La protection des données à caractère personnel en droit européen

Herveg, Jean; Van Gyseghem, Jean-Marc

Published in:
Journal européen des droits de l'homme

Publication date:
2020

Document Version
le PDF de l'éditeur

La protection des données à caractère personnel en droit européen – Chronique de jurisprudence (2019)

Personal Data Protection in European Law – Column of case-law (2019)

Jean Herveg & Jean-Marc Van Gyseghem[1]

Résumé

La chronique analyse la contribution de la Cour européenne des droits de l'homme et des juridictions de l'Union européenne à la protection des données pour l'année 2019.

Pour cette période, les arrêts et décisions de la Cour européenne des droits de l'homme qui furent retenus concernent la protection de l'identité des individus, les litiges en matière de filiation, le phénomène de la « Lustration », l'équilibre entre liberté d'expression, vie privée, réputation et honneur, la protection des communications et le harcèlement, la conservation des données par la police, la protection des données saisies lors de perquisitions chez des avocats, la protection contre les mesures de surveillance secrète, la protection contre les caméras cachées à des fins d'intimidation et la protection de la vie privée en prison.

Pour ce qui concerne la Cour de justice de l'Union européenne, les arrêts en matière de protection des données à caractère personnel qui sont nettement moins nombreux que ceux de la Cour européenne des droits de l'homme permettent d'analyser des aspects de la directive 95/46 tels que son champ d'application matériel, le droit de recours juridictionnel, la conservation des données,

Abstract

The paper analyses the contribution of the case law of the European Court of Human Rights and the courts of the European Union to data protection for the year 2019.

For this period, the judgments and decisions of the European Court of Human Rights that were upheld concern the protection of identity, filiation disputes, the phenomenon of "lustration", the balance between freedom of expression, privacy, reputation and honor, the protection of communications in relation to harassment, data retention by the police, protection of data seized during searches of lawyers' offices, protection against secret surveillance measures, protection against hidden cameras for the purpose of intimidation, and the protection of privacy in prison.

The Court of Justice of the European Union, and even if the number of decisions is much less than the ones from the European Court of Justice, had, during 2019, the opportunity to deal with various concepts brought by Directive 95/46 as rationae materiae, effective judicial remedy, conservation of personal data, etc. It is worth noting that, if some decisions concern Directive 95/46, they can be transposed to the General Data

[1] This work has been done with the financial support from the European Union's Horizon 2020 general MGA program under Grant Agreements n° 830892 (SPARTA). Cette publication a également été réalisée avec le support financier de FEDER dans le cadre du portefeuille de projets WAL-E-CITIES (2017-2020) pour la Région wallonne. La publication ne reflète que l'opinion de ses auteurs et la Commission européenne ne peut être tenue responsable de l'usage qui en serait fait.

etc. Il est utile de noter que, si certains arrêts concernent la directive 95/46, ils sont transposables au Règlement général sur la protection des données (RGPD) dès lors que les principes relatifs à la protection des données n'ont pas été modifiés.

Protection Regulation (GDPR) as the data protection principles have not been modified.

I. La protection des données dans la jurisprudence de la Cour européenne des droits de l'homme

A. Rappel : la règle du seuil minimum de gravité

Le critère du manque de préjudice important a été conçu pour permettre à la Cour de traiter rapidement les requêtes à caractère futile afin de se concentrer sur sa mission essentielle, qui est d'assurer au niveau européen la protection juridique des droits garantis par la Convention et ses Protocoles[2].

Issue du principe *de minimis non curat praetor*, cette condition de recevabilité renvoie à l'idée que la violation d'un droit, quelle que soit sa réalité d'un point de vue strictement juridique, doit atteindre un seuil minimum de gravité pour justifier un examen par une juridiction internationale.

L'appréciation de ce seuil est, par nature, relative et dépend des circonstances de l'espèce. Cette appréciation doit tenir compte tant de la perception subjective du requérant que de l'enjeu objectif du litige[3].

Afin de vérifier si la violation d'un droit a atteint le seuil minimum de gravité il y a lieu de prendre en compte notamment les éléments suivants : la nature du droit prétendument violé, la gravité de l'incidence de la violation alléguée dans l'exercice d'un droit et/ou les conséquences éventuelles de la violation sur la situation personnelle du requérant[4].

B. Protection de l'identité

1. *Protection de l'identité ethnique*

L'identité ethnique est un aspect relatif à l'identité des individus et qui relève de la sphère personnelle protégée par l'article 8[5].

[2] Cour eur. D.H., arrêt du 24 janvier 2019, n[os] 54414/13 et 54264/15, *Cordella et autres c. Italie*, § 135.
[3] *Ibid.*, § 136.
[4] *Ibid.*, § 137.
[5] Cour eur. D.H., arrêt du 16 mai 2019, n[o] 9825/13, *Tasev c. Macédoine du Nord*, § 32.

Le fait de refuser aux membres d'une minorité le droit de choisir de se soumettre aux règles applicables aux personnes qui ne font pas parties d'une minorité, constitue non seulement un traitement discriminatoire mais aussi une violation d'un droit d'une importance majeure dans le domaine de la protection des minorités, c'est-à-dire le droit à la libre auto-identification. L'aspect négatif de ce droit, à savoir le droit de choisir de ne pas être traité comme un membre d'une minorité, n'est pas limité de la même manière que l'aspect positif de ce droit. Le choix en question doit être totalement libre et informé. Il doit être respecté tant par les membres de la minorité que par l'État lui-même[6].

2. *Changement du nom de famille*

La Convention ne contient pas de disposition explicite en matière de nom. En tant que moyen d'identification personnelle et de rattachement à une famille, le nom d'une personne n'en concerne pas moins la vie privée et familiale de celle-ci[7].

Que l'État et la société aient un intérêt à en réglementer l'usage ne suffit pas pour exclure la question du nom d'une personne du domaine de la vie privée et familiale, conçue comme englobant, dans une certaine mesure, le droit pour l'individu de nouer des relations avec ses semblables[8].

Il peut exister de justes motifs amenant un individu à vouloir changer de nom. Toutefois, des restrictions légales à pareille possibilité peuvent se justifier dans l'intérêt public, par exemple pour permettre d'assurer un enregistrement exact de la population ou pour permettre de sauvegarder les moyens d'une identification personnelle et relier à une famille les porteurs d'un nom donné. Dans le domaine de la réglementation du changement de nom, les États jouissent d'une large marge d'appréciation et la Cour n'a pas vocation à se substituer aux autorités internes compétentes pour déterminer la politique la plus opportune en la matière. La mission de la Cour se limite à apprécier sous l'angle de la Convention les décisions que les juridictions nationales ont rendues dans l'exercice de leur pouvoir d'appréciation[9].

Les autorités nationales sont en principe mieux placées pour apprécier le niveau de désagrément imputable à l'usage d'un nom plutôt que d'un autre dans leur société nationale. Pour déterminer s'il y a eu violation dans un cas donné, la Cour doit examiner si l'application de la législation répond à la souplesse nécessaire aux besoins des personnes qui demandent le changement de leur nom[10].

---

6 *Ibid.*, § 33.
7 Cour eur. D.H., arrêt du 25 juin 2019, n^os^ 18684/07 et 21101/07, *Aktas et Aslaniskender c. Turquie*, § 42.
8 *Idem*.
9 *Ibid.*, § 45.
10 *Ibid.*, § 47.

Dans ce contexte, les juridictions nationales doivent démontrer qu'elles ont mis en balance les intérêts en jeu. En l'espèce, les juridictions nationales se sont contentées d'un examen purement formaliste des textes législatifs et réglementaires sans avoir pris en compte les situations spécifiques et personnelles de chacun des intéressés, ni les arguments soulevés par ceux-ci et sans avoir procédé à une mise en balance des intérêts en jeu. Le Gouvernement turc n'a pas plus démontré en quoi le changement des noms des requérants pour des noms qui ne sont pas de langue turque était susceptible de troubler de quelque manière que ce soit l'intérêt public[11].

3. *Reconnaissance de l'identité de genre*

Le droit au respect de la vie privée recouvre l'identité de genre en tant que composante de l'identité personnelle. Cela vaut pour tous les individus, y compris les personnes transgenres qui n'ont pas subi de traitement de changement de sexe ou qui ne souhaitent pas en subir un[12].

L'article 8 impose aussi aux États une obligation positive de garantir à leurs citoyens le droit au respect effectif de leur intégrité physique et psychologique. Cette obligation peut impliquer l'adoption de mesures spécifiques, y compris la mise à disposition d'un moyen efficace et accessible de protéger le droit au respect de la vie privée. Ces mesures peuvent comprendre à la fois la mise en place d'un cadre réglementaire de mécanismes juridictionnels et d'exécution protégeant les droits des individus ainsi que la mise en œuvre, le cas échéant, de ces mesures dans différents contextes[13].

En l'espèce, la Cour a considéré que l'État ne disposait pas d'un cadre juridique offrant des procédures rapides, transparentes et accessibles permettant de changer l'indication du sexe des personnes transgenres dans leur certificat de naissance[14].

4. *Changement de nom sur un diplôme*

Les questions relatives au nom d'une personne relèvent du droit à la vie privée. En ce qui concerne les documents officiels, la rétention de documents d'identité ou le refus de délivrer de nouveaux documents d'identité qui sont nécessaires dans la vie quotidienne, par exemple pour s'identifier auprès des autorités publiques, pour recevoir des soins médicaux ou pour trouver un emploi, constitue une ingérence dans le droit au respect de la vie privée[15].

---

[11] *Ibid.*, §§ 47-48.
[12] Cour eur. D.H., arrêt du 17 janvier 2019, n° 29683/16, *X c. Ancienne république yougoslave de Macédoine*, § 38.
[13] *Ibid.*, § 63.
[14] *Ibid.*, § 70.
[15] Cour eur. D.H., arrêt du 21 novembre 2019, n° 200/15, *P.R. c. Autriche*, § 26.

La Cour observe que dans certains pays, comme l'Autriche, une grande importance est accordée aux diplômes universitaires en général. Elle note qu'il est aussi courant de s'adresser à une personne en indiquant son diplôme universitaire même en dehors des milieux professionnels. Un diplôme universitaire peut donc être étroitement lié au nom d'une personne. En outre, un diplôme universitaire en soi, qui est le résultat d'une carrière universitaire réussie, doit être considéré comme un aspect pertinent de l'identité personnelle d'une personne[16].

S'il est vrai qu'en refusant de délivrer un nouveau diplôme ou une version amendée, le droit du candidat en tant que tel de porter son diplôme universitaire n'a pas été enfreint, il s'est néanmoins vu refuser un document généralement accepté indiquant son nouveau nom pour prouver son titre universitaire. La Cour estime qu'il est probable que le requérant, en tant qu'avocat diplômé, sera confronté à plusieurs occasions dans lesquelles il lui sera demandé de fournir des preuves de ses études en présentant un document officiel délivré par l'université. En outre, l'utilisation injustifiée d'un diplôme universitaire constitue une infraction administrative en Autriche. Ainsi, l'exigence faite au requérant d'apporter la preuve qu'il utilise légalement un titre universitaire en présentant un diplôme contenant son ancien nom, est contraire à son droit, reconnu en droit autrichien, d'avoir son nom changé[17]. Il y a dès lors ingérence dans l'exercice du droit au respect de la vie privée.

Dans le cas d'espèce, un aspect très spécifique de la vie privée est concerné. Même si l'on ne peut pas dire que les valeurs fondamentales ou des aspects essentiels de la vie privée ont été altérés, la Cour, néanmoins, accepte que l'impact de l'absence d'une nouvelle version du diplôme ou d'un certificat modifié est significatif, alors que l'obligation positive peut être considérée comme relativement étroite et précise, l'impact éventuel sur l'État ne semblant pas être conséquent[18].

S'il est vrai qu'il existe un intérêt général du public à garantir la sécurité juridique et exclure les possibilités de fraude en ce qui concerne la délivrance des diplômes universitaires, la présente affaire ne concerne pas la délivrance d'un diplôme mais simplement la modification d'un diplôme qui avait déjà été accordé dans le passé. La Cour ne voit pas comment la délivrance d'une nouvelle version du diplôme modifié ou d'un duplicata portant le nouveau nom, pourrait nuire à la fiabilité d'un tel document ou à l'attribution du titre universitaire lui-même[19].

La Cour ne méconnaît pas le fait que cela peut impliquer une certaine charge administrative. Toutefois, cela ne peut pas justifier en soi un refus inconditionnel car l'université semble libre, par exemple, d'imposer des frais et de poser des conditions à pareille requête. En l'espèce, le refus de modifier le diplôme était fondé sur

[16] *Ibid.*, § 28.
[17] *Ibid.*, § 29.
[18] *Ibid.*, § 43.
[19] *Ibid.*, § 44.

des considérations purement formelles, sans tenir compte des raisons spécifiques avancées par le requérant, et donc sans procéder à une mise en balance des intérêts en présence[20].

En outre, la Cour ne discerne aucune raison qui pourrait justifier le refus de la délivrance d'un diplôme [ou certificat] modifié[21].

C. Litiges en matière de filiation

1. *Procédures en matière de paternité*

Les procédures ayant trait à la paternité tombent sous l'empire de l'article 8 de la Convention. Ce dernier protège non seulement la vie « familiale » mais aussi la vie « privée », qui englobe des aspects de l'identité physique et sociale d'un individu[22].

Pour trancher une action en établissement de paternité, les tribunaux doivent tenir compte de l'intérêt supérieur de l'enfant[23]. Il revient aussi aux juridictions nationales de ménager un juste équilibre entre le droit d'un requérant de voir dissiper sans retard inutile son incertitude quant à son identité personnelle et le droit du père présumé de ne pas subir de tests ADN[24].

2. *Recherche de son identité*

Chacun a un intérêt vital, protégé par l'article 8 de la Convention, à connaître la vérité sur son identité et à éliminer toute incertitude à ce sujet[25].

Le droit de connaître ses ascendants s'inscrit dans le cadre du concept de « vie privée » qui englobe des aspects importants de l'identité personnelle d'un individu, comme l'identité de ses parents. En outre, il n'y a pas de raison de principe pour que la notion de « vie privée » soit interprétée de manière à exclure la détermination d'une relation juridique ou biologique entre un enfant né hors mariage et son père naturel[26].

Si, d'une part, les personnes ont le droit de connaître leur identité, d'autre part, l'intérêt d'un père putatif à être protégé contre des allégations concernant des circonstances qui remontent à de nombreuses années ne peut être nié. Enfin, d'autres intérêts peuvent entrer en jeu, tels que ceux de tiers (principalement ceux de la famille du père putatif) et les intérêts généraux de la sécurité juridique[27].

---

[20] *Ibid.*, § 44.
[21] *Ibid.*, § 44.
[22] Cour eur. D.H., décision du 10 septembre 2019, n° 69681/13, *M. c. Roumanie*, § 38.
[23] Cour eur. D.H., décision du 10 septembre 2019, n° 69681/13, *M. c. Roumanie*, § 45 ; arrêt du 15 octobre 2019, n° 44690/09, *Çapin c. Turquie*, § 77.
[24] Cour eur. D.H., décision du 10 septembre 2019, n° 69681/13, *M. c. Roumanie*, § 45.
[25] Cour eur. D.H., arrêt du 15 octobre 2019, n° 44690/09, *Çapin c. Turquie*, § 77.
[26] *Ibid.*, § 33.
[27] *Ibid.*, § 53.

3. *Obligation de se soumettre à un test ADN*

Le prélèvement et la conservation de matériel cellulaire ainsi que l'établissement et la conservation de profils ADN sur la base de ce matériel cellulaire, constituent des ingérences dans le droit au respect de la vie privée[28].

Le respect de la vie privée exige que chacun puisse établir les détails de son identité en tant qu'être humain individuel. Le droit d'un individu à ces informations est important en raison de ses implications formatrices pour sa personnalité. Il s'agit notamment d'obtenir les informations nécessaires pour découvrir la vérité sur des aspects importants de son identité personnelle, comme l'identité de ses parents[29].

Si des enfants putatifs ont un intérêt vital à recevoir les informations nécessaires pour découvrir la vérité sur un aspect important de leur identité personnelle, il faut garder à l'esprit que la protection des tiers (comme les personnes soumises au test) peut s'opposer à ce que ceux-ci soient contraints de se soumettre à des tests médicaux de toute nature, y compris des tests ADN[30]. Même dans les litiges en matière de paternité, il faut évaluer si la procédure de prise de décision, vue globalement, est juste et fournit une protection appropriée des intérêts protégés par l'article 8[31].

Dans le contexte des tests ADN en matière de paternité, l'intérêt d'un individu à connaître sa filiation ne diminue pas avec le temps[32].

L'obligation de se soumettre à un examen médical, que ce soit dans le domaine civil ou pénal, n'est pas en soi contraire à la primauté du droit (« the rule of law »)[33].

4. *Qualité des expertises médico-légales*

Compte tenu du poids décisif que peuvent avoir les expertises médico-légales dans le cadre de procédures judiciaires qui ont trait à l'identité personnelle, il est nécessaire que ces expertises soient réalisées dans des conditions excluant l'arbitraire et assurant la confiance des justiciables dans l'action de la justice et la crédibilité du système en son ensemble. Cela n'exclut pas que les soupçons de faux portant sur de telles expertises soient vérifiés dans le cadre d'une procédure distincte, de nature pénale. En effet, la procédure pénale semble, par sa nature et par son déroulement, la plus apte à vérifier si des éléments fautifs, constitutifs d'une infraction, sont intervenus lors de la réalisation de l'expertise médico-légale. Si,

[28] Cour eur. D.H., arrêt du 29 janvier 2019, n° 62257/15, *Mifsud c. Malte*, §§ 54 et 61. La Cour a déjà jugé qu'il n'y avait pas d'ingérence lorsque la personne a donné volontairement les échantillons.
[29] *Ibid.*, § 56.
[30] *Ibid.*, § 57.
[31] *Ibid.*, § 59.
[32] *Ibid.*, § 60.
[33] *Ibid.*, § 71.

dans l'absolu, on ne saurait exclure que, par l'action délictuelle de quelqu'un ou par des épisodes de corruption, les résultats ou les modalités de réalisation de tests soient faussés, les allégations de tels agissements, lorsqu'elles sont étayées par un commencement de preuve, doivent pouvoir être soumises à l'examen efficace des tribunaux[34].

5. *Délai de prescription pour contester sa paternité*

Les procédures concernant l'établissement ou la contestation de la paternité concernent la vie privée en vertu de l'article 8, qui englobe des aspects importants de son identité personnelle[35].

Un délai de prescription rigide d'un an, ne souffrant d'aucune exception, pour introduire une procédure en contestation de paternité à partir de l'enregistrement de la naissance de l'enfant, ne peut pas être considéré comme « nécessaire dans une société démocratique » car il ne permet pas de prendre en compte les circonstances particulières de chaque cas, pas plus que de prendre en compte les souhaits des personnes concernées. Il n'y a donc pas de juste équilibre entre l'intérêt général à la protection de la sécurité juridique des relations familiales et le droit du père enregistré de voir sa paternité contestée à la lumière de preuves biologiques[36].

6. *Délai de prescription en recherche de paternité*

La Cour a déjà admis que l'introduction d'un délai pour l'introduction d'une action en paternité était justifiée par le désir d'assurer la sécurité juridique. Par conséquent, l'existence d'un délai de prescription n'est pas, en soi, incompatible avec la Convention. Ce que la Cour doit vérifier dans chaque cas d'espèce, c'est si la nature du délai en question et/ou la manière dont il est appliqué est compatible avec la Convention[37].

La Cour prend en considération un certain nombre de facteurs lorsqu'elle effectue le « test de la balance des intérêts » lors de l'examen des cas concernant les délais de prescription pour les actions en paternité. Ainsi, le moment précis où un demandeur prend conscience de la réalité biologique est pertinent. La Cour examine si les circonstances justifiant une action en paternité particulière existaient avant ou après l'expiration du délai applicable. En outre, la Cour examine s'il existe un autre type de recours lorsque le délai de prescription est écoulé. Cela vise, par exemple, l'existence de recours permettant d'obtenir une prolongation du délai ou des exceptions à l'application du délai dans les situations où une personne prend conscience de la réalité biologique après l'expiration du délai de prescrip-

[34] Cour eur. D.H., décision du 10 septembre 2019, n° 69681/13, *M. c. Roumanie*, § 46.
[35] Cour eur. D.H., arrêt du 9 juillet 2019, n° 76594/11, *Romanov c. Russie*, § 24.
[36] *Ibid.*, § 25.
[37] Cour eur. D.H., arrêt du 15 octobre 2019, n° 44690/09, *Çapin c. Turquie*, § 57.

tion. L'aune à laquelle ces facteurs sont mesurés consiste à déterminer si une présomption légale a prévalu sur la réalité biologique et sociale et, dans l'affirmative, si, dans les circonstances propres à l'espèce, cela est compatible avec l'obligation d'assurer un respect « effectif » de la vie privée et familiale, compte tenu de la marge d'appréciation laissée à l'État ainsi que des faits établis et des souhaits des personnes concernées[38].

En appliquant ces principes généraux aux affaires de paternité, la Cour a établi une distinction entre les cas où les délais mis en place pour engager une action en paternité avaient un caractère absolu et les cas où le droit interne prévoyait une prolongation des délais si des circonstances pertinentes étaient connues après leur expiration mais que les demandeurs ne pouvaient pas en bénéficier[39]. Dans le premier cas, la Cour considère qu'il y a violation de l'article 8 en raison de l'application d'un délai absolu qui a été imposé indépendamment de la connaissance par l'enfant des circonstances entourant l'identité de son père[40]. Dans le second cas, après avoir établi que les délais n'étaient pas absolus, la Cour détermine si les requérants ont agi avec une diligence suffisante pour bénéficier de la possibilité d'introduire un recours après l'expiration du délai[41].

D. Le phénomène de la « Lustration »

Les mesures de lustration qui visent à écarter des personnes liées à un régime politique antérieur (notamment aux anciens régimes communistes) concernent le droit au respect de leur vie privée, car elles affectent la réputation et/ou les perspectives professionnelles[42]. Plusieurs aspects typiques de la vie peuvent être affectés par un licenciement, une rétrogradation, une non-admission à une profession ou d'autres mesures défavorables similaires. Ces aspects concernent (i) le « cercle intime » de la personne concernée, (ii) la possibilité pour celle-ci d'établir et de développer des relations avec d'autres personnes, et (iii) la réputation sociale et professionnelle de la personne concernée. La question de la vie privée se pose généralement de deux manières : soit en raison des raisons sous-jacentes à la mesure contestée (dans ce cas, la Cour utilise l'approche fondée sur la raison), soit en raison des conséquences pour la vie privée (dans ce cas, la Cour utilise l'approche fondée sur les conséquences)[43]. Dans ce dernier cas, il faut démontrer de manière convaincante que les conséquences présentent un seuil de gravité suffisant[44] pour que l'article 8 trouve à s'appliquer.

[38] *Ibid.*, § 58.
[39] *Ibid.*, § 59.
[40] *Ibid.*, § 60.
[41] *Ibid.*, § 61.
[42] Cour eur. D.H., arrêt du 17 octobre 2019, n° 5881/15, *Polyakh et autres c. Ukraine*, § 204.
[43] *Ibid.*, § 205.
[44] *Ibid.*, § 206.

La Cour distingue différents types de « lustration »[45]. Elle rappelle qu'en tout cas, la « lustration » ne peut pas servir de punition, de châtiment ou de revanche[46].

Il faut fournir des raisons convaincantes à la Cour pour justifier un dispositif législatif de lustration qui ne se base pas sur une approche individualisée dans laquelle le comportement de chaque personne concernée fait l'objet d'une évaluation individualisée. Il faut, de plus, un contrôle parlementaire et judiciaire de ces mesures et tenir compte de la sévérité des mesures appliquées. Le cadre législatif doit être étroitement adapté pour répondre de manière proportionnée aux impératifs sociaux urgents qu'il cherche à rencontrer[47].

La Cour estime depuis longtemps que le moment de l'adoption et de la mise en œuvre des mesures de « lustration » post-communiste sont des considérations essentielles dans l'évaluation de leur proportionnalité[48].

L'un des principes clés de la jurisprudence de la Cour en matière de « lustration » est que les mesures de « lustration » sont, par nature, temporaires et que la nécessité objective de la restriction des droits individuels résultant de cette procédure diminue avec le temps[49].

E. Liberté d'expression, vie privée, réputation et honneur

1. *Protection de la réputation*

Le droit d'une personne à la protection de sa réputation est couvert par l'article 8 de la Convention en tant qu'élément du droit au respect de la vie privée[50]. La réputation d'une personne fait partie de son identité personnelle et de son intégrité morale, qui relèvent tous les deux de sa vie privée même si cette personne fait l'objet de critiques dans le cadre d'un débat public. Cependant, l'atteinte à la réputation doit atteindre un certain seuil de gravité et avoir été portée de manière à nuire à la jouissance personnelle du droit au respect de la vie privée[51].

En règle, les limites de la critique admissible sont plus larges à l'égard d'un homme politique [ou tout autre personnage public], visé en cette qualité, que d'un simple particulier. À la différence du second, le premier s'expose inévitablement et

[45] *Cfr Ibid.*, §§ 263-264.
[46] *Cfr Ibid.*, § 276 (voy. aussi le § 277).
[47] *Cfr Ibid.*, § 293.
[48] *Cfr Ibid.*, § 316.
[49] *Cfr Ibid.*, § 317.
[50] Cour eur. D.H., arrêt du 22 janvier 2019, n° 72068/10, *Taskaya et Ersoy c. Turquie*, §§ 38 et 50 ; arrêt du 19 mars 2019, n° 43624/14, *Hoiness c. Norvège*, § 63.
[51] Cour eur. D.H., arrêt du 22 janvier 2019, n° 72068/10, *Taskaya et Ersoy c. Turquie*, §§ 38 et 50 ; arrêt du 19 mars 2019, n° 43624/14, *Hoiness c. Norvège*, § 64. Voy. aussi : Cour eur. D.H., décision du 23 avril 2019, n° 58996/11, *Kwiatkowski c. Pologne*, § 32 ; arrêt du 7 mai 2019, n^{os} 11436/06 et 22912/06, *Mityanin et Leonov c. Russie*, § 112 ; décision du 14 mai 2019, n° 48174/11, *Niemczyk c. Pologne*, § 24 ; décision du 24 septembre 2019, n° 58955/13, *Vucina c. Croatie*, §§ 30-31 ; arrêt du 22 octobre 2019, n° 76969/11, *Stroea c. Roumanie*, § 24 ; décision du 22 octobre 2019, n° 74002/13, *Libicki c. Pologne*, § 39.

consciemment à un contrôle attentif de ses faits et gestes tant par les journalistes que par la masse des citoyens. Il doit, par conséquent, montrer une plus grande tolérance[52].

2. *Protection de la réputation de groupe*

Tout stéréotype négatif d'un groupe, lorsqu'il atteint un certain niveau, est susceptible d'avoir un impact sur le sentiment d'identité du groupe et sur les sentiments de valeur et de confiance en soi des membres du groupe. C'est en ce sens qu'il peut être considéré comme affectant la vie privée des membres du groupe. Des considérations similaires s'appliquent lorsqu'il s'agit de la diffamation des anciens prisonniers de Mauthausen qui, en tant que survivants de l'Holocauste, peuvent être considérés comme constituant un groupe social (fut-il hétérogène)[53].

3. *Importance de la liberté de la presse*

La liberté de la presse joue un rôle fondamental et essentiel dans le bon fonctionnement d'une société démocratique[54].

Si la presse ne doit pas franchir certaines limites, concernant notamment la protection de la réputation et des droits d'autrui, il lui incombe de communiquer, dans le respect de ses devoirs et de ses responsabilités, des informations et des idées sur toutes les questions d'intérêt général, y compris celles qui se rapportent à l'administration de la justice. La marge d'appréciation des autorités nationales se trouve ainsi circonscrite par l'intérêt d'une société démocratique à permettre à la presse de jouer son rôle indispensable de « chien de garde »[55].

4. *Obligations des journalistes*

Les journalistes doivent agir de bonne foi, sur la base de faits exacts, et fournir des informations « fiables et précises » dans le respect de l'éthique journalistique. Une certaine dose « d'exagération » ou de « provocation » est permise dans le cadre de l'exercice de la liberté journalistique[56].

Toutefois, une distorsion de la réalité, opérée de mauvaise foi, peut transgresser les limites de la critique acceptable. Ainsi, une affirmation véridique peut se doubler de remarques supplémentaires, de jugements de valeur, de suppositions, voire d'insinuations, susceptibles de créer une image erronée aux yeux du public.

---

[52] Cour eur. D.H., décision du 23 avril 2019, n° 58996/11, *Kwiatkowski c. Pologne*, § 39 ; décision du 22 octobre 2019, n° 74002/13, *Libicki c. Pologne*, § 43. Pour un exemple de personnage public, voy. : la décision du 14 mai 2019 (n° 48174/11, *Niemczyk c. Pologne*, §§ 27-28).
[53] Cour eur. D.H., arrêt du 10 octobre 2019, n° 4782/18, *Lewit c. Autriche*, § 46.
[54] Cour eur. D.H., arrêt du 22 janvier 2019, n° 72068/10, *Taskaya et Ersoy c. Turquie*, § 51.
[55] *Ibid.*, § 51.
[56] *Ibid.*, § 51.

Or, la mission d'information comporte nécessairement des devoirs, des responsabilités et des limites que les organes de presse doivent s'imposer spontanément. C'est particulièrement le cas lorsque le récit médiatique tend à imputer des faits d'une particulière gravité à des personnes nommément citées, une telle imputation comportant le risque de désigner ces personnes à la vindicte populaire[57].

En principe, la presse devrait pouvoir s'appuyer, en toute bonne foi, sur le contenu des rapports officiels sans avoir à entreprendre des recherches indépendantes[58]. Cela signifie que les journalistes doivent être libres de rendre compte des événements sur la base d'informations recueillies auprès de sources officielles sans autre vérification, notamment en ce qui concerne la véracité des faits présentés dans le document officiel. Cela vaut aussi pour les informations données oralement par un procureur chargé des relations avec la presse, constituant ainsi une base factuelle suffisante pour un article « fondé » sur ces informations[59].

Lorsqu'une photographie publiée dans le cadre d'un reportage sur une procédure pénale en cours n'a pas de valeur informative en soi, il doit y avoir des raisons impérieuses capables de justifier une atteinte au droit du défendeur au respect de sa vie privée. Les éléments suivants doivent être pris en compte : la position de la personne concernée, la position du journal ainsi que la nature et le sujet de l'article [60].

5. *Distinction entre déclarations de fait et jugements de valeur*

La Cour rappelle la distinction qu'elle opère entre déclarations de fait et jugements de valeur. La matérialité des déclarations de fait peut se prouver. Par contre, les jugements de valeur ne se prêtent pas à une démonstration de leur exactitude. En conséquence, l'obligation de les prouver est impossible à remplir. Imposer pareille preuve porte atteinte à la liberté d'opinion. Toutefois, ce n'est pas pour cela que les jugements de valeur seraient immunisés de toute limite. Ainsi, en cas de jugement de valeur, la proportionnalité de l'ingérence dépend de l'existence d'une « base factuelle » suffisante sur laquelle reposent les propos litigieux. À défaut, le jugement de valeur pourrait se révéler être excessif. Pour distinguer une imputation de fait d'un jugement de valeur, il faut tenir compte des circonstances de l'espèce et de la tonalité générale des propos, étant entendu que des assertions sur des questions d'intérêt public peuvent constituer à ce titre des jugements de valeur plutôt que des déclarations de fait[61].

[57] *Ibid.*, § 52.
[58] Cour eur. D.H., arrêt du 7 mai 2019, n^os^ 11436/06 et 22912/06, *Mityanin et Leonov c. Russie*, § 109.
[59] *Ibid.*, § 109.
[60] *Ibid.*, § 110.
[61] Cour eur. D.H., arrêt du 22 janvier 2019, n° 72068/10, *Taskaya et Ersoy c. Turquie*, § 53. Voy. aussi : Cour eur. D.H., décision du 14 mai 2019, n° 48174/11, *Niemczyk c. Pologne*, § 30.

6. *Critères à prendre en considération lors de la mise en balance des droits en présence*

Les critères pertinents pour apprécier la mise en balance du droit au respect de la vie privée et du droit à la liberté d'expression, sont les suivants :

- la contribution à un débat d'intérêt général ;
- la notoriété de la personne visée ;
- l'objet du reportage ;
- le comportement antérieur de la personne concernée ;
- le contenu, la forme et les répercussions de la publication ;
- ainsi que, le cas échéant, les circonstances de l'espèce.

La Cour rappelle à cet égard que si la mise en balance entre ces deux droits s'est faite dans le respect de ces critères, il faut des raisons sérieuses pour que celle-ci substitue son avis à celui des juridictions nationales[62].

D'autres aspects liés à la liberté d'expression peuvent être pertinents en ce qui concerne les sites en ligne, comme[63] :

- le contexte dans lequel les commentaires ont été formulés ;
- les mesures appliquées par le site pour prévenir ou enlever les commentaires diffamants ;
- la responsabilité des auteurs des commentaires comme alternative à la responsabilité de l'intermédiaire ;
- et les conséquences des procédures pour le site.

Dans l'affaire *Hoiness*, la Cour a pris en compte le fait que les forums du site n'étaient pas intégrés dans la présentation des informations sur le site et ne s'inscrivaient donc pas dans la ligne éditoriale du site[64]. Au contraire, il y avait des modérateurs qui contrôlaient le contenu des forums et les participants aux forums pouvaient cliquer sur un bouton pour notifier leurs réactions aux commentaires. De plus, le site pouvait aussi intervenir par voie d'email[65].

[62] Cour eur. D.H., arrêt du 22 janvier 2019, n° 72068/10, *Taskaya et Ersoy c. Turquie*, § 54 ; arrêt du 22 octobre 2019, n° 76969/11, *Stroea c. Roumanie*, §§ 26-27. Voy. aussi la mise en œuvre de ces critères dans la décision du 24 septembre 2019 (n° 58955/13, *Vucina c. Croatie*) et dans l'arrêt du 22 octobre 2019 (n° 76969/11, *Stroea c. Roumanie*, §§ 28 et s.). Pour un exemple de non-respect de mise en œuvre de ces critères, voy. : Cour eur. D.H., arrêt du 7 mai 2019, n° 30669/11, *Kavak c. Turquie*.
[63] Cour eur. D.H., arrêt du 19 mars 2019, n° 43624/14, *Hoiness c. Norvège*, § 67.
[64] *Ibid.*, § 71.
[65] *Ibid.*, § 72. Voy. le § 73.

7. *Publication de photographies concernant un personnage public*

La vie privée comprend les informations personnelles dont un individu peut légitimement s'attendre à ce qu'elles ne soient pas publiées sans son consentement, notamment la publication de photos[66].

Les critères pertinents pour la mise en balance du droit au respect de la vie privée et du droit à la liberté d'expression sont les mêmes[67] :

- la contribution à un débat d'intérêt général ;
- la notoriété de la personne visée ;
- l'objet du reportage ;
- le comportement antérieur de la personne vis-à-vis des médias ;
- le contenu, la forme et les répercussions de la publication ;
- et, en ce qui concerne des photos, les circonstances de leur prise.

C'est aux journalistes qu'il appartient de décider s'il est nécessaire ou non de reproduire le support de leurs informations pour en assurer la crédibilité, étant entendu que le lien entre la photo et l'article ne doit pas être ténu, artificiel ou arbitraire[68].

Un personnage public d'une notoriété certaine ne peut pas prétendre de la même manière à une protection de son droit à la vie privée qu'une personne privée inconnue du public[69].

F. Protection des communications et harcèlement

L'envoi et la réception de communications sont couverts par la notion de correspondance. Tant les communications depuis le lieu de travail que depuis le domicile sont couvertes par les notions de vie privée et de correspondance. Afin de savoir si les notions de vie privée et de correspondance s'appliquent, la Cour a examiné à plusieurs occasions la question de savoir si la personne concernée pouvait se prévaloir d'une attente raisonnable que sa vie privée serait respectée et protégée, tout en rappelant qu'il s'agissait d'un élément significatif mais pas nécessairement décisif[70].

Ce n'est pas parce qu'un email concerne à la fois des questions professionnelles et privées ou qu'il a été envoyé depuis une adresse électronique professionnelle que

66 Cour eur. D.H., décision du 25 juin 2019, nº 14047/16, *Guttenberg c. Allemagne*, § 24.
67 *Ibid.*, § 26.
68 *Ibid.*, § 27.
69 *Ibid.*, § 28.
70 Cour eur. D.H., décision du 14 mai 2020, nº 70573/17, *Garamukanwa c. Royaume-Uni*, § 22.

cela signifie automatiquement que cet email tombe en dehors du champ d'application de la vie privée[71].

À partir du moment où un individu était au courant qu'un de ses collègues de travail l'accusait de harcèlement et au vu des circonstances propres à la cause, cet individu ne pouvait pas raisonnablement s'attendre à ce que des communications postérieures à ce moment demeureraient privées, d'autant qu'il n'avait jamais contesté l'utilisation de ces communications durant les procédures disciplinaires et qu'il avait lui-même fourni des communications privées aux instances disciplinaires[72].

G. Conservation de données par la police

La simple conservation de données (ici des données à caractère personnel) constitue une ingérence dans le droit au respect de la vie privée des requérants[73].

Pour être prévue par la loi, la mesure contestée doit avoir un certain fondement en droit interne. Mais, de plus, la loi en question doit présenter certaines qualités : être accessible à la personne concernée et prévisible quant à ses effets. Le droit interne doit donc offrir une protection juridique adéquate contre l'arbitraire et, en conséquence, indiquer avec suffisamment de clarté la portée et le pouvoir discrétionnaire conféré aux autorités compétentes et les modalités de son exercice[74].

La Cour rappelle que des questions de protection des données peuvent se poser à différents moments importants, notamment durant la collecte, la conservation, l'utilisation et la communication des données[75].

À propos de la collecte de données par la police, la Cour a relevé les éléments suivants dans l'affaire *Catt c. Royaume-Uni*[76] :

1° il est difficile de déterminer l'étendue exacte et le contenu des données collectées et rassemblées pour constituer la base de données mais il était possible de savoir que la police possédait pareille base de données ;
2° la collecte de données n'a pas une base légale claire et cohérente[77].

[71] *Ibid.*, § 25.
[72] *Ibid.*, §§ 23-29. Il ne faut pas voir dans cette décision une quelconque diminution de la protection des communications électroniques par rapport aux décisions antérieures et qui sont reprises dans les chroniques précédentes en la matière.
[73] Cour eur. D.H., arrêt du 24 janvier 2019, n° 43514/15, *Catt c. Royaume-Uni*, § 93.
[74] *Ibid.*, § 94.
[75] *Ibid.*, § 95.
[76] *Ibid.*, §§ 98-99.
[77] Voy. aussi le § 105 de l'arrêt du 24 janvier 2019 (n° 43514/15, *Catt c. Royaume-Uni*).

Toutefois, la Cour a considéré que le cadre régissant la collecte des données de la personne concernée ne pouvait pas être considéré indépendamment des dispositions régissant la conservation et l'utilisation des données à caractère personnel[78].

À propos de la conservation et de l'utilisation des données, la Cour a relevé la définition très lâche de la finalité poursuivie (en l'espèce, l'extrémisme national) et le fait que les données du requérant pouvaient être potentiellement conservées indéfiniment. Elle a toutefois relevé que les données ne seraient pas communiquées à des parties tierces et que le requérant avait la possibilité d'introduire une requête en vue de l'effacement des données[79]. En conséquence, la question de savoir si la collecte, la conservation et l'utilisation des données à caractère personnel du requérant étaient prévues par la loi était étroitement liée à la question plus large de savoir si l'ingérence était nécessaire dans une société démocratique[80].

Pour rappel, l'ingérence dans le droit au respect de la vie privée est nécessaire dans une société démocratique si elle répond à un besoin social impérieux, si elle est proportionnée au but légitime poursuivi et si les raisons invoquées par les autorités nationales pour la justifier sont pertinentes et suffisantes, étant entendu que les autorités nationales compétentes disposent d'une marge d'appréciation à cet égard[81].

La Cour rappelle également l'importance d'examiner le respect des principes de l'article 8 lorsque les pouvoirs conférés à l'État sont obscurs, ce qui crée un risque d'arbitraire, surtout lorsque la technologie disponible est de plus en plus sophistiquée[82].

En l'espèce, la Cour est d'accord avec le fait qu'il est inhérent à la nature de la collecte d'informations par la police que celle-ci collecte en premier les données avant de pouvoir en évaluer l'intérêt[83]. En l'espèce, la Cour a considéré que la collecte de données était justifiée dès lors que le requérant s'était publiquement et de manière répétée aligné sur les activités d'un groupe de protestations violent (et potentiellement criminel) que la police devait contrôler[84]. Par contre, la Cour a considéré qu'il n'y avait pas de besoin social impérieux à conserver les données du requérant, même si elle est d'accord qu'il faut être prudent avant de se substituer à la police dans l'évaluation des informations susceptibles de les aider dans la réalisation de ses missions[85]. En l'espèce, la Cour a souligné le fait qu'elle ne remettait pas en question le fait qu'il ait pu y avoir un besoin social impérieux de conserver les données du requérant. Toutefois, elle a noté qu'en l'absence de règle fixant un délai maximum de conservation, le requérant dépendait totalement de

[78] Cour eur. D.H., arrêt du 24 janvier 2019, n° 43514/15, *Catt c. Royaume-Uni,* § 99.
[79] *Ibid.*, § 105.
[80] *Ibid.*, § 106.
[81] *Ibid.*, § 109.
[82] *Ibid.*, § 114.
[83] *Ibid.*, § 117.
[84] *Ibid.*, § 118.
[85] *Ibid.*, § 119.

l'application des garanties très souples visant à assurer la conservation proportionnée de ses données. La Cour a noté que lorsqu'un État choisissait de mettre en place pareil système, le besoin de garanties procédurales effectives devenait un élément décisif dans son appréciation. Ces garanties procédurales doivent permettre l'effacement de ces données une fois que leur conservation devient disproportionnée[86].

À cet égard, la Cour a notamment relevé que la décision de conserver les données du requérant n'avait pas pris en compte le fait qu'il s'agissait de données sensibles qui requéraient, de ce fait, une protection plus élevée et que, dans le cas présent, la conservation de ces données devait avoir eu un effet dissuasif pour la personne concernée[87].

Enfin, la Cour a indiqué qu'il serait totalement contraire au besoin de protéger la vie privée si le Gouvernement du Royaume-Uni pouvait créer une base de données de manière telle qu'il ne serait pas possible de la contrôler ou de la modifier facilement et de s'en prévaloir pour justifier un refus d'effacer une information de cette base de données[88].

H. Protection des données saisies lors de perquisitions chez des avocats

Les saisies opérées dans les bureaux ou les cabinets d'avocats s'analysent en une ingérence dans le droit au respect du domicile et de la correspondance, tel que celui-ci est protégé par l'article 8 de la Convention. De plus, le terme « correspondance » recouvre aussi les disques durs informatiques et les données électroniques, fichiers informatiques et messagerie d'un cabinet d'avocats[89].

La conservation d'une copie des données électroniques saisies dans le cabinet d'avocats des requérants constitue en soi une ingérence dans les relations de ceux-ci avec leurs clients, alors même que cette relation est protégée par le secret professionnel. Il n'est pas nécessaire que les données soient déchiffrées, transcrites et officiellement attribuées aux requérants pour qu'il y ait ingérence. En vérité, il n'y a plus de secret professionnel qui tienne lorsque les autorités publiques demeurent en possession d'une copie de données protégées par le secret professionnel[90].

Une ingérence ne saurait passer pour « prévue par la loi » que si, d'abord, elle a une base en droit interne. Dans un domaine couvert par le droit écrit (tel que dans le cas d'espèce), la « loi » est le texte en vigueur tel que les juridictions compé-

[86] *Ibid.*, § 119.
[87] *Ibid.*, § 123.
[88] *Ibid.*, § 127.
[89] Cour eur. D.H., arrêt du 3 décembre 2019, n° 14704/12, *Kirdök et autres c. Turquie*, § 34.
[90] *Ibid.*, § 36.

tentes l'ont interprété. Les mots « prévue par la loi » ont aussi trait à la qualité de la loi en question : ils exigent l'accessibilité de celle-ci aux personnes concernées et une formulation assez précise pour leur permettre en s'entourant, au besoin, de conseils éclairés, de prévoir, à un degré raisonnable dans les circonstances de la cause, les conséquences pouvant résulter d'un acte déterminé et de régler leur conduite. Cette expression implique donc notamment que la législation interne doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à recourir à des mesures affectant leurs droits protégés par la Convention[91].

Les mesures imposant aux avocats un certain nombre d'obligations susceptibles de concerner les relations avec leurs clients, par exemple dans le cadre de la lutte contre les infractions pénales, doivent être impérativement encadrées d'une façon stricte, les avocats occupant une situation centrale dans l'administration de la justice[92].

Quant au cas particulier des saisies opérées dans le cabinet d'un avocat, la Cour rappelle qu'elles doivent impérativement être assorties de garanties spéciales de procédure, puisque ces saisies portent incontestablement atteinte au secret professionnel, qui est la base de la relation de confiance qui existe entre l'avocat et son client. D'ailleurs, la protection du secret professionnel fait partie des droits de la défense au sens de l'article 6 de la Convention. Elle est notamment le corollaire du droit qu'a le client d'un avocat de ne pas contribuer à sa propre incrimination, ce qui présuppose que les autorités cherchent à fonder leur argumentation sans recourir à des éléments de preuve obtenus par la contrainte ou les pressions, au mépris de la volonté de l'« accusé »[93].

En ce qui concernent les garanties spéciales de procédure devant être assorties à ces mesures de saisie chez un avocat, la Cour rappelle en premier lieu qu'elles doivent être encadrées par des règles prévisibles particulièrement claires et précises quant à leur adoption et leur mise en application. La Cour rappelle en deuxième lieu que ces mesures doivent faire l'objet d'un contrôle particulièrement rigoureux. Surtout, la législation et la pratique doivent offrir des garanties adéquates et suffisantes contre les abus et l'arbitraire. Saisi d'allégations motivées selon lesquelles des documents précisément identifiés avaient été saisis alors qu'ils relevaient de la confidentialité avocat-client, le juge doit effectuer un « contrôle concret de proportionnalité » et ordonner, le cas échéant, leur restitution[94].

[91] *Ibid.*, § 43.
[92] *Ibid.*, § 49.
[93] *Ibid.*, § 50.
[94] *Ibid.*, § 51.

En l'espèce, la Cour a retenu notamment les éléments suivants[95] :

1° Les requérants, avocats, n'étaient pas visés par l'enquête pénale ; ils partageaient leur bureau avec un autre avocat qui faisait l'objet des poursuites pénales dans le cadre desquelles la perquisition avait été ordonnée.
2° Les requérants avaient fait valoir devant les autorités judiciaires que les données électroniques saisies lors de cette perquisition, à savoir celles sur le disque dur de l'ordinateur de bureau et sur la clé USB, leur appartenaient et relevaient de leur secret professionnel entre avocats et clients.
3° Dans l'ordonnance de perquisition, le juge avait indiqué d'une façon large l'étendue des perquisitions, en énonçant le but de cette opération comme « recueillir les éléments de preuve et saisir les objets » qui pourraient montrer que le suspect menait des activités au sein de l'organisation terroriste KCK/PKK.
4° Cette ordonnance ne précisait pas quels objets ou documents concrets ou spécifiques devraient être trouvés aux adresses mentionnées, y compris au cabinet d'avocats des requérants, ni comment ces éléments seraient pertinents pour l'enquête pénale concernée. L'ordonnance en question a ainsi permis aux autorités chargées de l'enquête d'examiner, en termes généraux, toutes les données électroniques se trouvant dans les bureaux des requérants, sans tenir spécialement compte qu'il s'agissait d'un cabinet d'avocats et qu'il pourrait y avoir des documents déposés par les clients à leurs conseils.
5° L'ampleur large de l'ordonnance s'est reflétée dans la manière dont elle a été exécutée. Bien qu'un représentant du barreau d'Istanbul et l'une des requérants aient assisté à la perquisition et que les données saisies aient été placées dans un sac scellé, aucune autre mesure de protection spéciale n'était en place contre l'ingérence dans le secret professionnel. En effet, aucune procédure de filtrage des documents ou des données électroniques protégés par le secret professionnel ne semble avoir été suivie et/ou aucune interdiction explicite de saisir des données protégées par ce secret n'a été imposée pendant la perquisition en cause. Au contraire, l'ensemble des données se trouvant sur le disque dur de l'ordinateur utilisé conjointement par les avocats qui partageaient les locaux ainsi que sur une clé USB ont été saisies.
6° Une fois le secret professionnel des relations avocats-clients invoqué et le retour des données électroniques saisies demandé, la loi imposait aux autorités judiciaires une obligation de procéder rapidement à un examen des données saisies et, le cas échéant, de restituer aux requérants ou de détruire les données protégées par ce secret. Cependant, la législation et la pratique du droit national n'étaient pas claires sur les conséquences attribuées à un éventuel manquement par les autorités judiciaires à cette obligation.
7° La cour d'assises a définitivement refusé la restitution ou la destruction des copies saisies des données en cause, avec une motivation mentionnant seulement la régularité des actes de perquisition effectués dans les bureaux, en laissant sans réponse l'allégation spécifique d'une atteinte à la confidentialité des

[95] *Ibid.*, §§ 52-57.

relations avocats-clients. Il ressort du dossier que la cour d'assises aurait implicitement accepté les raisons soulevées par le parquet pour justifier le refus du retour des données saisies, à savoir que ces données n'étant pas encore transcrites, on ne pouvait pas savoir à qui elles appartenaient exactement. La Cour considère qu'un tel motif de rejet n'est non seulement pas clairement prévu par la loi, mais s'avère également contraire à l'essence du secret professionnel protégeant les relations avocats-clients. En tout état de cause, on ne saurait conclure que l'examen de la demande des requérants par les autorités judiciaires ait été en conformité avec l'obligation d'assurer un contrôle particulièrement rigoureux des mesures concernant des données relevant du secret professionnel des avocats.

8° Un recours en mise en cause de la responsabilité de l'État, de nature indemnitaire, se distingue clairement d'un recours en nullité d'une saisie litigieuse et, partant, il n'aurait pas été de nature à permettre le retour ou la destruction des copies relevant du secret professionnel, tels que recherchés par les requérants, de sorte que l'on ne peut y voir un « contrôle efficace » au sens de l'article 8.

Il y a donc eu violation de l'article 8, les mesures imposées aux requérants quant à la saisie de leurs données électroniques et au refus de les restituer ou de les détruire n'ayant répondu à aucun besoin social impérieux. En tout état de cause, ces mesures n'étaient pas proportionnées aux buts légitimes visés et, de ce fait, elles n'étaient pas nécessaires dans une société démocratique[96].

I. Protection contre les mesures de surveillance

1. *Mesures de surveillance secrète – Écoutes téléphoniques*

Les conversations téléphoniques sont couvertes par les notions de vie privée et de correspondance et leur surveillance constitue une ingérence dans l'exercice des droits protégés par l'article 8[97].

Dans le cadre de mesures secrètes de surveillance telles que l'interception des communications, l'exigence de prévisibilité de la loi ne signifie pas qu'un individu doit être en mesure de prévoir quand les autorités sont susceptibles d'intercepter ses communications afin qu'il puisse adapter sa conduite en conséquence. Toutefois, lorsqu'un pouvoir exécutif est exercé en secret, les risques d'arbitraire sont évidents. Dès lors, le droit interne doit être suffisamment clair afin de donner aux individus une indication adéquate quant aux circonstances et aux conditions dans lesquelles ces autorités publiques sont habilitées à recourir à de telles mesures[98].

[96] *Ibid.*, § 58 (la Cour a donc souligné l'absence de garanties procédurales suffisantes dans la loi telle qu'interprétée et appliquée par les autorités judiciaires dans le cas d'espèce).
[97] Cour eur. D.H., arrêt du 28 mai 2019, n° 173/15, *Liblik et autre c. Estonie*, § 125.
[98] *Ibid.*, § 128.

En outre, étant donné que la mise en œuvre pratique des mesures de surveillance secrète des communications n'est pas soumise au contrôle des personnes concernées ni à celui du grand public, il serait contraire au principe de la primauté du droit que le pouvoir discrétionnaire accordé à l'exécutif ou au juge soit exprimé en termes de pouvoir illimité. Par conséquent, la loi doit indiquer l'étendue de ce pouvoir discrétionnaire conféré aux autorités compétentes et les modalités de son exercice avec suffisamment de clarté pour donner à l'individu une protection adéquate contre toute ingérence arbitraire[99].

À cet égard, la Cour a souligné la nécessité de prévoir des garanties. Compte tenu du risque qu'un système de surveillance secrète pour la protection de la sécurité nationale puisse saper ou même détruire la démocratie sous le couvert de la défendre, la Cour doit être convaincue qu'il existe des garanties contre les abus qui soient adéquates et efficaces[100].

Cette évaluation dépend de toutes les circonstances de l'affaire, tels que la nature, la portée et la durée des mesures possibles, les motifs requis pour les ordonner, les autorités compétentes pour les autoriser, les exécuter et les superviser, ainsi que le type de recours prévu par le droit national[101].

L'examen et la supervision des mesures de surveillance secrètes peuvent intervenir à trois stades : lorsque la surveillance est ordonnée pour la première fois, lorsqu'elle est en cours d'exécution ou après qu'elle ait pris fin. En ce qui concerne les deux premiers stades, la nature même et la logique de la surveillance secrète imposent que la surveillance elle-même ainsi que son contrôle, soient effectués à l'insu de la personne concernée. Par conséquent, puisque l'individu sera nécessairement empêché d'introduire un recours efficace de sa propre initiative ou de participer directement aux procédures de contrôle, il est essentiel que les procédures établies fournissent elles-mêmes des garanties adéquates et équivalentes pour la sauvegarde des droits de la personne surveillée[102].

La Cour a souligné l'importance que l'autorité habilitée à autoriser la surveillance secrète puisse vérifier s'il existe des soupçons raisonnables contre la personne concernée et, en particulier, s'il existe des indices concrets qui permettent de suspecter cette personne de planifier, de commettre ou d'avoir commis des actes criminels ou d'autres actes, et qui peuvent donner lieu à des mesures de surveillance secrètes. Cette autorité doit aussi pouvoir vérifier si la mesure est nécessaire dans une société démocratique (ce qui renvoie principalement au test de proportionnalité), autrement dit de voir si l'objectif ne peut pas être atteint par des moyens moins invasifs[103].

---

[99] *Ibid.*, § 129.
[100] *Ibid.*, § 130.
[101] *Ibid.*, § 130 ; arrêt du 5 décembre 2019, n° 43478/11, *Hambardzumyan c. Arménie*, § 61.
[102] Cour eur. D.H., arrêt du 28 mai 2019, n° 173/15, *Liblik et autre c. Estonie*, § 130.
[103] *Ibid.*, § 136.

Cette vérification, ainsi que l'obligation d'exposer les motifs pertinents dans les décisions par lesquelles la surveillance secrète est autorisée, constituent une garantie importante qui assure que les mesures n'ont pas été ordonnées au hasard, de manière irrégulière ou sans un examen approprié[104].

En ce qui concerne la pratique consistant à valider rétroactivement la mesure de surveillance, la Cour constate que la protection garantie par un examen préalable du recours à la mesure de surveillance secrète n'est pas nécessairement la même que celle fournie par un examen *a posteriori*[105].

2. *Surveillance téléphonique – autorisation judiciaire*

La Cour a rappelé que l'absence de motivation de l'ordonnance d'un juge d'instruction (à laquelle s'ajoute la pratique qui consiste à contourner ce manquement en fournissant une justification rétrospective du recours à la surveillance secrète), n'était pas conforme au droit interne applicable et ne fournissait pas des garanties suffisantes contre d'éventuels abus. De telles pratiques ne sont pas compatibles avec l'exigence de légalité, ni suffisantes pour maintenir l'ingérence dans le droit du requérant au respect de sa vie privée et de sa correspondance à ce qui est « nécessaire dans une société démocratique »[106].

La surveillance secrète constituant une grave ingérence dans le droit au respect de la vie privée, l'autorisation judiciaire ne peut pas être rédigée en des termes si vagues qu'elle laisse place à des spéculations et des hypothèses quant à son contenu et, surtout, quant à la personne à l'égard de laquelle la mesure donnée est appliquée[107].

3. *Divulgation à la presse d'extraits d'écoutes téléphoniques*

Les conversations téléphoniques sont couvertes par les notions de « vie privée » et de « correspondance »[108].

S'agissant de la publication d'extraits d'écoutes téléphoniques dans la presse à propos d'une affaire criminelle qui avait retenu l'attention des médias, la Cour rappelle que l'intérêt public à recevoir des informations ne concerne que les faits en lien avec les charges criminelles en cause[109].

---

[104] *Ibid.*, § 136. Pour un exemple de motivation insuffisante, voy. : Cour eur. D.H., arrêt du 6 juin 2019, n° 40429/14, *Bosak et autres c. Croatie*, §§ 45-47.
[105] Cour eur. D.H., arrêt du 28 mai 2019, n° 173/15, *Liblik et autre c. Estonie*, § 141.
[106] Cour eur. D.H., décision du 22 janvier 2019, n^{os} 14590/15 et 25405/15, *S. Ringwald c. Croatie* et *V. Ringwald c. Croatie*, § 33.
[107] Cour eur. D.H., arrêt du 5 décembre 2019, n° 43478/11, *Hambardzumyan c. Arménie*, § 65.
[108] Cour eur. D.H., décision du 19 novembre 2019, n° 39273/07, *Man et autres c. Roumanie*, § 103.
[109] *Ibid.*, § 104.

4. *Conservation dans des archives secrètes d'informations obtenues par des mesures de surveillance secrète*

Le simple fait de mémoriser dans un registre secret des données relatives à la vie privée d'un individu constitue une ingérence, peu importe que les informations mémorisées fussent ou non utilisées par la suite. De même, la collecte et la conservation systématiques d'informations par des services de sécurité sur certains individus, même sans recours à des méthodes de surveillance secrète, constituent une ingérence dans la vie privée de ces personnes[110].

La conservation dans des archives secrètes de données collectées au moyen d'écoutes de communications téléphoniques privées révélant des informations sur la conduite des requérants et qui leur ont valu d'être poursuivis par les autorités du parquet et les instances disciplinaires du parquet, constitue une ingérence dans leur droit au respect de la vie privée[111].

En ce qui concerne la proportionnalité de la mesure, la Cour a pris en compte le fait que les conditions dans lesquelles les données avaient été conservées [dans des archives secrètes] visait à préserver leur confidentialité et à garantir leur protection contre tout accès non autorisé[112]. La Cour a ensuite pris en compte le fait que l'utilisation des données était prohibée par la loi et que c'est pour cette raison qu'elles avaient été écartées des procédures[113]. Enfin, la Cour a constaté que la durée de conservation légale avait été respectée et que les données qui perdaient leur utilité pouvaient être supprimées des archives secrètes à la demande des personnes concernées[114].

5. *Surveillance sur le lieu du travail*

Dans un arrêt du 17 octobre 2019, la Grande Chambre a revu l'affaire *Lopez Ribalda et autres c. Espagne* qui concerne la surveillance de travailleurs à l'aide de caméras cachées.

La Cour a d'abord rappelé que la notion de « vie privée » était une notion large, qui ne se prêtait pas à une définition exhaustive ; elle recouvre l'intégrité physique et morale d'une personne ainsi que de multiples aspects de son identité physique et sociale. Elle englobe notamment des éléments d'identification d'un individu tels que son nom ou sa photographie[115].

La Cour poursuit en rappelant que la notion de vie privée ne se limite pas à un « cercle intime », où chacun peut mener sa vie personnelle sans intervention exté-

[110] Cour eur. D.H., décision du 18 juin 2019, n° 45501/08, *Kumpialowska c. Pologne*, § 41.
[111] *Ibid.*, § 42.
[112] *Ibid.*, § 46.
[113] *Ibid.*, § 47.
[114] *Ibid.*, § 48.
[115] Cour eur. D.H. (GC), arrêt du 17 octobre 2019, n^{os} 1874/13 et 8567/13, *Lopez Ribalda et autres c. Espagne*, § 87.

rieure, mais qu'elle englobe également le droit de mener une « vie privée sociale », à savoir la possibilité pour l'individu de nouer et de développer des relations avec ses semblables et le monde extérieur. À ce titre, la Cour n'exclut pas les activités professionnelles pas plus que les activités qui ont lieu dans un contexte public. Il existe en effet une zone d'interaction entre l'individu et autrui qui, même dans un contexte public, peut relever de la vie privée[116].

Un certain nombre d'éléments entrent en ligne de compte lorsqu'il s'agit de déterminer si la vie privée d'une personne est touchée par des mesures prises en dehors de son domicile ou de ses locaux privés. Puisqu'à certaines occasions les gens se livrent sciemment ou intentionnellement à des activités qui sont ou peuvent être enregistrées ou rapportées publiquement, ce qu'un individu est raisonnablement en droit d'attendre quant au respect de sa vie privée peut constituer un facteur significatif, quoique pas nécessairement décisif[117].

S'agissant de la surveillance des actions d'un individu au moyen de matériel photo ou vidéo, la surveillance des faits et gestes d'une personne dans un lieu public au moyen d'un dispositif photographique ne mémorisant pas les données visuelles ne constitue pas en elle-même une forme d'ingérence dans la vie privée. En revanche, des considérations tenant à la vie privée peuvent surgir dès lors que des données à caractère personnel, notamment les images d'une personne identifiée, sont recueillies et enregistrées de manière systématique ou permanente. Comme la Cour l'a rappelé, l'image d'un individu est l'un des attributs principaux de sa personnalité, parce qu'elle exprime son originalité et lui permet de se différencier de ses pairs. Le droit de chacun à la protection de son image constitue ainsi l'une des conditions essentielles de son épanouissement personnel et présuppose principalement la maîtrise par l'individu de son image. Si pareille maîtrise implique dans la plupart des cas la possibilité pour l'individu de refuser la diffusion de son image, elle comprend en même temps le droit pour lui de s'opposer à la captation, la conservation et la reproduction de celle-ci par autrui[118].

Pour déterminer si l'article 8 trouve à s'appliquer, il faut aussi regarder si la personne concernée a été ciblée par la mesure de surveillance ou si des informations à caractère personnel ont été traitées, utilisées ou rendues publiques d'une manière ou dans une mesure excédant ce à quoi elle pouvait raisonnablement s'attendre[119].

En ce qui concerne plus particulièrement la vidéosurveillance sur le lieu de travail, la Cour a rappelé que la vidéosurveillance effectuée par l'employeur à l'insu d'une salariée, pendant environ cinquante heures sur une période de deux semaines, et l'utilisation de l'enregistrement obtenu dans la procédure devant les juridictions

116 *Ibid.*, § 88.
117 *Ibid.*, § 89.
118 *Ibid.*, § 89.
119 *Ibid.*, § 90.

du travail pour justifier son licenciement, constituaient une atteinte au droit au respect de la vie privée. La Cour a aussi rappelé que la vidéosurveillance non dissimulée de professeurs d'université pendant qu'ils dispensaient leurs cours, dont les enregistrements étaient conservés pendant un mois et consultables par le doyen de la faculté, a également été jugée attentatoire à la vie privée[120].

En l'espèce les requérantes avaient fait l'objet d'une vidéosurveillance mise en place par leur employeur sur leur lieu de travail pendant une durée de dix jours et dirigée vers les caisses du supermarché et leurs alentours. Ainsi, si les requérantes n'étaient pas individuellement ciblées par la vidéosurveillance, il n'est pas contesté que les trois premières d'entre elles, qui travaillaient aux caisses, ont pu être filmées tout le long de leur journée de travail, alors que les quatrième et cinquième requérantes l'ont été au moment où elles y passaient[121].

S'agissant de l'attente raisonnable que les requérantes pouvaient avoir concernant la protection et le respect de leur vie privée, la Cour relève que leur lieu de travail, un supermarché, était ouvert au public et que les activités filmées, à savoir l'encaissement des achats effectués par les clients, n'étaient pas de nature intime ou privée. La Cour considère que l'attente qu'elles pouvaient avoir, s'agissant de la protection de leur vie privée, était donc nécessairement réduite. Cependant, même dans des espaces publics, la création d'un enregistrement systématique ou permanent d'images de personnes identifiées et le traitement subséquent des images ainsi recueillies peut soulever des questions touchant à la vie privée des individus concernés. La Cour relève à cet égard que le droit interne prévoyait un cadre légal explicite qui obligeait le responsable d'un système de vidéosurveillance, même situé dans un espace public, à avertir au préalable les personnes faisant l'objet d'une telle surveillance. Les requérantes avaient au demeurant été informées de l'installation par leur employeur d'autres caméras (celles-ci visibles) et qui étaient dirigées vers les entrées et sorties du magasin. Dans ces circonstances, la Cour a considéré que les requérantes pouvaient raisonnablement s'attendre à ne pas faire l'objet d'une vidéosurveillance dans les autres espaces du magasin sans en avoir été préalablement informées[122].

En ce qui concerne le traitement et l'utilisation des enregistrements vidéo, la Cour note que ceux-ci ont été visionnés par plusieurs personnes travaillant pour l'employeur des requérantes, avant même que ces dernières ne soient informées de leur existence. En outre, ces enregistrements ont servi de base au licenciement des requérantes et ils ont été utilisés comme moyens de preuve dans la procédure devant le juge du travail[123].

120 *Ibid.*, § 91.
121 *Ibid.*, § 92.
122 *Ibid.*, § 93.
123 *Ibid.*, § 94.

S'agissant de la surveillance des employés sur le lieu de travail, la Cour estime que l'article 8 laissait à l'appréciation des États le choix d'adopter ou non une législation spécifique concernant la vidéosurveillance ou la surveillance de la correspondance et des communications non professionnelles des travailleurs. Elle rappelle néanmoins que, quelle que soit la latitude dont jouissent les États dans le choix des moyens propres à protéger les droits en cause, les juridictions internes doivent s'assurer que la mise en place par un employeur de mesures de surveillance portant atteinte au droit au respect de la vie privée ou de la correspondance des travailleurs est proportionnée et s'accompagne de garanties adéquates et suffisantes contre les abus[124].

La Cour considère que les juridictions nationales doivent tenir compte des facteurs suivants lorsqu'elles procèdent à la mise en balance des différents intérêts en jeu afin de s'assurer de la proportionnalité des mesures de vidéosurveillance sur le lieu de travail en tenant compte de la spécificité des relations de travail et du développement des nouvelles technologies qui permettent des mesures de surveillance de plus en plus intrusives dans la vie privée des travailleurs[125] :

1° Le travailleur a-t-il été informé de la possibilité que l'employeur prenne des mesures de vidéosurveillance ainsi que de la mise en place de telles mesures ? Si, en pratique, cette information peut être concrètement communiquée au personnel de diverses manières, en fonction des spécificités factuelles de chaque cas, l'avertissement doit en principe être clair quant à la nature de la surveillance et préalable à sa mise en place.
2° Quels ont été l'ampleur de la surveillance opérée par l'employeur et le degré d'intrusion dans la vie privée du travailleur ? À cet égard, il convient de prendre en compte notamment le caractère plus ou moins privé du lieu dans lequel intervient la surveillance, les limites spatiales et temporelles de celle-ci, ainsi que le nombre de personnes ayant accès à ses résultats.
3° L'employeur a-t-il justifié par des motifs légitimes le recours à la surveillance et l'ampleur de celle-ci ? Sur ce point, plus la surveillance est intrusive, plus les justifications requises doivent être sérieuses.
4° Était-il possible de mettre en place un système de surveillance reposant sur des moyens et des mesures moins intrusives ? À cet égard, il convient d'apprécier en fonction des circonstances particulières de chaque espèce si le but légitime poursuivi par l'employeur pouvait être atteint de manière moins intrusive dans la vie privée des travailleurs.
5° Quelles ont été les conséquences de la surveillance pour le travailleur qui en a fait l'objet ? Il convient notamment de vérifier de quelle manière l'employeur a utilisé les résultats de la mesure de surveillance et s'ils ont servi à atteindre le but déclaré de la mesure.
6° Le travailleur s'est-il vu offrir des garanties adéquates, notamment lorsque les mesures de surveillance de l'employeur avaient un caractère intrusif ? Ces

[124] *Ibid.*, § 114.
[125] *Ibid.*, § 116.

> garanties peuvent être mises en œuvre, parmi d'autres moyens, par l'information fournie aux employés concernés ou aux représentants du personnel sur la mise en place et sur l'ampleur de la vidéosurveillance, par la déclaration de l'adoption d'une telle mesure à un organisme indépendant ou par la possibilité d'introduire une réclamation.

Il appartiendra ensuite à la Cour de vérifier si le droit interne et, en particulier, l'application qui en a été faite par les juridictions, ont offert, dans leur mise en balance des intérêts en jeu, une protection suffisante au droit au respect de la vie privée[126].

Usuellement sont en jeu le droit au respect de la vie privée des travailleurs d'un côté et, de l'autre côté, l'intérêt de l'employeur d'assurer la bonne marche de l'entreprise par l'exercice de son pouvoir de direction[127].

Toujours dans l'affaire *Lopez Ribalda*, la mise en place de la vidéosurveillance était justifiée par les soupçons, nourris par le directeur du magasin en raison des pertes importantes constatées sur plusieurs mois, que des vols avaient été commis. Les juridictions internes ont également tenu compte de l'intérêt légitime pour l'employeur d'adopter des mesures afin de découvrir les responsables des pertes constatées et de les sanctionner, dans le but d'assurer la protection de ses biens et le bon fonctionnement de l'entreprise[128].

Les juridictions internes ont ensuite examiné l'ampleur de la mesure de surveillance et le degré d'intrusion dans la vie privée des requérantes et ont retenu que la mesure était limitée en ce qui concernait les espaces et le personnel surveillés – puisque les caméras ne couvraient que les caisses, susceptibles d'être à l'origine des pertes constatées –, et que sa durée dans le temps n'avait pas dépassé ce qui était nécessaire pour confirmer les soupçons de vol. La Cour a considéré que cette appréciation n'était pas déraisonnable[129].

En même temps, la Cour souligne le fait que les requérantes travaillaient dans un lieu ouvert au public et impliquaient un contact permanent avec des clients. La Cour estime à cet égard qu'il faut distinguer (dans l'analyse de la proportionnalité d'une mesure de vidéosurveillance), les différents lieux dans lesquels celle-ci est réalisée à l'aune de l'attente en matière de protection de la vie privée que le salarié peut raisonnablement avoir. Cette attente est très importante dans les endroits relevant de l'intimité, tels que des toilettes ou des vestiaires, où se justifie une protection accrue, voire une interdiction de procéder à une vidéosurveillance. Cette attente demeure forte dans les espaces de travail fermés, tels

[126] *Ibid.*, § 117. Voy. le contrôle opéré en l'espèce par la Cour aux §§ 118 et s.
[127] En ce sens, *Ibid.*, § 122.
[128] *Ibid.*, § 123.
[129] *Ibid.*, § 124.

que les bureaux. Mais elle est manifestement réduite dans les endroits visibles ou accessibles aux collègues ou, comme en l'espèce, à un large public[130].

En ce qui concerne l'ampleur de la mesure dans le temps, la Cour relève que si l'employeur n'avait pas au préalable fixé la durée de la vidéosurveillance, dans les faits celle-ci a duré dix jours et a cessé dès que les employés responsables ont été identifiés. La durée de la surveillance n'apparaît dès lors pas en soi excessive. Enfin, seuls le responsable du magasin, la représentante légale de l'entreprise et la déléguée syndicale ont visionné les enregistrements obtenus au moyen de la vidéosurveillance litigieuse avant que les requérantes n'en soient informées. Compte tenu de ces éléments, la Cour considère que l'intrusion dans la vie privée des requérantes ne revêtait pas un degré de gravité élevé[131].

Pour ce qui est des conséquences de la surveillance litigieuse pour les requérantes, la Cour constate que celles-ci ont été importantes puisque les intéressées ont été licenciées sur la base des enregistrements obtenus par ce moyen. Elle observe néanmoins que la vidéosurveillance et les enregistrements n'ont pas été utilisés par l'employeur à d'autres fins que celle de trouver les responsables des pertes de produits constatées et de les sanctionner[132].

Les juridictions internes ont par ailleurs considéré qu'il n'existait pas d'autre moyen permettant d'atteindre le but légitime poursuivi et que la mesure devait dès lors être jugée « nécessaire ». La Cour aurait souhaité à cet égard que les juridictions internes examinent de manière plus approfondie la possibilité pour l'employeur de recourir à d'autres mesures, moins intrusives pour la vie privée des travailleurs. Toutefois, la Cour relève que l'ampleur des pertes constatées par l'employeur pouvaient donner à penser que des vols avaient été commis par plusieurs personnes et qu'informer l'un quelconque des membres du personnel risquait effectivement de compromettre le but de la vidéosurveillance qui était de découvrir d'éventuels responsables de vols mais aussi de s'assurer des preuves permettant de prendre des mesures disciplinaires à leur égard[133].

La Cour relève ensuite que le droit interne prévoyait un certain nombre de garanties visant à prévenir les ingérences abusives dans les droits des personnes dont les données personnelles faisaient l'objet d'une collecte ou d'un traitement. Ainsi, la loi sur la protection des données donnait notamment à ces personnes le droit d'en être informées de manière préalable, ainsi qu'un droit d'accès, de rectification et de suppression des données récoltées. Une exigence de proportionnalité dans la collecte et l'utilisation des images obtenues au moyen de la vidéosurveillance était expressément posée par l'instruction n° 1/2006 et, selon la jurisprudence du Tribunal constitutionnel, les juridictions internes devaient contrôler le caractère

130 *Ibid.*, § 125.
131 *Ibid.*, § 126.
132 *Ibid.*, § 127.
133 *Ibid.*, § 128.

adéquat, nécessaire et proportionné de telles mesures au regard des droits fondamentaux garantis par la Constitution[134].

S'agissant enfin de savoir si les requérantes avaient été informées de la mise en place de la vidéosurveillance, la Cour note qu'il n'est pas contesté que deux types de caméras avaient été installées dans le supermarché où travaillaient les intéressées : d'une part, des caméras visibles dirigées vers les entrées et sorties du magasin, dont l'employeur avait informé le personnel et, d'autre part, des caméras cachées orientées vers les caisses, dont ni les requérantes ni les autres membres du personnel n'avaient été informés. Il ressort par ailleurs des observations des parties qu'un ou plusieurs panneaux d'information avaient été placés dans le supermarché pour signaler la présence de caméras de surveillance au public mais la teneur exacte des informations indiquées sur ces panneaux n'est pas connue[135].

La Cour observe que si tant la loi espagnole que les normes internationales et européennes pertinentes semblent ne pas exiger le consentement préalable des personnes qui font l'objet d'une vidéosurveillance ou, plus généralement, dont les données personnelles sont collectées, ces normes établissent qu'il est, en principe, nécessaire d'informer ces personnes de façon claire et préalable de l'existence et des modalités d'une telle collecte, ne serait-ce que de manière générale. La Cour considère que l'exigence de transparence et le droit à l'information qui en découle revêtent un caractère fondamental, en particulier dans le contexte des relations de travail, où l'employeur dispose à l'égard des salariés de pouvoirs importants dont il convient d'éviter tout abus. La Cour rappelle cependant que l'information donnée à la personne faisant l'objet d'une surveillance et son ampleur ne sont que l'un des critères à prendre en compte pour apprécier la proportionnalité d'une telle mesure dans un cas donné. Toutefois, si une telle information fait défaut, les garanties découlant des autres critères revêtiront d'autant plus d'importance[136].

Compte tenu de l'importance que revêt le droit à l'information dans pareil cas, la Cour estime que seul un impératif prépondérant relatif à la protection d'intérêts publics ou privés importants pourrait justifier l'absence d'une information préalable[137].

Toutefois, en l'espèce, eu égard notamment au degré moindre d'intrusion dans la vie privée des requérantes et aux raisons légitimes ayant motivé la mise en place de la vidéosurveillance, la Cour estime que les juridictions du travail ont pu, sans dépasser la marge d'appréciation dont disposent les autorités nationales, considérer que l'atteinte à la vie privée des requérantes était proportionnée. En effet, si la Cour ne saurait accepter que, de manière générale, le moindre soupçon que des détournements ou d'autres irrégularités aient été commis par des employés

134 *Ibid.*, § 129.
135 *Ibid.*, § 130.
136 *Ibid.*, § 131.
137 *Ibid.*, § 133.

puisse justifier la mise en place d'une vidéosurveillance secrète par l'employeur, l'existence de soupçons raisonnables que des irrégularités graves avaient été commises et l'ampleur des manques constatés en l'espèce peuvent apparaître comme des justifications sérieuses. Cela est d'autant plus vrai dans une situation où le bon fonctionnement d'une entreprise est mis à mal par des soupçons d'irrégularités commises non par un seul employé mais par l'action concertée de plusieurs employés, dans la mesure où cette situation a pu créer un climat général de méfiance dans l'entreprise[138].

La Cour note, par ailleurs, que les requérantes disposaient d'autres voies de recours. Elle rappelle en outre que la protection effective du droit au respect à la vie privée dans le cadre de la vidéosurveillance sur le lieu de travail peut être assurée par différents moyens qui peuvent relever du droit du travail mais aussi du droit civil, administratif ou pénal[139].

J. Protection contre les caméras cachées à des fins d'intimidation

Les faits qui comprennent le filmage clandestin de la requérante dans sa propre maison et d'aspects très intimes de sa vie, relèvent clairement de sa vie privée[140].

Lorsqu'une facette particulièrement importante de l'existence ou de l'identité d'un individu est en jeu, ou lorsque les activités en jeu concernent un aspect très intime de la vie privée, la marge d'appréciation reconnue à l'État est réduite en conséquence[141].

En particulier, une dissuasion efficace contre les actes graves, lorsque des valeurs fondamentales et des aspects essentiels de la vie privée sont en jeu, exige des États qu'ils veillent à ce que des dispositions pénales efficaces soient mises en place. En ce qui concerne ces actes graves, l'obligation positive de l'État peut également s'étendre aux questions relatives à l'efficacité de l'enquête pénale[142].

Dans l'affaire *Khadija Ismaylova c. Azerbaïdjan*, la Cour a considéré que les faits reprochés étaient graves et constitutifs d'une atteinte à la dignité humaine : une intrusion dans le domicile de la requérante sous la forme d'une intrusion non consentie dans son appartement et de l'installation tout aussi non consentie d'une caméra cachée à l'intérieur de son appartement ; une invasion grave, flagrante et extraordinairement forte de sa vie privée sous la forme du filmage non autorisé d'aspects des plus intimes de sa vie privée, qui s'étaient déroulés dans le sanctuaire de son domicile et la diffusion publique ultérieure de ces images ; et, enfin,

138 *Ibid.*, § 134.
139 *Ibid.*, §§ 136-136.
140 Cour eur. D.H., arrêt du 10 janvier 2019, n[os] 65286/13 et 57270/14, *Khadija Ismaylova c Azerbaïdjan*, § 106.
141 *Ibid.*, § 115.
142 *Ibid.*, § 115.

la réception d'une lettre la menaçant de l'humilier publiquement. La requérante était une journaliste connue et il y avait un lien plausible entre son activité professionnelle et les intrusions en question, dont le but était de la faire taire[143]. Au vu de la gravité des faits et la méthode de protection choisie par les autorités nationales, la Cour considère que la protection effective et concrète de la requérante exigeait que des mesures effectives soient prises dans le cadre de l'enquête pénale en vue d'identifier et de poursuivre le ou les auteurs de ces actes[144].

Pour qu'une enquête soit considérée comme « efficace », elle doit en principe pouvoir conduire à l'établissement des faits et à l'identification et la sanction des responsables. Il ne s'agit pas d'une obligation de résultat, mais d'une obligation de moyens[145].

Dans l'examen de l'efficacité des enquêtes pénales, la Cour a déjà recouru au test du « défaut significatif ». Cela consiste à déterminer si les lacunes présumées de l'enquête sont si importantes qu'elles constituent un manquement aux obligations positives de l'État en vertu de l'article 8. La Cour ne s'attarde pas sur les allégations portant sur des erreurs mineures ou isolées dans l'enquête ; elle ne remplace pas les autorités nationales dans l'appréciation des faits de l'affaire et elle ne décide pas non plus des éventuels auteurs présumés ou de leur responsabilité pénale. Mais, en raison de ce que les faits concernaient une journalise connue et critique du gouvernement, il était de la plus haute importance d'investiguer si les menaces étaient liées aux activités professionnelles de la requérante ainsi que l'identité de leur auteur[146].

La diffusion publique dans la presse d'un rapport intermédiaire d'investigation qui contenait l'adresse de la requérante (une femme mariée), l'identité et la profession de son amant qui figurait dans les vidéos clandestines prises chez elle, le nom de son bailleur et des membres de sa famille, ainsi que le nom et les professions de ses amis et collègues et de la personne à qui elle avait sous-loué son appartement ainsi que leur arrangement financier, constituent une ingérence dans le droit au respect de la vie privée de la requérante, toutes ces informations, prises dans leur globalité, étant relatives à sa vie privée[147]. En l'espèce, la Cour a considéré que cette ingérence ne poursuivait pas un but légitime et n'était pas nécessaire dans une société démocratique[148].

[143] *Ibid.*, § 116.
[144] *Ibid.*, § 117.
[145] *Ibid.*, § 118.
[146] *Ibid.*, §§ 118-120.
[147] *Ibid.*, § 142.
[148] *Ibid.*, §§ 147-148. Sur la violation de l'article 10, voy. les §§ 158-166.

K. Protection de la vie privée en prison

1. *Rappel : maintien des droits fondamentaux en prison*

Les détenus continuent de jouir de tous les droits fondamentaux garantis par la Convention, à l'exception du droit à la liberté lorsqu'une détention régulière entre expressément dans le champ d'application de l'article 5 de la Convention. Les circonstances de l'emprisonnement, comme des considérations en termes de sécurité et de prévention des crimes et désordres, peuvent justifier des restrictions de certains de ces droits. Toutefois, ces restrictions doivent être justifiées dans chaque cas individuel[149]. Ainsi, alors que la détention, comme toute autre mesure privative de liberté, entraîne par nature des restrictions à la vie privée et familiale, les personnes privées de leur liberté ne perdent pas leurs droits garantis par la Convention (en ce compris le droit au respect de leur vie familiale), de sorte que toute restriction à ce droit doit être justifiée dans chaque cas[150].

2. *Protection de la correspondance en prison*

En matière de contrôle de la correspondance des détenus, la législation interne doit, notamment, opérer des distinctions entre les différentes catégories de personnes avec lesquelles les détenus peuvent correspondre (autorités publiques, institutions internationales, proches et avocats). Elle doit aussi détailler la manière dont le contrôle va être réalisé, en ce compris la participation ou l'intervention des détenus dans le cadre du contrôle. Elle doit aussi dire si les détenus ont le droit de savoir si le contenu de leurs correspondances a été altéré. Si le contrôle est automatique, sans limite dans le temps et sans justification, et sans recours, il n'y a pas de protection des détenus contre des ingérences injustifiées à leur droit au respect de leur correspondance[151].

3. *Confidentialité des communications en prison et protection du colloque singulier entre l'avocat et son client*

La communication d'une personne avec un avocat dans le cadre de l'assistance juridique relève de la vie privée puisque l'objectif de cette interaction est de permettre à une personne de prendre des décisions éclairées sur sa vie. Le plus souvent, les informations communiquées à l'avocat concernent des questions intimes et personnelles ou des sujets sensibles. Il s'ensuit donc que, que ce soit dans le cadre de l'assistance à un procès civil ou pénal ou dans le cadre de la recherche de conseils juridiques généraux, les personnes qui consultent un avocat peuvent raisonnablement s'attendre à ce que leur communication soit privée et confidentielle[152].

---

[149] Cour eur. D.H., arrêt du 9 avril 2019, n° 11236/09, *Altay c. Turquie* (§ 2), § 47 ; Cour eur. D.H., arrêt du 2 juillet 2019, n° 27057/06, *Gorlov et autres c. Russie*, § 81.
[150] Cour eur. D.H., arrêt du 27 août 2019, n° 74141/10, *Izmestyev c. Russie*, § 120.
[151] Voy. : Cour eur. D.H., arrêt du 21 mars 2019, n° 41920/09, *Burgazly c. Ukraine*, § 61.
[152] Cour eur. D.H., arrêt du 9 avril 2019, n° 11236/09, *Altay c. Turquie* (§ 2), § 49.

Il est dans l'intérêt général que toute personne qui souhaite consulter un avocat soit libre de le faire dans des conditions qui favorisent une discussion complète et sans entrave. C'est pour cette raison que la relation avocat-client est, en principe, privilégiée.

La communication confidentielle avec son avocat est protégée par la Convention en tant que garantie importante du droit à la défense. La Cour a déjà insisté sur l'importance du droit des prisonniers à communiquer avec son avocat hors de portée d'écoute des autorités pénitentiaires.

Pour la Cour, les prisonniers pourraient se sentir inhibés dans leur discussion avec leurs avocats en présence d'un fonctionnaire, non seulement pour les questions relatives aux litiges en cours, mais aussi pour signaler les abus dont ils pourraient être victimes, par crainte de représailles. La Cour observe en outre que le privilège de la relation avocat-client et l'obligation des autorités nationales de garantir la confidentialité des communications entre un détenu et son représentant choisi sont des normes internationales reconnues[153].

Il n'y a pas lieu de distinguer les différents types de correspondance avec les avocats, pas plus que les différents types de discussions avec les avocats. En conséquence, en règle, toute communication orale aussi bien que toute correspondance entre un avocat et son client est protégée par l'article 8[154].

La possibilité d'y apporter des restrictions ne se conçoit que dans des circonstances exceptionnelles comme la prévention de la perpétration de crimes graves ou de violations graves de la sécurité pénitentiaire[155].

4. *Surveillance vidéo permanente dans les cellules*

Le fait de placer une personne sous surveillance vidéo permanente pendant sa détention (qui entraîne déjà une limitation considérable de la vie privée d'une personne), doit être considéré comme une ingérence grave dans le droit au respect de la vie privée[156].

Pour être prévue par la loi, l'ingérence doit avoir un certain fondement en droit interne et être compatible avec le principe de la primauté du droit. La loi doit donc être suffisamment accessible et prévisible, c'est-à-dire formulée avec suffisamment de précision pour permettre à l'individu (le cas échéant avec des conseils appropriés) d'adapter son comportement. Pour que le droit interne réponde à ces exigences, il doit offrir une protection juridique adéquate contre l'arbitraire et, en

[153] *Ibid.*, § 50.
[154] *Ibid.*, § 51.
[155] *Ibid.*, § 52.
[156] Cour eur. D.H., arrêt du 2 juillet 2019, n° 27057/06, *Gorlov et autres c. Russie*, § 82 ; arrêt du 27 août 2019, n° 74141/10, *Izmestyev c. Russie*, § 121.

conséquence, indiquer avec suffisamment de clarté l'étendue du pouvoir discrétionnaire conféré aux autorités compétentes et les modalités de son exercice. La Cour doit aussi s'assurer qu'il existe des garanties suffisantes et efficaces contre les abus. Cette appréciation dépend de l'ensemble des circonstances de l'espèce, telles que la nature, la portée et la durée des mesures possibles, les motifs requis pour les ordonner, les autorités compétentes pour les autoriser, les exécuter et les contrôler, ainsi que le type de recours prévu par le droit national[157].

Il appartient en premier aux autorités nationales et, en particulier aux juridictions, d'interpréter et d'appliquer le droit interne. Toutefois, il convient de vérifier si la manière dont le droit interne est interprété et appliqué a des effets qui sont compatibles avec les principes de la Convention tels qu'interprétés à la lumière de la jurisprudence de la Cour[158].

II. La protection des données dans la jurisprudence du Tribunal et de la Cour de justice de l'Union européenne

A. Les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne

Au niveau de la place de la Charte dans la protection des droits fondamentaux dans l'Union européenne, le Tribunal a précisé, dans un arrêt du 12 septembre 2019, que « la protection des données à caractère personnel, consacrée actuellement à l'article 8 de la Charte, joue un rôle fondamental pour l'exercice du droit au respect de la vie privée, consacré actuellement à l'article 7 de ladite Charte. Le respect du caractère confidentiel des informations sur la santé constitue l'un des droits fondamentaux protégés par l'ordre juridique de l'Union (arrêt du 8 avril 1992, *Commission/Allemagne*, C-62/90, EU:C:1992:169, point 23) »[159]. Cependant, « les droits consacrés aux articles 7 et 8 de la Charte n'apparaissent pas comme étant des prérogatives absolues, mais doivent être pris en considération au regard de leur fonction dans la société (arrêt du 17 octobre 2013, *Schwarz*, C-291/12, EU:C:2013:670, point 33) »[160].

La Cour a également eu l'occasion de définir, dans un arrêt du 3 octobre 2019, le concept de données à caractère personnel en rappelant que « le respect du droit à la vie privée à l'égard du traitement des données à caractère personnel, reconnu par les articles 7 et 8 de la Charte, se rapporte à toute information concernant une

[157] Cour eur. D.H., arrêt du 2 juillet 2019, n° 27057/06, *Gorlov et autres c. Russie*, § 85 (voy. aussi le § 94).
[158] *Ibid.*, § 86 (voy. les §§ 85-98 sur l'absence de prévisibilité de la mise sous surveillance vidéo permanente dans le cas d'espèce, ainsi que les §§ 124-130 de l'arrêt du 27 août 2019 (n° 74141/10, *Izmestyev c. Russie*) : « le droit russe n'est pas suffisamment accessible et prévisible car il n'indique pas avec assez de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités internes dans le domaine de la vidéosurveillance de détenus condamnés purgeant une peine privative de liberté »).
[159] Trib. UE, 12 septembre 2019, *XI c. Commission européenne*, T/528/18, § 57.
[160] *Ibid.*, § 57.

personne physique identifiée ou identifiable (arrêt du 9 novembre 2010, *Volker und Markus Schecke et Eifert*, C-92/09 et C-93/09, EU:C:2010:662, point 52) »[161].

L'on constate que la notion de données à caractère personnel donnée par la Charte est identique à celle figurant au RGPD ainsi que le principe de minimisation.

Dans ce même arrêt, la Cour a également précisé que « selon une jurisprudence constante, la protection du droit fondamental au respect de la vie privée au niveau de l'Union exige que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire [avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 140 et jurisprudence citée] »[162].

Au niveau de la balance entre le droit à la vie privée et la liberté d'expression, la Cour a précisé que « si les droits de la personne concernée protégés par les articles 7 et 8 de la Charte prévalent, en règle générale, sur la liberté d'information des internautes, cet équilibre peut toutefois dépendre, dans des cas particuliers, de la nature de l'information en question et de sa sensibilité pour la vie privée de la personne concernée ainsi que de l'intérêt du public à disposer de cette information, lequel peut varier, notamment, en fonction du rôle joué par cette personne dans la vie publique (voir, en ce sens, arrêt du 13 mai 2014, *Google Spain et Google*, C-131/12, EU:C:2014:317, point 81) »[163].

Dans ce même arrêt, la Cour a fait sienne la jurisprudence de la Cour européenne des droits de d'homme selon laquelle :

> « [les] demandes adressées par les personnes concernées en vue de l'interdiction, en vertu de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, d'une mise à disposition sur Internet, par les différents médias, d'anciens reportages concernant un procès pénal qui avait été dirigé contre ces personnes, appellent un examen du juste équilibre à ménager entre le droit au respect de la vie privée desdites personnes et, notamment, la liberté d'information du public. Dans la recherche de ce juste équilibre, il doit être tenu compte du rôle essentiel que la presse joue dans une société démocratique et qui inclut la rédaction de comptes rendus et de commentaires sur les procédures judiciaires. En outre, à la fonction des médias consistant à communiquer de telles informations et idées s'ajoute le droit, pour le public, d'en recevoir. La Cour européenne des droits de l'homme a reconnu, dans ce contexte, que le public avait un intérêt non seulement à être informé sur un événement d'actualité, mais aussi à pouvoir faire des recherches sur des événements passés, l'étendue de l'intérêt du public quant aux procédures pénales étant toutefois variable et pouvant évoluer au cours du temps en fonction, notamment, des

[161] C.J.U.E., 3 octobre 2019, *Staatssecretaris van Justitie en Veiligheid c. A, B, P*, C-70/18, § 54.
[162] C.J.U.E., *ibid.*, § 56.
[163] C.J.U.E., 24 septembre 2019, *GC, AF, BH et ED c. Commission nationale de l'informatique et des libertés (CNIL)*, C-136/17, § 66.

circonstances de l'affaire (Cour EDH, 28 juin 2018, *M. L. et W. W. c. Allemagne*, CE:ECHR:2018:0628JUD006079810, § 89 et 100 à 102) »[164].

B. Le règlement 1049/2001 du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission

Le règlement 1049/2001 règle l'accès du public aux documents des institutions européennes. Ainsi, le principe général est l'accès mais des exceptions sont prévues « en raison de certains intérêts publics et privés »[165].

Dans de nombreux arrêts, la Cour doit rappeler que ce règlement a un objectif différent du 45/2001 du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel[166]. « Le premier vise à assurer la plus grande transparence possible du processus décisionnel des autorités publiques ainsi que des informations qui fondent leurs décisions. Il vise donc à faciliter au maximum l'exercice du droit d'accès aux documents ainsi qu'à promouvoir de bonnes pratiques administratives. Le second vise à assurer la protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, lors du traitement de données à caractère personnel (arrêt du 29 juin 2010, *Commission/Bavarian Lager,* C-28/08 P, EU:C:2010:378, point 49). Il s'ensuit que, contrairement au règlement nº 1049/2001, le règlement nº 45/2001 ne vise pas à faciliter l'exercice du droit d'accès aux documents (voir, en ce sens, arrêt du 17 juillet 2014, *YS e.a.*, C-141/12 et C-372/12, EU:C:2014:2081, point 47) »[167].

Cette différence a un impact au niveau du droit d'accès dès lors que « les droits d'accès respectivement prévus par ces deux règlements n'ont ni le même objet ni les mêmes bénéficiaires. En effet, l'article 2 du règlement nº 1049/2001 vise à permettre au public, c'est-à-dire à tout citoyen et à toute personne physique ou morale, d'accéder aux documents détenus par les institutions. L'article 13 du règlement nº 45/2001 vise, quant à lui, à permettre l'accès, par les seules personnes concernées, à leurs données à caractère personnel, c'est-à-dire à des informations les concernant en tant que personnes identifiées ou identifiables, sans prévoir que lesdites personnes puissent, à ce titre, également accéder aux documents contenant lesdites données. À cet égard, il convient de noter que l'article 13, sous c), du règlement nº 45/2001 prévoit seulement que la personne concernée a le droit

[164] C.J.U.E., *ibid.*, § 76.
[165] Trib. UE, 11 juillet 2019, *BP c. Agence des droits fondamentaux de l'Union européenne (FRA)*, T-838/16, §230.
[166] Le règlement 45/2001 a été abrogé par le règlement 2018/1725 du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (Texte présentant de l'intérêt pour l'EEE). Le raisonnement tenu par la Cour lui est cependant transposable.
[167] Trib. UE, 14 février 2019, *RE c. Commission européenne*, T-903/16, § 32.

d'obtenir « la communication, sous une forme intelligible, des données faisant l'objet des traitements »[168].

C. Champ d'application territorial de la directive 95/46 et du RGPD

Il est utile de rappeler ainsi que l'a fait la Cour dans son arrêt du 24 septembre 2019 qu'« il ressort du considérant 10 de la directive 95/46 et des considérants 10, 11 et 13 du règlement 2016/679, lequel a été adopté sur le fondement de l'article 16 TFUE, que l'objectif de cette directive et de ce règlement est de garantir un niveau élevé de protection des données à caractère personnel dans l'ensemble de l'Union »[169].

Il découle de cette limite territoriale que « lorsque l'exploitant d'un moteur de recherche fait droit à une demande de déréférencement en application [des articles 12, sous b), 14, premier alinéa, sous a) de la directive 95/46/CE et 17, paragraphs 1, du RGPD], il est tenu d'opérer ce déréférencement non pas sur l'ensemble des versions de son moteur, mais sur les versions de celui-ci correspondant à l'ensemble des États membres, et ce, si nécessaire, en combinaison avec des mesures qui, tout en satisfaisant aux exigences légales, permettent effectivement d'empêcher ou, à tout le moins, de sérieusement décourager les internautes effectuant une recherche sur la base du nom de la personne concernée à partir de l'un des États membres d'avoir, par la liste de résultats affichée à la suite de cette recherche, accès aux liens qui font l'objet de cette demande »[170].

D. Champ d'application matériel de la directive 95/46 et du RGPD

La directive 95/46 prévoyait qu'elle ne s'appliquait pas aux traitements de données à caractère personnel effectués par « les États membres dans le cadre d'activités qui relèvent du champ d'application du chapitre 2 du titre V du traité sur l'Union européenne », « par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces » et « par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques »[171] ; exception qui est reprise par le RGPD en son article 2, c)[172].

---

168 Trib. UE, *ibid.*, § 33.
169 C.J.U.E., 24 septembre 2019, *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)*, C-507/17, § 54.
170 C.J.U.E., *ibid.*, dispositif de l'arrêt.
171 Article 3, 2 de la directive 95/46.
172 « Le présent règlement ne s'applique pas au traitement de données à caractère personnel effectué :
(…)
c) par une personne physique dans le cadre d'une activité strictement personnelle ou domestique ;
(…) ».

La Cour, dans son arrêt du 14 février 2019, a eu l'occasion de préciser que les exceptions doivent « faire l'objet d'une interprétation stricte (voir, en ce sens, arrêts du 27 septembre 2017, *Puškár*, C-73/16, EU:C:2017:725, point 38, et du 10 juillet 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, point 37) »[173]. Ainsi, « l'enregistrement et la publication de la vidéo [de policiers dans un commissariat alors que l'auteur de la vidéo y était interrogé] ne sauraient être regardés comme un traitement de données à caractère personnel réalisé dans l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, ni comme un traitement ayant pour objet la sécurité publique, la défense, la sûreté de l'État ou les activités de l'État dans le domaine du droit pénal, au sens de l'article 3, paragraphe 2, premier tiret, de la directive 95/46. À cet égard, la Cour a déjà jugé que les activités mentionnées à titre d'exemples par ladite disposition sont, dans tous les cas, des activités propres aux États ou aux autorités étatiques, étrangères aux domaines d'activité des particuliers (voir, en ce sens, arrêt du 27 septembre 2017, *Puškár*, C-73/16, EU:C:2017:725, point 36 et jurisprudence citée) »[174].

De plus, la publication, sans restriction d'accès, d'une vidéo « sur un site Internet de vidéos sur lequel les utilisateurs peuvent envoyer, regarder et partager celles-ci, rendant ainsi accessibles des données à caractère personnel à un nombre indéfini de personnes, le traitement de données à caractère personnel en cause au principal ne s'inscrit pas dans le cadre de l'exercice d'activités exclusivement personnelles ou domestiques (voir, par analogie, arrêts du 6 novembre 2003, *Lindqvist*, C-101/01, EU:C:2003:596, point 47 ; du 16 décembre 2008, *Satakunnan Markkinapörssi et Satamedia*, C-73/07, EU:C:2008:727, point 44 ; du 11 décembre 2014, *Ryneš*, C-212/13, EU:C:2014:2428, points 31 et 33, ainsi que du 10 juillet 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, point 42) »[175].

Dans ce même arrêt, la Cour a également précisé que « le fait de procéder à un enregistrement vidéo de membres de la police dans le cadre de l'exercice de leurs fonctions n'est pas de nature à exclure un tel type de traitement de données à caractère personnel du champ d'application de la directive 95/46. En effet, ainsi que l'a relevé Madame l'avocate générale au point 29 de ses conclusions, cette directive ne prévoit aucune exception qui exclurait du champ d'application de ladite directive les traitements de données à caractère personnel concernant des fonctionnaires. Par ailleurs, il ressort de la jurisprudence de la Cour que la circonstance qu'une information s'inscrit dans le contexte d'une activité professionnelle n'est pas de nature à lui ôter sa qualification de "donnée à caractère personnel" (voir, en ce sens, arrêt du 16 juillet 2015, *ClientEarth et PAN Europe/EFSA*, C-615/13 P, EU:C:2015:489, point 30 et jurisprudence citée) »[176].

À noter que cet enseignement est totalement transposable au RGPD.

[173] C.J.U.E., *Sergejs Buivids c. Datu valsts inspekcija*, C-345/17, § 41.
[174] C.J.U.E., *ibid.*, C-345/17, § 42.
[175] C.J.U.E., *ibid.*, C-345/17, § 43.
[176] C.J.U.E., *ibid.*, C-345/17, §§ 44-46.

E. Notion de responsable du traitement

Au cours de l'année 2019, la Cour a, à nouveau, eu l'occasion de rappeler sa jurisprudence en vertu de laquelle « conformément à l'objectif poursuivi par la directive 95/46 de garantir un niveau élevé de protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel, l'article 2, sous d), de cette directive définit de manière large la notion de "responsable du traitement" comme visant la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel (voir, en ce sens, arrêt du 5 juin 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388, points 26 et 27) »[177].

Elle complète cela en précisant que

- « l'objectif de cette disposition est d'assurer, par une définition large de la notion de "responsable", une protection efficace et complète des personnes concernées (arrêts du 13 mai 2014, *Google Spain et Google*, C-131/12, EU:C:2014:317, point 34, ainsi que du 5 juin 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388, point 28) »[178] ;
- « une personne physique ou morale qui influe, à des fins qui lui sont propres, sur le traitement de données à caractère personnel et participe de ce fait à la détermination des finalités et des moyens de ce traitement peut être considérée comme étant responsable du traitement, au sens de l'article 2, sous d), de la directive 95/46 (arrêt du 10 juillet 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, point 68) »[179] ;
- « la responsabilité conjointe de plusieurs acteurs pour un même traitement, en vertu de cette disposition, ne présuppose pas que chacun d'eux ait accès aux données à caractère personnel concernées (voir, en ce sens, arrêts du 5 juin 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388, point 38, et du 10 juillet 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, point 69) »[180] ;
- « l'existence d'une responsabilité conjointe ne se traduit pas nécessairement par une responsabilité équivalente, pour un même traitement de données à caractère personnel, des différents acteurs. Au contraire, ces acteurs peuvent être impliqués à différents stades de ce traitement et selon différents degrés, de telle sorte que le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte de toutes les circonstances pertinentes du cas d'espèce (voir, en ce sens, arrêt du 10 juillet 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, point 66) »[181].

177 C.J.U.E., 29 juillet 2019, *Fashion ID GmbH & Co. KG c. Verbraucherzentrale NRW eV*, C-40/17, § 65.
178 C.J.U.E., *ibid.*, § 66.
179 C.J.U.E., *ibid.*, § 68.
180 C.J.U.E., *ibid.*, § 69.
181 C.J.U.E., *ibid.*, § 70.

Dans l'arrêt du 29 juillet 2019, la Cour a considéré que la société Fashion ID devait être considérée comme responsable du traitement en ayant inséré sur son site Internet le bouton « j'aime » de Facebook car[182] :

– « elle semble avoir offert la possibilité à Facebook Ireland d'obtenir des données à caractère personnel des visiteurs de son site Internet, une telle possibilité étant déclenchée dès le moment de la consultation d'un tel site, et ce indépendamment du fait que ces visiteurs soient membres du réseau social Facebook ou qu'ils aient cliqué sur le bouton "j'aime" de Facebook ou encore qu'ils aient connaissance d'une telle opération » ;
– « les opérations de traitement de données à caractère personnel dont Fashion ID est susceptible de déterminer, conjointement avec Facebook Ireland, les finalités et les moyens sont, au regard de la définition de la notion de "traitement à caractère personnel" figurant à l'article 2, sous b), de la directive 95/46, la collecte et la communication par transmission des données à caractère personnel des visiteurs de son site Internet ».

Elle a poursuivi son raisonnement en analysant les deux conditions pour que Fashion ID puisse être considérée comme responsable du traitement conjointement avec Facebook, à savoir la détermination de la finalité et des moyens :

– Moyens[183] :
  • « Fashion ID semble avoir inséré sur son site Internet le bouton "j'aime" de Facebook mis à la disposition des gestionnaires de sites Internet par Facebook Ireland, tout en étant conscient que celui-ci sert d'outil de collecte et de transmission de données à caractère personnel des visiteurs de ce site, que ceux-ci soient membres ou non du réseau social Facebook ».
  • « En insérant un tel module social sur son site Internet, Fashion ID influe, par ailleurs, de manière déterminante sur la collecte et la transmission des données à caractère personnel des visiteurs dudit site au profit du fournisseur dudit module, en l'occurrence Facebook Ireland, qui, en l'absence de l'insertion dudit module, n'auraient pas lieu ».
– Finalité :
  • « il semble que l'insertion par Fashion ID du bouton "j'aime" de Facebook sur son site Internet lui permet d'optimiser la publicité pour ses produits en les rendant plus visibles sur le réseau social Facebook lorsqu'un visiteur de son site Internet clique sur ledit bouton. C'est afin de pouvoir bénéficier de cet avantage commercial consistant en une telle publicité accrue pour ses produits que Fashion ID, en insérant un tel bouton sur son site Internet, semble avoir consenti, à tout le moins implicitement, à la collecte et à la communication par transmission des données à caractère personnel des visiteurs de son site, ces opérations de traitement étant effectuées dans l'intérêt économique tant de Fashion ID que de Facebook Ireland, pour qui le fait de

[182] C.J.U.E., *ibid.*, §§ 75-78.
[183] C.J.U.E., *ibid.*, §§ 77-79.

pouvoir disposer de ces données à ses propres fins commerciales constitue la contrepartie de l'avantage offert à Fashion ID »[184].

La Cour a également souligné qu'« un site Internet, tel que celui de Fashion ID, est visité tant par des personnes qui sont membres du réseau social Facebook et qui disposent ainsi d'un compte sur ce réseau social que par ceux qui n'en disposent pas. Dans ce dernier cas, la responsabilité du gestionnaire d'un site Internet, tel que Fashion ID, à l'égard du traitement des données à caractère personnel de ces personnes apparaît encore plus importante, car la simple consultation d'un tel site, comportant le bouton "j'aime" de Facebook, semble déclencher le traitement de leurs données à caractère personnel par Facebook Ireland (voir, en ce sens, arrêt du 5 juin 2018, *Wirtschaftsakademie Schleswig-Holstein,* C-210/16, EU:C:2018:388, point 41) »[185].

À noter cependant que la Cour a opéré un distinguo entre le traitement initial et le traitement ultérieur opéré par Facebook dès lors qu'« il apparaît, de prime abord, exclu que Fashion ID détermine les finalités et les moyens des opérations de traitement de données à caractère personnel ultérieures, effectuées par Facebook Ireland après leur transmission à cette dernière, de sorte que Fashion ID ne saurait être considérée comme étant responsable de ces opérations »[186].

Dans un nouvel arrêt concernant un moteur de recherche, la Cour a rappelé que l'exploitant d'un moteur de recherche doit être considéré comme un responsable du traitement pour le traitement qu'il effectue (trouver des informations publiées ou placées sur Internet par des tiers, à les indexer de manière automatique, à les stocker temporairement et, enfin, à les mettre à la disposition des internautes selon un ordre de préférence)[187] « dans la mesure où l'activité d'un moteur de recherche est susceptible d'affecter significativement et de manière additionnelle par rapport à celle des éditeurs de sites web les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel »[188].

En effet, « le traitement de données à caractère personnel effectué dans le cadre de l'activité d'un moteur de recherche se distingue de et s'ajoute à celui effectué par les éditeurs de sites web, consistant à faire figurer ces données sur une page web, et cette activité joue un rôle décisif dans la diffusion globale desdites données en ce qu'elle rend celles-ci accessibles à tout internaute effectuant une recherche à partir du nom de la personne concernée, y compris aux internautes qui, autrement, n'auraient pas trouvé la page web sur laquelle ces mêmes données sont publiées. De plus, l'organisation et l'agrégation des informations publiées sur Internet effectuées par les moteurs de recherche dans le but de faciliter à

[184] C.J.U.E., *ibid.*, § 80.
[185] C.J.U.E., *ibid.*, § 83.
[186] C.J.U.E., *ibid.*, § 76.
[187] C.J.U.E., 24 septembre 2019, *GC, AF, BH et ED c. Commission nationale de l'informatique et des libertés (CNIL)*, C-136/17, § 35.
[188] C.J.U.E., *ibid.*, C-136/17, § 37.

leurs utilisateurs l'accès à celles-ci peuvent conduire, lorsque la recherche de ces derniers est effectuée à partir du nom d'une personne physique, à ce que ceux-ci obtiennent par la liste de résultats un aperçu structuré des informations relatives à cette personne trouvables sur Internet leur permettant d'établir un profil plus ou moins détaillé de la personne concernée (arrêt du 13 mai 2014, *Google Spain et Google,* C-131/12, EU:C:2014:317, points 35 à 37) »[189]. À noter que cette responsabilité ne peut s'entendre qu'au niveau du référencement de pages Internet ou, plus spécifiquement, des liens vers celles-ci[190].

F. Notion d'« activités de journalisme »

Monsieur Buivids qui avait publié une vidéo de policiers prise dans le commissariat alors qu'il y était pour une déposition dans le cadre d'une procédure d'infraction administrative soulevait l'argument selon lequel il devait bénéficier des exceptions liées aux activités de journalisme. En réponse à cet argument, la Cour a rappelé que cette notion ne pouvait pas être liée au statut de journaliste de la personne[191] et que « les "activités de journalisme" sont celles qui ont pour finalité la divulgation au public d'informations, d'opinions ou d'idées, sous quelque moyen de transmission que ce soit (voir, en ce sens, arrêt du 16 décembre 2008, *Satakunnan Markkinapörssi et Satamedia,* C-73/07, EU:C:2008:727, point 61) »[192].

De plus, « le fait, pour M. Buivids, d'avoir mis en ligne cet enregistrement sur un tel site Internet, en l'occurrence le site www.youtube.com, ne saurait, en soi, ôter à ce traitement de données à caractère personnel la qualité d'avoir été effectué "aux seules fins de journalisme", au sens de l'article 9 de la directive 95/46. En effet, il y a lieu de tenir compte de l'évolution et de la multiplication des moyens de communication et de diffusion d'informations. Ainsi, la Cour a déjà jugé que le support au moyen duquel les données traitées sont transmises, classique tel que le papier ou les ondes hertziennes, ou électronique tel que l'Internet, n'est pas déterminant pour apprécier s'il s'agit d'une activité "aux seules fins de journalisme" (voir, en ce sens, arrêt du 16 décembre 2008, *Satakunnan Markkinapörssi et Satamedia,* C-73/07, EU:C:2008:727, point 60) »[193].

La Cour tempère cependant ce principe en précisant qu'« il ne saurait être considéré que toute information publiée sur Internet, portant sur des données à caractère personnel, relève de la notion d'"activités de journalisme" et bénéficie à ce titre des exemptions et des dérogations prévues à l'article 9 de la directive 95/46 »[194] et « s'il s'avère que l'enregistrement et la publication de cette vidéo n'avaient pas pour seule finalité la divulgation au public d'informations, d'opinions ou d'idées, il ne pourra être considéré que le traitement des données à

189 C.J.U.E., *ibid.*, C-136/17, § 36.
190 C.J.U.E., *ibid.*, C-136/17, § 46.
191 C.J.U.E., *Sergejs Buivids c. Datu valsts inspekcija*, C-345/17, § 55.
192 C.J.U.E., *ibid.*, § 53.
193 C.J.U.E., *ibid.*, §§ 56-57.
194 C.J.U.E., *ibid.*, §§ 56-57.

caractère personnel en cause au principal a été effectué aux "seules fins de journalisme" »[195]. La Cour précise également que les exceptions liées à la notion d'« activités de journalisme » ne peuvent être appliquées « que dans la seule mesure où elles s'avèrent nécessaires pour concilier deux droits fondamentaux, à savoir le droit à la protection de la vie privée et celui à la liberté d'expression (voir, en ce sens, arrêt du 16 décembre 2008, *Satakunnan Markkinapörssi et Satamedia,* C-73/07, EU:C:2008:727, point 55) »[196].

G. Base de licéité

1. *Consentement*

Dans une affaire liée au consentement de l'internaute à l'installation de cookies via une case cochée par défaut, la Cour a fait siens les propos de l'avocat général qui avait conclu que « l'exigence d'une "manifestation" de volonté de la personne concernée évoque clairement un comportement actif et non pas passif. Or, un consentement donné au moyen d'une case cochée par défaut n'implique pas un comportement actif de la part de l'utilisateur d'un site Internet »[197]. Elle complète ce raisonnement en considérant qu'« il apparaît pratiquement impossible de déterminer de manière objective si l'utilisateur d'un site Internet a effectivement donné son consentement au traitement de ses données personnelles en ne décochant pas une case cochée par défaut ainsi que, en tout état de cause, si ce consentement a été donné de manière informée »[198].

La Cour conclut donc de manière logique que « le consentement visé à l'article 2, sous f), et à l'article 5, paragraphe 3, de la directive 2002/58, lus conjointement avec l'article 2, sous h), de la directive 95/46, n'est dès lors pas valablement donné lorsque le stockage d'informations ou l'accès à des informations déjà stockées dans l'équipement terminal de l'utilisateur d'un site Internet est autorisé au moyen d'une case cochée par défaut par le fournisseur du service, que l'utilisateur devrait décocher pour refuser de donner son consentement »[199]. Cette interprétation « s'impose, à plus forte raison, à la lumière du [RGPD] »[200].

2. *Intérêt légitime*

La Cour a eu l'occasion, dans un arrêt du 11 décembre 2019, de préciser la notion d'intérêt légitime en considérant que l'article 7, f), de la directive 95/46 devenu article 6, 1, f sous le RGPD « prévoit trois conditions cumulatives pour qu'un trai-

195 C.J.U.E., *ibid.*, § 62.
196 C.J.U.E., *ibid.*, § 63.
197 C.J.U.E., 1er octobre 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV c. Planet49 GmbH*, C-673/17, § 52.
198 C.J.U.E., *ibid.*, § 55.
199 C.J.U.E., *ibid.*, § 57.
200 C.J.U.E., *ibid.*, § 60. Dans le considérant 32 RGPD, « l'expression du consentement pourrait se faire notamment en cochant une case lors de la consultation d'un site Internet. Ledit considérant exclut en revanche expressément qu'il y ait un consentement en cas de silence, de cases cochées par défaut ou d'inactivité » (§ 62).

tement de données à caractère personnel soit licite, à savoir, premièrement, la poursuite d'un intérêt légitime par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, deuxièmement, la nécessité du traitement des données à caractère personnel pour la réalisation de l'intérêt légitime poursuivi et, troisièmement, la condition tenant à ce que les droits et les libertés fondamentaux de la personne concernée par la protection des données ne prévalent pas sur l'intérêt légitime poursuivi (arrêt du 4 mai 2017, *Rīgas satiksme,* C-13/16, EU:C:2017:336, point 28) »[201].

Dans cet arrêt qui concernait la mise en place de caméras de surveillance dans les espaces communs d'un immeuble, la Cour a ainsi considéré que « l'objectif que vise, en substance, le responsable du traitement des données lorsqu'il met en place un système de vidéosurveillance tel que celui en cause au principal, à savoir la protection des biens, de la santé et de la vie des copropriétaires d'un immeuble, est susceptible d'être qualifié d'"intérêt légitime", au sens de l'article 7, sous f), de la directive 95/46 »[202]. Il faut cependant que cet intérêt soit « né et actuel à la date du traitement et ne pas présenter de caractère hypothétique à cette date »[203] et « il ne saurait cependant être nécessairement exigé, lors de l'appréciation de l'ensemble des circonstances du cas d'espèce, qu'il ait été porté antérieurement atteinte à la sécurité des biens et des personnes »[204]. Par ailleurs, il faut également que la mesure soit nécessaire dès lors que « la Cour a rappelé que les dérogations et les restrictions au principe de protection des données à caractère personnel doivent s'opérer dans les limites du strict nécessaire (arrêt du 4 mai 2017, *Rīgas satiksme*, C-13/16, EU:C:2017:336, point 30 et jurisprudence citée) »[205]. De plus, cette condition de « nécessité du traitement doit être examinée conjointement avec le principe dit de la "minimisation des données" consacré à l'article 6, paragraphe 1, sous c), de la directive 95/46, selon lequel les données à caractère personnel doivent être "adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement" »[206].

Dans un autre arrêt, la Cour a pu préciser que dans une situation de responsabilité conjointe et « dans laquelle le gestionnaire d'un site Internet insère sur ledit site un module social permettant au navigateur du visiteur de ce site de solliciter des contenus du fournisseur dudit module et de transmettre à cet effet audit fournisseur des données à caractère personnel du visiteur, il est nécessaire que ce gestionnaire et ce fournisseur poursuivent chacun, avec ces opérations de traite-

[201] C.J.U.E., 11 décembre 2019, *TK c. Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, § 40.
[202] C.J.U.E., *ibid.*, § 42 ; voy., par analogie, arrêt du 11 décembre 2014, *Ryneš*, C-212/13, § 34.
[203] C.J.U.E., *ibid.*, § 44.
[204] C.J.U.E., *ibid.*, § 44.
[205] C.J.U.E., *ibid.*, § 46.
[206] C.J.U.E., *ibid.*, § 48. « La proportionnalité du traitement des données par la voie d'un dispositif de vidéosurveillance doit être appréciée en tenant compte des modalités concrètes de mise en place et de fonctionnement de ce dispositif, lesquelles doivent en limiter l'incidence sur les droits et libertés des personnes concernées tout en garantissant l'efficacité du système de vidéosurveillance en cause » (§ 50).

ment, un intérêt légitime, au sens de l'article 7, sous f), de la directive 95/46, afin que celles-ci soient justifiées dans son chef »[207].

H. Balance d'intérêts

La Cour a rappelé dans un arrêt du 17 janvier 2019 relatif à la poursuite d'infractions en matière de TVA qu'il appartient au législateur national de « modifier sa réglementation et de garantir que le régime procédural applicable à la poursuite des infractions portant atteinte aux intérêts financiers de l'Union ne soit pas conçu de telle manière qu'il présente, pour des raisons inhérentes à celui-ci, un risque systémique d'impunité des faits constitutifs de telles infractions, ainsi que d'assurer la protection des droits fondamentaux des personnes poursuivies (arrêt du 5 juin 2018, *Kolev e.a.*, C-612/15, EU:C:2018:392, point 65) »[208]. Il y a donc lieu, dans le chef de tout législateur national d'opérer une juste balance entre, d'une part, la nécessité de poursuivre des faits infractionnels et, d'autre part, de garantir le respect des droits fondamentaux parmi lesquels figure la protection des données à caractère personnel.

Il est utile de relever que la Cour a également mis cette obligation à charge des juridictions nationales en précisant que :

> « l'obligation de garantir un prélèvement efficace des ressources de l'Union ne dispense pas les juridictions nationales du respect nécessaire des droits fondamentaux garantis par la Charte et des principes généraux du droit de l'Union, dès lors que les procédures pénales ouvertes pour des infractions en matière de TVA constituent une mise en œuvre du droit de l'Union, au sens de l'article 51, paragraphe 1, de la Charte. Dans le domaine pénal, ces droits et ces principes généraux doivent être respectés non seulement lors des procédures pénales, mais aussi au cours de la phase de l'enquête préliminaire, dès l'instant où la personne concernée se trouve accusée (voir, en ce sens, arrêts du 5 décembre 2017, *M.A.S. et M.B.*, C-42/17, EU:C:2017:936, point 52 ; du 5 juin 2018, *Kolev e.a.*, C-612/15, EU:C:2018:392, points 68 et 71, ainsi que du 20 mars 2018, *Di Puma et Zecca*, C-596/16 et C-597/16, EU:C:2018:192, point 31 et jurisprudence citée) »[209].

Dans ce même arrêt, il a été précisé que « les écoutes téléphoniques constituent une ingérence dans le droit à la vie privée, consacré à l'article 7 de la Charte. Une telle ingérence ne peut être admise, conformément à l'article 52, paragraphe 1, de la Charte, que si elle est prévue par la loi et si, dans le respect du contenu essentiel de ce droit et du principe de proportionnalité, elle est nécessaire et répond effectivement à des objectifs d'intérêt général reconnus par l'Union (voir, en ce sens, arrêt du 17 décembre 2015, *WebMindLicenses*, C-419/14, EU:C:2015:832,

[207] C.J.U.E., 29 juillet 2019, *Fashion ID GmbH & Co. KG c. Verbraucherzentrale NRW eV*, C-40/17, § 97.
[208] C.J.U.E., 17 janvier 2019, *Spetsializiran nakazatelen sad (tribunal pénal spécialisé, Bulgarie) c. Petar Dzivev, Galina Angelova, Georgi Dimov et Milko Velkov*, C-310/16, § 31.
[209] C.J.U.E., *Idem*, § 33.

points 71 et 73) »[210]. Sur la base de ce rappel, la Cour a considéré que le « droit de l'Union ne saurait imposer au juge national d'écarter l'application [de règles de procédure imposant au juge national d'écarter de la procédure pénale des éléments de preuve, tels que des écoutes téléphoniques, nécessitant une autorisation judiciaire préalable lorsque cette autorisation a été émise par une autorité judiciaire incompétente], même si l'utilisation des éléments de preuve recueillis illégalement était susceptible d'augmenter l'efficacité des poursuites pénales permettant aux autorités nationales de sanctionner, dans certains cas, le non-respect du droit de l'Union (voir par analogie, s'agissant des règles de procédure internes conférant l'autorité de la chose jugée à une décision juridictionnelle, arrêt du 24 octobre 2018, *XC e.a.*, C-234/17, EU:C:2018:853, point 53 ainsi que jurisprudence citée) »[211].

I. Notion de données à caractère personnel

La Cour a confirmé que les données biométriques constituent bien des données à caractère personnel au sens de l'article 2, sous b), de la directive 95/46 et, qu'en outre, elles « relèvent d'une catégorie particulière de données, au sens de l'article 8, paragraphe 1, de cette directive »[212]. Cela implique, selon la Cour, que « les dérogations à la protection de ces données et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire, conformément à la jurisprudence de la Cour issue de l'arrêt du 21 décembre 2016, *Tele2 Sverige et Watson e.a.* (C-203/15 et C-698/15, EU:C:2016:970, point 96) »[213].

L'arrêt considère cependant que le fait de prendre dix empreintes digitales et un image faciale, outre que cela « permet d'identifier de manière fiable la personne concernée »[214], « ne revêt pas un caractère intime et n'entraîne pas non plus un désagrément physique ou psychique particulier pour la personne concernée (voir, en ce sens, arrêt du 17 octobre 2013, *Schwarz,* C-291/12, EU:C:2013:670, point 48) »[215].

Dans un arrêt du 16 janvier 2019, la Cour a pu rappeler que les données fiscales sont des données à caractère personnel et qu'un « numéro d'identification fiscale constitue, par sa nature même, une donnée fiscale se rapportant à une personne physique identifiée ou identifiable et, partant, une donnée à caractère personnel. En outre, en raison du lien établi entre le numéro d'identification fiscale d'une personne précisément identifiée et l'information relative au centre des impôts compétent à l'égard d'une telle personne, effectué par les autorités douanières,

[210] C.J.U.E., *Idem*, § 36.
[211] C.J.U.E., *Idem*, § 38.
[212] C.J.U.E., 3 octobre 2019, *Staatssecretaris van Justitie en Veiligheid c. A, B, P*, C-70/18, § 29.
[213] C.J.U.E., *Idem*, § 29.
[214] C.J.U.E., *Idem*, § 58.
[215] C.J.U.E., *Idem*, § 58.

cette information doit également être considérée comme une donnée à caractère personnel »[216].

Il en va de même pour les images enregistrées par une caméra ainsi que l'a rappelé la Cour dans un cet arrêt du 14 février 2019 relatif à l'enregistrement de policiers dans un commissariat lors d'une déposition par l'auteur de la vidéo en considérant que s'il « est possible de voir et d'entendre les membres de la police sur la vidéo en cause, (…) il y a lieu de considérer que les images des personnes ainsi enregistrées constituent autant de données à caractère personnel, au sens de l'article 2, sous a), de la directive 95/46 »[217].

Au niveau des données à caractère personnel visées aux articles 9 et 10 du RGPD, la Cour a précisé que « l'interdiction et les restrictions qu'[ils] établissent s'appliquent, sous réserve des exceptions prévues par [la] directive et [le] règlement, à tout type de traitement des catégories particulières de données visées par lesdites dispositions et à l'ensemble des responsables effectuant de tels traitements »[218] et qu'« aucune autre disposition de ladite directive ou dudit règlement ne prévoit une dérogation générale à cette interdiction ou à ces restrictions en faveur d'un traitement tel que celui effectué dans le cadre de l'activité d'un moteur de recherche »[219].

Ainsi, « il résulte de l'économie générale de ces textes que l'exploitant d'un tel moteur doit, à l'instar de tout autre responsable du traitement, assurer, dans le cadre de ses responsabilités, de ses compétences et de ses possibilités, que le traitement des données à caractère personnel qu'il effectue satisfait aux exigences, respectivement, de la directive 95/46 ou du règlement 2016/679 »[220]. Et la Cour de compléter son raisonnement en confirmant qu'« une interprétation de l'article 8, paragraphes 1 et 5, de la directive 95/46 ou de l'article 9, paragraphe 1, et de l'article 10 du règlement 2016/679 qui exclurait, *a priori* et de façon générale, l'activité d'un moteur de recherche des exigences spécifiques que ces dispositions prévoient par rapport aux traitements portant sur les catégories particulières des données qui y sont visées irait à l'encontre de la finalité desdites dispositions, consistant à assurer une protection accrue à l'encontre de tels traitements qui, en raison de la sensibilité particulière de ces données, sont susceptibles de constituer, ainsi qu'il ressort également du considérant 33 de cette directive et du considérant 51 de ce règlement, une ingérence particulièrement grave dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, garantis par les articles 7 et 8 de la Charte »[221].

---

[216] C.J.U.E., *Deutsche Post AG c. Hauptzollamt Köln*, C-496/17, §56.
[217] C.J.U.E., *Sergejs Buivids c. Datu valsts inspekcija*, C-345/17, §32.
[218] C.J.U.E., 24 septembre 2019, *GC, AF, BH et ED c. Commission nationale de l'informatique et des libertés (CNIL)*, C-136/17, § 42.
[219] C.J.U.E., *Idem*, § 43.
[220] C.J.U.E., *Idem*, § 43.
[221] C.J.U.E., *Idem*, § 44.

Au niveau du contenu de l'article 10 du RGPD, la Cour a précisé que « les informations concernant une procédure judiciaire menée contre une personne physique, telles que celles relatant sa mise en examen ou le procès, et, le cas échéant, la condamnation qui en a résulté, constituent des données relatives aux "infractions" et aux "condamnations pénales", au sens de l'article 8, paragraphe 5, premier alinéa, de la directive 95/46 et de l'article 10 du règlement 2016/679, et ce indépendamment du fait que, au cours de cette procédure judiciaire, la commission de l'infraction pour laquelle la personne était poursuivie a effectivement été établie ou non »[222].

En ce qui concerne les données à caractère médical, la Cour a confirmé sa jurisprudence en rappelant que « compte tenu du caractère extrêmement intime et sensible des données à caractère médical, le traitement de ces données appelle un examen particulièrement rigoureux. En effet, il ressort de la jurisprudence que le respect du caractère confidentiel des informations sur la santé constitue l'un des droits fondamentaux protégés par l'ordre juridique de l'Union (arrêt du 8 avril 1992, *Commission/Allemagne,* C-62/90, EU:C:1992:169, point 23). Ce principe est capital non seulement pour protéger la vie privée des malades, mais également pour préserver leur confiance dans le corps médical et les services de santé en général (Cour EDH, 25 février 1997, *Z c. Finlande,* CE:ECHR:1997:0225JUD002200993, point 95) »[223].

J. Notion de traitement

Dans le même arrêt du 14 février 2019, la Cour a rappelé sa jurisprudence antérieure en ce qu'elle considère que « dans le cadre d'un système de vidéosurveillance, la Cour a déjà jugé qu'un enregistrement vidéo des personnes stocké dans un dispositif d'enregistrement continu, à savoir le disque dur de ce système, constitue, conformément à l'article 2, sous b), et à l'article 3, paragraphe 1, de la directive 95/46, un traitement de données à caractère personnel automatisé (voir, en ce sens, arrêt du 11 décembre 2014, *Ryneš,* C-212/13, EU:C:2014:2428, points 23 et 25) »[224]. De plus, « le fait qu'un tel enregistrement n'a eu lieu qu'une seule fois est sans incidence sur la question de savoir si cette opération relève du champ d'application de la directive 95/46. En effet, ainsi qu'il ressort du libellé de l'article 2, sous b), de cette directive, lu en combinaison avec l'article 3, paragraphe 1, de celle-ci, ladite directive s'applique à "toute opération" qui constitue un traitement de données à caractère personnel, au sens de ces dispositions »[225].

Le fait de publier des données à caractère personnel sur une page Internet a également été considéré comme consistant en un traitement[226]. De plus, « faire appa-

[222] C.J.U.E., *Idem*, § 72.
[223] Trib. UE, 12 septembre 2019, *XI c. Commission européenne*, T-528/18, § 67.
[224] C.J.U.E., *Sergejs Buivids c. Datu valsts inspekcija*, C-345/17, § 34.
[225] C.J.U.E., *Idem*, § 36.
[226] C.J.U.E., *Idem*, § 36. Cet appel rappelle également l'arrêt *Lindqvist*, 6 novembre 2003, C-101/01, point 25 ainsi que celui du 13 mai 2014, *Google Spain et Google*, C-131/12, point 26.

raître des informations sur une page Internet implique de réaliser une opération de chargement de cette page sur un serveur ainsi que les opérations nécessaires pour rendre cette page accessible aux personnes qui se sont connectées à Internet. Ces opérations sont effectuées, au moins en partie, de manière automatisée (voir, en ce sens, arrêt du 6 novembre 2003, *Lindqvist,* C-101/01, EU:C:2003:596, point 26). Ainsi, il convient de considérer que le fait de publier sur un site Internet de vidéos sur lequel les utilisateurs peuvent envoyer, regarder et partager celles-ci un enregistrement vidéo, telle la vidéo en cause, sur lequel figurent des données à caractère personnel, constitue un traitement automatisé en tout ou en partie de ces données, au sens de l'article 2, sous b), et de l'article 3, paragraphe 1, de la directive 95/46 »[227].

Dans un autre arrêt et fidèle à sa jurisprudence, la Cour a rappelé que « l'activité d'un moteur de recherche consistant à trouver des informations publiées ou placées sur Internet par des tiers, à les indexer de manière automatique, à les stocker temporairement et, enfin, à les mettre à la disposition des internautes selon un ordre de préférence donné doit être qualifiée de "traitement de données à caractère personnel" »[228].

La Cour précise ainsi que « le traitement de données à caractère personnel effectué dans le cadre de l'activité d'un moteur de recherche se distingue de et s'ajoute à celui effectué par les éditeurs de sites web, consistant à faire figurer ces données sur une page web, et cette activité joue un rôle décisif dans la diffusion globale desdites données en ce qu'elle rend celles-ci accessibles à tout internaute effectuant une recherche à partir du nom de la personne concernée, y compris aux internautes qui, autrement, n'auraient pas trouvé la page web sur laquelle ces mêmes données sont publiées. De plus, l'organisation et l'agrégation des informations publiées sur Internet effectuées par les moteurs de recherche dans le but de faciliter à leurs utilisateurs l'accès à celles-ci peuvent conduire, lorsque la recherche de ces derniers est effectuée à partir du nom d'une personne physique, à ce que ceux-ci obtiennent par la liste de résultats un aperçu structuré des informations relatives à cette personne trouvables sur Internet leur permettant d'établir un profil plus ou moins détaillé de la personne concernée (arrêt du 13 mai 2014, *Google Spain et Google,* C-131/12, EU:C:2014:317, points 35 à 37) »[229].

K. Droit à l'information de la personne concernée

Le Tribunal a rappelé, dans une affaire opposant une ancienne agente de l'Agence européenne pour l'environnement (AEE) à cette dernière[230], que l'article 12 du règlement 45/2001 impose au responsable du traitement de, « dès l'enregistrement des données ou, si la communication de données à un tiers est envisagée,

[227] C.J.U.E., *Idem*, §§ 38-39.
[228] C.J.U.E., 24 septembre 2019, *GC, AF, BH et ED c. Commission nationale de l'informatique et des libertés (CNIL)*, C-136/17, § 35 ; voy. aussi C.J.U.E., 13 mai 2014, *Google Spain et Google*, C-131/12, § 41.
[229] C.J.U.E., *Idem*, § 36.
[230] Trib. UE, 11 juin 2019, *TO c. Agence européenne pour l'environnement*, T-462/17.

au plus tard lors de la première communication de données, fournir à la personne concernée [les informations précisées par le règlement], sauf si la personne en est déjà informée »[231]. En l'espèce, l'AEE avait reçu d'un de ses co-contractants un courrier électronique contenant des données à caractère personnel concernant l'agente et ne l'en avait avertie que trois semaines après leur enregistrement. Le Tribunal a considéré que l'AEE avait enfreint l'article 12 du règlement 45/2001[232] et a été condamné à indemniser l'agente lésée. L'infraction était d'autant plus avérée que ce courrier électronique avait servi de base à la décision de l'AEE de mettre fin au contrat de de l'agente.

Il convient de relever que le RGPD ne soumet pas l'information à des délais aussi stricts. En effet, l'article 14, 3, du RGPD dispose que :

> « Le responsable du traitement fournit les informations (...) :
>
> a) dans un délai raisonnable après avoir obtenu les données à caractère personnel, mais ne dépassant pas un mois, eu égard aux circonstances particulières dans lesquelles les données à caractère personnel sont traitées ;
>
> b) si les données à caractère personnel doivent être utilisées aux fins de la communication avec la personne concernée, au plus tard au moment de la première communication à ladite personne ; ou
>
> c) s'il est envisagé de communiquer les informations à un autre destinataire, au plus tard lorsque les données à caractère personnel sont communiquées pour la première fois ».
>
> Dans un arrêt déjà cité ci-dessus, la Cour a pu rappeler que « l'exigence de traitement loyal des données à caractère personnel, prévue à l'article 6 de la directive 95/46 ou à l'article 5 du règlement 2016/679, implique une obligation d'informer les personnes concernées de la collecte de ces données par les autorités douanières en vue de leur traitement ultérieur (voir, en ce sens, arrêt du 1er octobre 2015, *Bara e.a.,* C-201/14, EU:C:2015:638, point 34) »[233].

Dans un autre arrêt, la Cour a précisé que le devoir d'information à charge d'un responsable du traitement conjoint, celui-ci doit « concerner l'opération ou l'ensemble des opérations de traitement des données à caractère personnel dont il détermine effectivement les finalités et les moyens »[234].

L. Accès aux données par la personne concernée

Le Tribunal de l'Union européenne a précisé le caractère continu et permanent de son droit d'accès à ses données à caractère personnel par toute personne concernée[235] dans un arrêt du 14 février 2019.

[231] Trib. UE, *Idem*, § 199.
[232] Trib. UE, *Idem*, § 199.
[233] C.J.U.E., *Deutsche Post AG c. Hauptzollamt Köln*, C-496/17, § 59.
[234] C.J.U.E., 29 juillet 2019, *Fashion ID GmbH & Co. KG c. Verbraucherzentrale NRW eV*, C-40/17, § 100.
[235] Trib. UE, 14 février 2019, *RE c. Commission européenne*, T-903/16, §§ 46 et 69.

Il est utile de noter que cette décision prise sur pied de l'article 13 du règlement 45/2001 est transposable au RGPD qui dispose, en son article 15 que « la personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel ». Le RGPD soumet cependant ce droit d'accès à une règle de temporalité dès lors que la personne concernée ne peut accéder aux données la concernant qu'à intervalles raisonnables[236], et ce pour éviter des demandes à répétition et abusives.

M. Droit à l'effacement

En matière d'effacement de référencement par un moteur de recherche, la Cour a rappelé que l'obligation à charge dudit moteur de recherche était indépendante du fait que les données à caractère personnel aient été ou pas effacées des pages Internet référencées[237].

Cependant, la Cour précise que ce droit à l'effacement est cependant soumis à une analyse du moteur du recherche qui devra « au titre des motifs d'intérêt public important visés à l'article 8, paragraphe 4, de la directive 95/46 ou à l'article 9, paragraphe 2, sous g), du règlement 2016/679 et dans le respect des conditions prévues à ces dispositions, si l'inclusion du lien vers la page web en question dans la liste affichée à la suite d'une recherche effectuée à partir du nom de la personne concernée est nécessaire à l'exercice du droit à la liberté d'information des internautes potentiellement intéressés à avoir accès à cette page web au moyen d'une telle recherche, protégée par l'article 11 de la Charte »[238].

Jean Herveg

Directeur de l'unité de recherche « Libertés et Société de l'Information » au Centre de Recherche Information, Droit et Société (www.crids.eu)
Avocat au barreau de Bruxelles (www.rawlingsgiles.be)
Auteur de la partie consacrée à la Cour européenne des droits de l'homme

Jean-Marc Van Gyseghem

Directeur de Recherche au Centre de Recherche Information, Droit et Société (www.crids.eu)
Avocat au barreau de Bruxelles (www.rawlingsgiles.be)
Auteur de la partie consacrée aux juridictions de l'Union européenne

[236] RGPD, considérant 63.
[237] C.J.U.E., 24 septembre 2019, *GC, AF, BH et ED c. Commission nationale de l'informatique et des libertés (CNIL)*, C-136/17, § 52 ; voy. aussi C.J.U.E., 13 mai 2014, *Google Spain et Google*, C-131/12, § 88.
[238] C.J.U.E., *Idem*, § 66.