cour de cassation parvint ensuite à la conclusion contraire, déclarant que le recours aurait dû être présenté par la voie électronique. La Cour a estimé que le requérant s'était vu imposer une charge disproportionnée qui rompait le juste équilibre entre, d'une part, le souci légitime d'assurer le respect des conditions formelles pour saisir les juridictions et d'autre part le droit d'accès au juge. À l'instar du requérant qui considérait qu'il était matériellement impossible de saisir le recours litigieux sur la plateforme e-barreau, la Cour a relevé, en particulier, que la remise par voie électronique de ce recours sur e-barreau supposait que l'avocat du requérant remplisse un formulaire en utilisant des notions juridiques impropres. Elle a également observé que le gouvernement français n'avait pas démontré que des informations précises relatives aux modalités d'introduction d'un tel recours se trouvaient à la disposition des utilisateurs. Elle a donc conclu qu'en faisant prévaloir le principe de l'obligation de communiquer par voie électronique pour saisir la cour d'appel sans prendre en compte les obstacles pratiques auxquels s'était heurté le requérant pour la respecter, la Cour de cassation avait fait preuve d'un formalisme que la garantie de la sécurité juridique et de la bonne administration de la justice n'imposait pas et qui devait, dès lors, être regardé comme excessif (§ 57). La Cour a ainsi estimé que ces circonstances avaient porté atteinte au droit pour le requérant d'accéder à un tribunal, et elle a conclu à une violation de l'article 6.

Dans l'affaire *Daugaard Sorensen c. Danemark*, 2024, la requérante avait signalé à la police qu'elle avait été violée. Les poursuites engagées contre l'auteur présumé des faits finirent par être abandonnées à cause d'erreurs commises par le procureur dans la notification de décisions relatives à l'affaire. La décision de deuxième instance aurait dû être notifiée à l'auteur présumé des faits par voie électronique sur le compte Digital Post (*e-Boks*) que l'intéressé était légalement tenu de posséder ; cette notification, qui était généralement une opération instantanée lorsqu'elle était faite en ligne, fut cependant effectuée au moyen d'une lettre recommandée qui ne parvint jamais à son

destinataire. Les délais de prescription expirèrent (§§ 12-16). La Cour a estimé qu'elle n'avait aucune raison de douter de l'efficacité du système en vigueur, et notamment du service de notification, mais que dans les circonstances de l'affaire, les erreurs procédurales commises par le parquet avaient privé la requérante de poursuites pénales ou d'un contrôle juridictionnel effectifs relativement à l'infraction de viol qu'elle avait dénoncée à la police (§§ 69-70). La Cour a conclu à un manquement aux obligations positives qui découlaient pour l'État défendeur des articles 3 et 8 de la Convention.

2. Audience contradictoire (communication des éléments de preuve) en matière pénale

L'égalité des armes est l'un des éléments inhérents à la notion de procès équitable. Elle veut que chaque partie se voie offrir une possibilité raisonnable de présenter sa cause dans des conditions qui ne la placent pas dans une situation de désavantage par rapport à son adversaire. Ce principe exige que soit ménagé un juste équilibre entre les parties et s'applique en matière tant civile que pénale. Un problème d'accès à des preuves peut surgir sur le terrain de l'article 6 sous son volet pénal dès lors que celles-ci sont pertinentes dans le procès du requérant, en particulier lorsqu'elles ont une incidence importante sur les charges retenues contre lui. En ce qui concerne la communication des preuves, des questions complexes peuvent naître lorsqu'il s'agit de la communication de données électroniques, lesquelles peuvent constituer une certaine masse d'informations pour l'accusation.

Dans l'affaire *Sigurður Einarsson et autres c. Islande*, 2019, les requérants, qui occupaient des postes élevés dans une banque qui fit faillite à la suite de la crise bancaire qui frappa l'Islande en 2008, furent poursuivis pour abus de confiance ou manipulation du marché, et furent déclarés coupables. Ils alléguaient que la défense n'avait pas eu accès aux volumineuses données recueillies par le parquet au stade de l'enquête et, notamment, qu'elle n'avait pas eu son mot à dire dans le tri électronique de ces données effectué par le parquet aux fins de la sélection des informations pertinentes à verser au dossier de l'enquête. Ils soutenaient que nul n'avait contrôlé la sélection par le parquet des documents à soumettre au tribunal et qu'on leur avait refusé l'accès à la compilation entière des données ainsi que la possibilité de faire une recherche dans ces données à l'aide du système électronique employé par le procureur (un système de recherche électronique appelé « Clearwell e-Discovery » ; §§ 16 et 63). La Cour a admis que par nature la « compilation entière des données » englobait forcément une masse de données *a priori* non pertinentes pour l'affaire, et que lorsque le parquet était en possession d'un grand volume de données non traitées, il pouvait être légitime qu'il passe les informations au crible afin de découvrir ce qui pourrait présenter un intérêt et, ainsi, de ramener le dossier à des proportions gérables. Elle a néanmoins considéré qu'une garantie importante dans le cadre d'un tel processus consistait en principe à assurer à la défense la possibilité de participer à l'établissement de critères permettant de déterminer ce qui était potentiellement pertinent (§ 90). Elle a également dit, en ce qui concerne les données identifiées ou balisées, que tout refus d'autoriser la défense à faire réaliser de nouvelles recherches parmi celles-ci soulevait en principe une question au regard de l'obligation de mettre en place des facilités nécessaires à la préparation de la défense (§ 91). Eu égard aux faits de la cause, la Cour a estimé que le défaut d'accès aux données concernées n'était pas de nature à priver les requérants d'un procès globalement équitable, et elle a conclu à une non-violation de l'article 6 de ce chef.

Dans l'affaire *Yüksel Yalçınkaya c. Türkiye* [GC], 2023, la condamnation du requérant reposait dans une mesure déterminante sur des données relatives à l'utilisation par l'intéressé d'une application de messagerie cryptée, « ByLock », qui avaient été soumises à l'examen d'un expert spécialisé dans l'analyse des preuves numériques (§ 80), mais auxquelles le requérant n'avait pas eu plein accès en temps voulu (§§ 335-336). La Cour a reconnu que les preuves électroniques étaient désormais omniprésentes dans les procès pénaux en raison de l'importance croissante du numérique dans tous les aspects de la vie. Elle a également noté que les éléments de preuve électroniques différaient à bien des égards des preuves classiques, notamment en ce qui concerne leur nature et les technologies spéciales qui sont requises pour leur collecte, leur sécurisation, leur traitement et leur analyse. Elle a exposé que, surtout, ce type de preuve soulevait des problématiques de fiabilité distinctes car il était

intrinsèquement plus susceptible de destruction, de dégradation, d'altération ou de manipulation. Elle a également rappelé que l'utilisation d'éléments de preuve électroniques non vérifiés dans une procédure pénale peut aussi poser des difficultés particulières pour les juges car la procédure et les technologies appliquées à la collecte de ces preuves sont complexes et peuvent dès lors diminuer la capacité des juges nationaux à établir leur authenticité, leur exactitude et leur intégrité. Elle a par ailleurs estimé que le maniement de preuves électroniques, en particulier lorsque les données étaient cryptées, volumineuses ou d'une grande envergure, confrontaient les autorités répressives et les organes judiciaires à d'importantes difficultés pratiques et procédurales, tant au stade de l'enquête qu'à celui du procès (§ 312). Elle a conclu, eu égard aux circonstances de l'affaire, à une violation de l'article 6.

Dans l'affaire *A.L. et E.J. c. France* (déc.), 2024, les requérants avaient été poursuivis au Royaume-Uni sur le fondement de leurs données d'utilisateurs de la solution de communication chiffrée EncroChat ; ces données avaient été captées à l'initiative des autorités françaises et transmises aux autorités répressives du Royaume-Uni, lesquelles les avaient utilisées en tant qu'éléments de preuve dans le cadre des poursuites dont les requérants faisaient l'objet dans ce pays (§§ 100-102). Les requêtes, qui avaient été introduites uniquement contre la France et principalement sous l'angle du droit des requérants au respect de leur vie privée, ont été déclarées irrecevables pour non-épuisement des voies de recours internes. La Cour a considéré que les requérants disposaient en France d'une voie de recours qui leur aurait permis de contester de façon effective la mesure de transmission de données ainsi que la mesure de captation. Elle a conclu que les intéressés n'avaient pourtant exercé aucun recours devant les juridictions françaises et qu'ils n'avaient justifié d'aucune circonstance particulière qui les aurait dispensés de le faire.

3. Principe d'immédiateté dans la procédure pénale

La Cour a dit que l'un des éléments importants d'un procès pénal équitable est la possibilité pour l'accusé d'être confronté aux témoins en la présence du juge qui au bout du compte statue. Ce principe d'immédiateté est une garantie importante du procès pénal en ce que les observations faites par le juge au sujet du comportement et de la crédibilité d'un témoin peuvent avoir des conséquences non négligeables pour l'accusé. Dès lors, un changement dans la composition de la juridiction de jugement après l'audition d'un témoin important doit en principe entraîner une nouvelle audition de ce dernier.

Par exemple, dans l'affaire *Cutean c. Roumanie*, 2014, la Cour a conclu à une violation de l'article 6 dans une affaire où aucun des juges de la formation initiale qui avaient entendu le requérant et les témoins au premier degré de juridiction n'étaient restés pour poursuivre les débats. Elle a également noté que les dépositions du requérant et des témoins constituaient des éléments qui étaient pertinents pour la condamnation et que le juge n'avait pas entendus en personne. Dans ces circonstances, la Cour a estimé que la disponibilité des procès-verbaux d'audition ne pouvait compenser l'absence d'immédiateté dans le procès (§§ 60-73).

De même, dans l'affaire *Cerovšek et Božičnik c. Slovénie*, 2017, la Cour a conclu à une violation de l'article 6 au motif que les verdicts contre les requérants, c'est-à-dire la reconnaissance de leur culpabilité et les peines infligées, avaient été prononcés non pas par le juge qui les avait rendus mais par d'autres juges qui n'avaient pas participé au procès (§§ 37-48).

Par ailleurs, dans l'affaire *Iancu c. Roumanie*, 2021, même si elle ne s'est pas prononcée sur la question de la pertinence du principe de l'immédiateté, la Cour a examiné à l'aune de ce principe la question de la signature d'un jugement par la présidente d'une juridiction pour le compte d'une juge qui avait pris part à l'examen de l'affaire mais qui s'était retirée avant le prononcé du jugement (§§ 52-60). Elle a conclu à une non-violation de l'article 6 § 1 en soulignant en particulier les éléments suivants : le jugement avait été adopté par la formation judiciaire qui avait examiné l'affaire et qui s'était livrée à une analyse directe des éléments de preuve ; le jugement avait été rédigé, conformément au droit

interne, par un magistrat assistant qui avait participé aux audiences et aux délibérations et qui avait exposé, au nom de la formation de jugement, les motifs sur lesquels reposait le verdict de condamnation ; la juge qui s'était retirée s'était trouvée dans l'impossibilité objective de signer le jugement ; la signature des décisions de justice par tous les membres n'était pas un standard commun à tous les États membres du Conseil de l'Europe ; le législateur national avait limité l'admissibilité de cette solution aux seuls cas où le juge titulaire se trouvait dans l'impossibilité de signer la décision, et la présidente de la juridiction avait signé le jugement au nom de la juge retirée et non pas en son nom propre.

Un problème peut aussi se poser concernant le principe de l'immédiateté lorsqu'une juridiction d'appel infirme une décision d'acquittement rendue par une juridiction inférieure sans procéder à un nouvel examen des éléments de preuve, notamment sans entendre les témoins ou les requérants eux-mêmes.

Dans l'affaire *Júlíus Þór Sigurþórsson c. Islande*, 2019, le requérant avait été accusé d'entente délictueuse sur les prix. Le principal élément à charge contre lui était l'enregistrement d'une conversation téléphonique lors de laquelle il avait échangé des informations sur les prix avec l'un des autres accusés. Le tribunal de jugement, qui avait pris les dépositions orales des accusés, acquitta ensuite le requérant. Pendant la procédure d'appel devant la Cour suprême, laquelle jouissait de la plénitude de juridiction, le requérant ne fut pas réentendu. La Cour suprême annula l'acquittement de l'intéressé et le condamna à une peine de neuf mois d'emprisonnement. La Cour a rappelé que lorsque la juridiction d'appel doit examiner une affaire en fait et en droit et procéder à une appréciation globale de la culpabilité ou de l'innocence du requérant, elle ne peut, dans un souci d'équité du procès, statuer à ce sujet sans évaluer directement les éléments de preuve présentés en personne par l'inculpé qui souhaite prouver qu'il n'a pas commis l'acte constituant prétendument une infraction pénale (§ 33). Elle a dit qu'en principe, toute juridiction d'appel infirmant un acquittement prononcé en première instance doit prendre des mesures positives pour assurer à l'accusé la possibilité d'être entendu, et qu'à défaut, la juridiction d'appel doit se contenter d'annuler l'acquittement prononcé par la juridiction inférieure et de renvoyer l'affaire pour qu'elle soit rejugée (§ 38). La Cour a conclu, eu égard aux circonstances de l'affaire, à une violation de l'article 6.

4. Biais dans le système

Dans plusieurs affaires la Cour a conclu à une violation du droit d'accès des requérants à un tribunal à raison de préjugés et de partis pris entretenus par les juridictions internes à l'égard des intéressés.

Par exemple, l'affaire *Moldovan et autres c. Roumanie (n° 2)*, 2005, avait été introduite par des villageois roms qui dénonçaient le meurtre de leurs proches et la destruction de leurs maisons. Relevant que les autorités avaient fait des remarques discriminatoires à plusieurs reprises et qu'elles avaient catégoriquement refusé d'accorder des indemnités pour préjudice moral, la Cour a observé que l'origine ethnique des intéressés semblait avoir influencé de manière décisive la durée et l'issue de la procédure interne (§§ 139-140). Elle a conclu à une violation de l'article 14 combiné avec l'article 6.

De même, dans l'affaire *Paraskeva Todorova c. Bulgarie*, 2010, une juridiction interne avait refusé de surseoir à l'exécution d'une peine d'emprisonnement infligée à une femme d'origine rom au motif que celle-ci appartenait à un groupe minoritaire pour lequel la condamnation avec sursis n'était pas une condamnation, et qu'une peine avec sursis n'aurait pas atteint les objectifs de la prévention générale et de la prévention spéciale (§ 38). La Cour a considéré que la requérante avait été victime d'une discrimination fondée sur l'origine ethnique et a conclu à une violation de l'article 14 combiné avec l'article 6.

5. Motivation des décisions

Selon la jurisprudence constante de la Cour, qui reflète un principe lié à la bonne administration de la justice, les décisions judiciaires doivent exposer de manière suffisante les motifs sur lesquels elles se fondent. La motivation des décisions a pour finalité de démontrer aux parties qu'elles ont été entendues et, ainsi, de contribuer à une meilleure acceptation par elles de la décision. En outre, elle oblige le juge à fonder son raisonnement sur des arguments objectifs et préserve aussi les droits de la défense.

Dans l'affaire *Moreira Ferreira c. Portugal (n° 2)* [GC], 2017, un arrêt de la Cour suprême avait rejeté la demande de révision d'un jugement pénal qui avait été présentée par la requérante à la suite d'un arrêt rendu par la Cour concluant à une violation de l'article 6. La Cour suprême avait considéré que l'arrêt de la Cour n'était pas inconciliable avec la condamnation prononcée contre la requérante et qu'il ne soulevait pas de doutes sérieux sur son bien-fondé. La requérante contestait l'interprétation faite par la Cour suprême de l'arrêt de la Cour. La Cour a rappelé dans ce contexte que l'étendue du devoir de motivation peut varier selon la nature de la décision et doit s'analyser à la lumière des circonstances de chaque espèce. Elle a ajouté que, sans exiger une réponse détaillée à chaque argument du plaignant, cette obligation présuppose que toute partie à une procédure judiciaire puisse s'attendre à une réponse spécifique et explicite aux moyens décisifs pour l'issue de la procédure en cause. Elle a également rappelé que dans les affaires d'ingérences dans l'exercice des droits protégés par la Convention, elle vérifie si la motivation des décisions rendues par les juridictions nationales n'est pas automatique ou stéréotypée (§ 84). Appliquant ces principes aux faits de la cause, la Cour a conclu à une non-violation de l'article 6.

Dans l'affaire *Yüksel Yalçınkaya c. Türkiye* [GC], 2023 (voir la section « Audience contradictoire » ci-dessus), dans laquelle les allégations selon lesquelles le requérant appartenait à une organisation terroriste armée reposaient dans une mesure déterminante sur son utilisation de l'application de messagerie cryptée ByLock, la Cour a considéré que le préjudice subi par la défense en raison des lacunes susmentionnées avait été aggravé par les défaillances du raisonnement des juridictions internes concernant les éléments provenant de ByLock (§ 337). Elle a rappelé qu'eu égard à l'importance pour la bonne administration de la justice que les décisions soient dûment motivées, le silence gardé par les juridictions internes sur des questions cruciales touchant au cœur de l'affaire avait également suscité, dans le chef du requérant, des craintes justifiées quant à leurs conclusions et quant au fait que la procédure pénale pût avoir été conduite « uniquement pour la forme » (§ 341). La Cour a conclu à une violation de l'article 6.

L'importance de la motivation des décisions dépasse le cadre de l'article 6 et a été rappelée par la Cour dans le contexte de l'application d'autres articles de la Convention. Par exemple, dans l'affaire *X c. Lettonie* [GC], 2013, la Cour s'est penchée sur les exigences procédurales inhérentes à l'article 8 et a conclu à une violation de cette disposition à raison d'un défaut d'examen approfondi de tous les éléments pertinents de la part des tribunaux lettons lorsqu'ils ont tranché la question du retour de l'enfant de la requérante à la lumière de la Convention de La Haye du 25 octobre 1980 sur les aspects civils de l'enlèvement international d'enfants (§§ 119-120). La Cour a rappelé à cet égard que les juridictions internes doivent se prononcer par une décision spécialement motivée au vu des circonstances de l'espèce. Elle a précisé que tant un refus de tenir compte d'arguments des parties qu'une insuffisance de motivation de la décision rejetant de tels arguments seraient contraires aux exigences de l'article 8 de la Convention, et que la prise en compte effective de telles allégations, attestée par une motivation des juridictions internes qui soit non pas automatique et stéréotypée, mais suffisamment circonstanciée, est nécessaire. Elle a rappelé, à l'égard de sa propre compétence, que la motivation des décisions rendues par les juridictions internes lui permet également d'assurer le contrôle européen qui lui est confié (§ 107). Appliquant ces principes aux circonstances de l'affaire, la Cour a conclu à une violation de l'article 8.

C. Interdiction de la discrimination (article 14, article 1 du Protocole n° 12 à la Convention)

1. Profilage racial

La discrimination fondée sur l'origine ethnique réelle ou supposée d'une personne constitue une forme de discrimination raciale qui, compte tenu de la dangerosité de ses conséquences, exige une vigilance spéciale et une réaction vigoureuse de la part des autorités. Celles-ci doivent recourir à tous les moyens dont elles disposent pour combattre le racisme, renforçant ainsi la conception démocratique de la société, dans laquelle la diversité est perçue non pas comme une menace, mais comme une richesse. La Cour a récemment eu à connaître de plusieurs affaires soulevant des questions relatives au profilage racial.

Dans l'affaire *Basu c. Allemagne*, 2022, la Cour s'est penchée sur la situation d'un ressortissant allemand d'origine indienne qui, avec sa fille, avait fait l'objet d'un contrôle d'identité à bord d'un train qui venait d'entrer en Allemagne depuis la République tchèque. Le requérant demanda aux policiers la raison de ce contrôle ; ils lui répondirent qu'il s'agissait d'un contrôle aléatoire. Le requérant soutenait que son identité avait été contrôlée à cause de sa couleur de peau. Dans une affaire similaire, *Muhammad c. Espagne*, 2022, le requérant et un de ses amis, tous deux ressortissants pakistanais de la même origine ethnique, avaient fait l'objet d'un contrôle d'identité sur la voie publique qui était uniquement motivé, selon eux, par des considérations raciales. Dans ces deux affaires, la Cour a estimé que dès lors que la personne concernée peut prétendre de manière défendable qu'elle a fait l'objet d'un contrôle d'identité en raison de ses caractéristiques raciales et que l'acte en question relève du champ d'application de l'article 8 (droit au respect de la vie privée et familiale), l'obligation qui pèse sur les autorités d'enquêter sur l'existence d'un lien possible entre des attitudes racistes et l'acte d'un agent de l'État doit passer pour faire implicitement partie de la responsabilité qui incombe aux autorités, en vertu de l'article 14 combiné avec l'article 8 (*Basu c. Allemagne*, 2022, § 33, et *Muhammad c. Espagne*, 2022, § 68). Dans les circonstances de ces deux affaires, la Cour a conclu à une violation de ces deux dispositions combinées dans l'affaire *Basu c. Allemagne*, 2022, et à une absence de violation de ces dispositions dans l'affaire *Muhammad c. Espagne*, 2022.

Dans l'affaire *Memedova et autres c. Macédoine du Nord*, 2023, les requérants alléguaient qu'en application d'une circulaire du ministère de l'Intérieur ordonnant le renforcement des contrôles aux frontières à l'égard des groupes de demandeurs d'asile potentiels désireux de se rendre à l'étranger, des gardes-frontières avaient refusé de les laisser quitter le pays, et que ce refus reposait sur un profilage ethnique des personnes d'origine rom. S'appuyant sur un certain nombre de rapports nationaux et internationaux sur la question, la Cour a conclu que la circulaire était exempte de tout libellé discriminatoire, mais qu'en raison de la manière dont elle avait été appliquée en pratique par les gardes-frontière, un nombre disproportionné de Roms s'étaient vu empêchés de voyager à l'étranger. Estimant que cette situation s'analysait en une différence de traitement qui ne répondait à aucune justification objective ou raisonnable, la Cour a conclu à une violation de l'article 14 combiné avec l'article 2 du Protocole n° 4 à la Convention (liberté de circulation).

Dans l'affaire *Wa Baile c. Suisse*, 2024, dans laquelle le requérant alléguait qu'il avait été interpellé et fouillé dans une gare au seul motif qu'il avait la peau foncée, la Cour a conclu à un manquement aux obligations procédurales inhérentes à l'article 14 combiné avec l'article 8 au motif que les juridictions (pénales et administratives) internes étaient restées en défaut de rechercher si le contrôle d'identité litigieux avait ou non obéi à une motivation raciste (§§ 93-103). Elle a par ailleurs rappelé que l'absence de garanties juridiques et administratives suffisantes est susceptible de donner lieu à des contrôles d'identité discriminatoires (§ 130) et elle a jugé, au regard des circonstances de l'affaire, que le Gouvernement n'avait pas été en mesure de réfuter la présomption selon laquelle le contrôle d'identité litigieux avait été effectué pour des motifs discriminatoires (§§ 131-135). En conséquence, elle a également conclu à une violation du volet matériel de l'article 14 combiné avec l'article 8.

2. Biais dans le système

La Cour a admis dans sa jurisprudence que peut être considérée comme discriminatoire une politique ou une mesure générale qui a des effets préjudiciables disproportionnés sur un groupe de personnes, même si elle ne vise pas spécifiquement ce groupe, et qu'une discrimination potentiellement contraire à la Convention peut résulter d'une situation de fait.

Tel était le cas dans l'affaire *D.H. et autres c. République tchèque* [GC], 2007. Les requérants, des enfants d'origine ethnique rom, avaient été placés dans des écoles spéciales pour les enfants présentant des déficiences mentales sur la base des résultats de tests qui avaient été appliqués à tous les enfants en âge d'être scolarisés. S'appuyant sur des données statistiques, les requérants alléguaient que dans ces tests, les références culturelles et la langue n'étaient pas adaptées à la population rom (§ 27), et que cela avait eu pour conséquence qu'un nombre disproportionné d'élèves roms avaient été placés dans des établissements destinés aux enfants atteints de déficiences mentales. La Cour a relevé que tous les enfants examinés avaient été soumis aux mêmes tests et que ces tests étaient conçus pour la population majoritaire et ne tenaient pas compte des particularités des Roms ; elle a estimé qu'il existait à tout le moins un risque que les tests en question fussent entachés de préjugés et que leurs résultats ne fussent pas lus à la lumière des particularités et des caractéristiques spécifiques des enfants roms qui les subissaient (§§ 200-201). Elle a conclu à une violation de l'article 14 combiné avec l'article 2 du Protocole n° 1 (droit à l'instruction).

3. Données médicales sensibles et accès aux soins médicaux

La Cour s'est penchée, dans sa jurisprudence, sur l'importance que revêt la confidentialité des données médicales sensibles pour la protection du droit au respect de la vie privée. Dans l'affaire *I. c. Finlande*, 2008, la requérante, qui était séropositive, alléguait que son dossier médical avait été rendu accessible à ses collègues. Elle travaillait comme infirmière dans un hôpital public et elle était soignée pour son infection au VIH dans le même établissement. Elle commença à soupçonner que ses collègues étaient au courant de sa maladie. Il lui fut impossible, à cause de la manière dont le registre des patients était alors tenu, d'obtenir des informations sur l'identité des personnes ayant consulté son dossier médical, et pour cette raison, d'obtenir réparation du préjudice causé par le défaut de protection allégué de son dossier médical confidentiel. La Cour a considéré que la confidentialité des dossiers médicaux était cruciale non seulement pour le respect de la vie privée des patients, mais aussi pour la préservation de leur confiance dans le corps médical et dans les services de santé en général. Elle a dit que ces considérations valaient particulièrement lorsqu'il s'agissait d'informations relatives à la séropositivité d'une personne, compte tenu du caractère particulièrement sensible des questions qui se rattachaient à cette maladie (§ 38), et elle a ainsi conclu à une violation de l'article 8. Si cette affaire n'a pas été considérée comme soulevant potentiellement une question de discrimination, il convient de noter que la Cour a admis dans sa jurisprudence que l'état de santé d'une personne, notamment la séropositivité, doit être considéré comme un motif de discrimination relevant de l'article 14 de la Convention ; elle a également dit que les personnes vivant avec le VIH constituent un groupe vulnérable victime de préjugés et de stigmatisation dans la société. Par conséquent, dans de tels cas, les États disposent d'une marge d'appréciation étroite pour adopter des mesures réservant à certains groupes un traitement particulier fondé sur la santé de leurs membres (*Kiyutin c. Russie*, 2011, §§ 57 et 64).

Dans plusieurs affaires, la Cour a examiné des allégations d'approches entachées de préjugés liés aux caractéristiques personnelles des requérants dans le domaine des soins médicaux. Les affaires *V.C. c. Slovaquie*, 2011, et *I.G. et autres c. Slovaquie*, 2012, portaient sur la stérilisation forcée de femmes roms. La Cour a dit que les États étaient tenus par l'obligation positive de mettre en place des garanties juridiques effectives pour protéger les femmes contre une stérilisation forcée et, en particulier, d'accorder une considération particulière à la santé reproductive des femmes roms. Elle a estimé à cet égard que la stérilisation forcée pratiquée de longue date sur cette minorité ethnique vulnérable

exigeait qu'une protection particulière fût accordée aux femmes roms (*V.C. c. Slovaquie*, 2011, §§ 154-155, et *I.G. et autres c. Slovaquie*, 2012, §§ 143-146). Dans ces deux affaires, la Cour a conclu à une violation des articles 3 (interdiction de la torture) et 8, et elle a estimé qu'il n'y avait pas lieu d'examiner séparément le grief de violation de l'article 14 formulé par les requérantes.

Une telle différence de traitement peut également se produire dans le domaine médical à cause des convictions religieuses du patient. Si elle n'a pas soulevé de questions sous l'angle de l'article 14, l'affaire *Pindo Mulla c. Espagne* [GC], 2024 portait sur le respect des instructions données par la patiente, pour des raisons liées à ses convictions religieuses, en matière de traitement médical. Dans cette affaire, la requérante, témoin de Jéhovah, avait fait enregistrer des directives médicales anticipées pour consigner son refus exprès de recevoir tout type de transfusion sanguine dans le cadre de soins médicaux, quelle qu'en fût la nature, même si sa vie était en danger, comme le lui dictaient ses croyances religieuses. Elle avait également signé un formulaire de consentement éclairé dans lequel elle exprimait son refus des transfusions sanguines. Il fut noté qu'elle acceptait tout traitement médical n'impliquant pas l'utilisation de sang. Elle fut par la suite transférée en urgence dans un autre hôpital, dans lequel elle reçut finalement une transfusion sanguine sur le fondement d'une décision prise par la juge de permanence. La demande adressée à la juge de permanence indiquait que la requérante était témoin de Jéhovah, qu'elle avait exprimé oralement son refus de tous types de traitement et qu'elle se trouverait dans un état très instable lorsqu'elle arriverait. La Cour a exposé la manière dont il y a lieu, dans une situation d'urgence, de concilier l'autonomie du patient avec son droit à la vie (§§ 138-140 et 146-147). Elle a dit que la décision de refus d'un traitement vital devait être « clair[e], précis[e] et dépourvu[e] d'ambiguïté » et « représente[r] la position du patient sur ce point au moment considéré » (§ 148). Elle a ajouté que s'il existait des motifs raisonnables de mettre en doute l'un de ces aspects, les membres des professions de santé étaient tenus de mettre en œuvre des mesures raisonnables pour déterminer quels pourraient être les souhaits du patient. Elle a précisé que lorsque, malgré la mise en œuvre de telles mesures, le médecin ou la juridiction nationale saisie se trouvent dans l'impossibilité d'établir clairement la volonté du patient, ils sont dans l'obligation de protéger la vie du patient en lui administrant des soins essentiels (§§ 149-150). Elle a souligné que, lorsqu'un État a choisi de mettre en place un système de directives médicales anticipées dont des patients se prévalent, il est important que ce système fonctionne effectivement (§ 156). Eu égard aux faits de la cause, la Cour a conclu à une violation de l'article 8 lu à la lumière de l'article 9 (liberté de pensée, de conscience et de religion).

4. Cyberviolence fondée sur le genre

La Cour a expressément considéré que la violence domestique est une forme de violence fondée sur le genre, celle-ci constituant elle-même une forme de discrimination à l'égard des femmes (*Opuz c. Turquie*, 2009, §§ 184-191 et *Volodina c. Russie*, 2019, § 110). Dans une série d'affaires, elle a en outre conclu à une violation des droits des requérantes dans le contexte de cyberviolences commises par des partenaires intimes : *Buturugă c. Roumanie*, 2020 et *Volodina c. Russie (n° 2)*, 2021. Si ces affaires n'ont pas été examinées sous l'angle de l'article 14 de la Convention, elles ont été envisagées dans le contexte général des violences domestiques tel qu'exposé dans l'arrêt *Opuz c. Turquie*, 2009.

L'affaire *Buturugă c. Roumanie*, 2020, portait sur des allégations de violence domestique et de violation par l'ex-époux de la requérante du secret de la correspondance électronique de l'intéressée. La requérante se plaignait de défaillances du système de protection des victimes de la violence domestique et critiquait le refus des autorités de prendre en compte sa plainte relative à une violation du secret de sa correspondance par son ex-époux. La Cour a estimé que l'État avait manqué à ses obligations positives en matière de violence domestique. Elle a considéré en particulier que les autorités nationales n'avaient pas abordé l'enquête pénale comme soulevant le problème spécifique de la violence domestique, et qu'elles n'avaient dès lors pas donné une réponse adaptée à la gravité des faits dénoncés par la requérante. Elle a considéré que l'enquête sur les actes de violence avait été défaillante et qu'aucun examen sur le fond de la plainte pour violation du secret de la correspondance,

qui était étroitement liée à la plainte pour violences, n'avait été effectué (§§ 75-78). Elle a observé que la cyberviolence est actuellement reconnue comme un aspect de la violence à l'égard des femmes et des filles et qu'elle peut se présenter sous diverses formes, dont les atteintes à la vie privée par des moyens informatiques, l'intrusion dans l'ordinateur de la victime et la captation, le partage et la manipulation des données et des images, y compris des données intimes (§ 74). Elle a ainsi conclu à une violation des articles 3 et 8.

Dans l'affaire *Volodina c. Russie (n° 2)*, 2021, la requérante alléguait que son ancien compagnon lui avait fait subir un cyberharcèlement. Elle indiquait que celui-ci avait usurpé son nom, ses données personnelles et des photos intimes d'elle pour créer de faux comptes sur les réseaux sociaux, qu'il avait placé un traceur GPS dans son sac à main, et qu'il lui avait envoyé des menaces de mort sur les réseaux sociaux. Elle avançait que les autorités avaient manqué à leur obligation de la protéger et de mener une enquête effective sur les allégations qu'elle avait formulées contre son ancien compagnon. La Cour a estimé que les autorités avaient manqué à leur obligation de protéger la requérante contre des violences graves, qu'elles n'avaient pas mené d'enquête effective alors même qu'elles disposaient des outils juridiques nécessaires pour poursuivre le compagnon de l'intéressée, et qu'elles n'avaient à aucun moment réfléchi à ce qui pouvait et aurait dû être fait pour protéger la requérante contre un harcèlement en ligne récurrent. La Cour a ainsi conclu à une violation de l'article 8.

Résumé

En se fondant sur la jurisprudence exposée ci-dessus, et sans toutefois se lancer dans des considérations concernant les effets de l'IA sur l'étendue et la protection futures des droits et des libertés fondamentaux, il est possible de dégager certaines conclusions générales.

Tout d'abord, au point d'intersection entre l'IA et la liberté d'expression se trouve un univers complexe et en constante évolution qui redessine les frontières de la communication à l'ère du numérique. Le développement des technologies numériques, et notamment l'essor des systèmes d'intelligence artificielle, produit des effets considérables tant sur l'exercice que sur la protection de la liberté d'expression ; il est indéniable que l'IA y incarne un double rôle, favorisant et menaçant potentiellement cette liberté. Il est essentiel de protéger tant le droit de communiquer des informations que celui d'en recevoir dans les médias traditionnels comme dans les médias numériques (voir *Delfi AS c. Estonie* [GC], 2015, à la section « Nouvelles technologies » ci-dessus, et *Big Brother Watch et autres c. Royaume-Uni* [GC], 2021, à la section « Transferts de données et protection des sources journalistiques » ci-dessus).

Ensuite, si l'utilisation des systèmes d'IA dans le domaine judiciaire présente un potentiel élevé, les avis divergent quant à la mesure dans laquelle l'IA peut réellement être employée dans le cadre du travail judiciaire. Un avis extrême consiste à remettre en cause l'idée qu'une juridiction humaine soit nécessaire, tandis que l'autre extrême consiste à soutenir qu'une appréciation humaine est requise pour toute décision judiciaire ayant une incidence sur les intérêts des justiciables. Il est en outre nécessaire de réfléchir d'une part à des moyens d'utiliser les compétences et connaissances juridiques traditionnelles pour faire en sorte que les systèmes d'IA contribuent à l'amélioration de l'efficacité et de la qualité du processus judiciaire en jouant un rôle d'assistants (ou de participants) productifs dans le cadre de ce processus, et d'autre part au degré d'intervention humaine requis.

Point tout aussi important, considérant le principe selon lequel le but de la Convention consiste à protéger des droits non pas théoriques ou illusoires, mais concrets et effectifs, le droit à un procès équitable ne peut passer pour effectif que si les demandes et observations des parties sont vraiment « entendues », c'est-à-dire dûment examinées par le tribunal (*García Ruiz c. Espagne* [GC], 1999, § 26). Cela étant, il est incontestable que les preuves électroniques sont désormais omniprésentes dans les procès pénaux en raison de l'importance croissante du numérique dans tous les aspects de la vie (*ibidem*, § 312). À cet égard, la Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement et les travaux de la CEPEJ sur la cartographie des systèmes d'IA ainsi que d'autres outils clés de cyberjustice appliqués dans la transformation numérique du système judiciaire offriront à la Cour des sources d'informations pertinentes (Centre de ressources sur la cyberjustice et l'IA – Commission européenne pour l'efficacité de la justice (CEPEJ) (coe.int)).

Enfin, il convient de rappeler que les systèmes d'IA ne sont pas exempts de biais et de discriminations. Ces problèmes peuvent avoir diverses origines, comme des biais dans les données d'entraînement, les choix de conception algorithmique, ou encore le contexte sociétal plus vaste dans lequel ces systèmes sont déployés. Compte tenu de la portée potentielle de l'application de l'IA dans la vie quotidienne, ils peuvent avoir de lourdes conséquences pour les droits individuels et accentuer les divergences et les différences qui peuvent être sources de discrimination. Ils peuvent exclure certaines catégories d'une protection effective ou se fonder sur des normes qui sont établies à partir de données représentatives de la majorité, qui sont dépourvues de sensibilité au contexte ; l'arrêt *D.H. et autres c. République tchèque* [GC], 2007 (voir la section « Interdiction de la discrimination » : « Biais dans le système » ci-dessus) illustre de manière édifiante, dans un contexte pré-numérique, les dangers liés aux biais dans les systèmes. Il est également urgent de se pencher sur l'utilisation potentielle de l'IA à des fins de cyberviolence entre partenaires intimes (voir *Buturugă c. Roumanie*, 2020, dans la section « Cyberviolence fondée sur le genre » ci-dessus). Les travaux du Comité d'expert·es du Conseil de

l'Europe sur la lutte contre la violence à l'égard des femmes et des filles facilitée par la technologie (GEC/PC-eVIO) seront pour la Cour une source d'informations utiles sur ce point.

Enfin et surtout, la Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit, son rapport explicatif, la méthodologie HUDERIA et le futur Manuel sur les droits humains et l'intelligence artificielle fourniront à la Cour des orientations importantes pour l'appréciation des obligations incombant aux États en matière d'IA et de protection des droits de l'homme dans les années à venir.

Annexe : jurisprudence

Ahmet Yıldırım c. Turquie, n° 3111/10, CEDH 2012

A.L. et E.J. c. France (déc.), n^os^ 44715/20 et 47930/21, 24 septembre 2024
Animal Defenders International c. Royaume-Uni [GC], n° 48876/08, CEDH 2013

Basu c. Allemagne, n° 215/19, 18 octobre 2022
Biancardi c. Italie, n° 77419/16, 25 novembre 2021
Big Brother Watch et autres c. Royaume-Uni [GC], n^os^ 58170/13 et 2 autres, 25 mai 2021
Bowman c. Royaume-Uni, 19 février 1998, *Recueil des arrêts et décisions* 1998-I
Buturugă c. Roumanie, n° 56867/15, 11 février 2020

Catt c. Royaume-Uni, n° 43514/15, 24 janvier 2019
Cerovšek et Božičnik c. Slovénie, n^os^ 68939/12 et 68949/12, 7 mars 2017
Parti communiste de Russie et autres c. Russie, n° 29400/05, 19 juin 2012
Cutean c. Roumanie, n° 53150/12, 2 décembre 2014

Daugaard Sorensen c. Danemark, n° 25650/22, 15 octobre 2024
Delfi AS c. Estonie [GC], n° 64569/09, CEDH 2015
D.H. et autres c. République tchèque [GC], n° 57325/00, CEDH 2007-IV

Comité de rédaction de Pravoye Delo et Shtekel c. Ukraine, n° 33014/05, 5 mai 2011

Farcaş et autres c. Roumanie [Comité], n° 30502/05, 5 juin 2018

García Ruiz c. Espagne [GC], n° 30544/96, CEDH 1999-I
Glukhin c. Russie, n° 11519/20, 4 juillet 2023

Hurbain c. Belgique [GC], n° 57292/16, 4 juillet 2023

I. c. Finlande, n° 20511/03, 17 juillet 2008
Iancu c. Roumanie, n° 2915/17, 23 février 2021
I.G. et autres c. Slovaquie, n° 15966/04, 13 novembre 2012

Júlíus Þór Sigurþórsson c. Islande, n° 38797/17, 16 juillet 2019

Kiyutin c. Russie, n° 2700/10, CEDH 2011

Magyar Jeti Zrt c. Hongrie, n° 11257/16, 4 décembre 2018
Magyar Tartalomszolgáltatók Egyesülete et Index.hu Zrt c. Hongrie, n° 22947/13, 2 février 2016
Memedova et autres c. Macédoine du Nord, n^os^ 42429/16 et 2 autres, 24 octobre 2023
Moldovan et autres c. Roumanie, n^os^ 41138/98 et 64320/01, CEDH 2005-VII
Moreira Ferreira c. Portugal (n° 2) [GC], n° 19867/12, 11 juillet 2017
Muhammad c. Espagne, n° 34085/17, 18 octobre 2022

Opuz c. Turquie, n° 33401/02, CEDH 2009
Orlovskaya Iskra c. Russie, n° 42911/08, 21 février 2017

Paraskeva Todorova c. Bulgarie, n° 37193/07, 25 mars 2010
Pentikäinen c. Finlande [GC], n° 11882/10, CEDH 2015
Pindo Mulla c. Espagne [GC], n° 15541/20, 17 septembre 2024

S. et Marper c. Royaume-Uni [GC], nos 30562/04 et 30566/04, CEDH 2008
Sanchez c. France [GC], no 45581/15, 15 mai 2023
Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande [GC], no 931/13, 27 juin 2017
Sigurður Einarsson et autres c. Islande, no 39757/15, 4 juin 2019

Thlimmenos c. Grèce [GC], no 34369/97, CEDH 2000-IV
Times Newspapers Ltd c. Royaume-Uni (nos 1 et 2), nos 3002/3 et 23676/03, CEDH 2009

V.C. c. Slovaquie, no 18968/07, 8 novembre 2011
Volodina c. Russie, no 41261/17, 9 juillet 2019
Volodina c. Russie (no. 2), no 40419/19, 14 septembre 2021

Wa Baile c. Suisse, nos 43868/18 et 25883/21, 20 février 2024

X c. Lettonie [GC], no 27853/09, CEDH 2013
Xavier Lucas c. France, no 15567/20, 9 juin 2022

Yüksel Yalçınkaya c. Türkiye [GC], no 15669/20, 26 septembre 2023

Zavodnik c. Slovénie, no 53723/13, 21 mai 2015