La protection des données à caractère personnel en droit européen : chronique de jurisprudence (2021)

Herveg, Jean; Van Gyseghem, Jean-Marc

Published in:
Journal européen des droits de l'homme

Publication date:
2022

Document Version
le PDF de l'éditeur

La protection des données à caractère personnel en droit européen – Chronique de jurisprudence (2021)

Personal Data Protection in European Law – Column of case-law (2021)

Jean Herveg et 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 2021.

Après un rappel relatif à l'articulation entre la protection des droits fondamentaux par l'Union européenne et celle offerte par la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, les arrêts sélectionnés de la Cour européenne des droits de l'homme concernent la protection de l'identité, la prescription de l'action en recherche de paternité, le droit d'accès, la protection des données relatives à la santé, la divulgation par des autorités fiscales de données de contribuables défaillants, la protection contre la cyberviolence, la protection des données dans les procédures judiciaires, la protection contre la surveillance « ciblée », la protection contre la surveillance « de masse », la protection contre la surveillance en prison, les perquisitions et saisies d'équipements informatiques et électroniques, les registres de police et les casiers judiciaires, la liberté d'expression, la vie privée, la réputation et l'honneur, et la protection des données et l'Internet.

Abstract

The column analyzes the contribution of the European Court of Human Rights and the courts of the European Union to data protection for the year 2021.

After a reminder on the articulation between the protection of fundamental rights by the European Union and that offered by the Convention for the Protection of Human Rights and Fundamental Freedoms, the selected judgments of the European Court of Human Rights concern the protection of identity, the statute of limitations for paternity proceedings, the right of access, the protection of health data, the disclosure by tax authorities of data of defaulting taxpayers, protection against cyber-violence, data protection in judicial proceedings, protection against "targeted" surveillance, protection against "mass" surveillance, protection against surveillance in prisons, search and seizure of computer and electronic equipments, police and criminal records, freedom of expression, privacy, reputation and honor, and data protection and the Internet.

[1] This work has been done with the financial support from the European Union's Horizon 2020 research and innovation program under Grant Agreements n[os] 830892 (SPARTA) & 958339 (DENiM). 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.

En ce qui concerne la Cour de justice de l'Union européenne, certains arrêts concernent des questions de compétences, de recevabilité des demandes mais également d'applicabilité directe d'un règlement européen. Par ailleurs, un arrêt très attendu par l'Autorité de protection des données a analysé de manière approfondie les compétences de l'autorité de contrôle et, plus particulièrement, dans un contexte de traitement transfrontalier avec l'intervention de la notion de chef de file. Un autre arrêt a porté sur les notions essentielles telles que données à caractère personnel, licéité de traitement et applicabilité de l'article 10 mais également d'« établissement » et de minimisation. Un arrêt concerne également la directive e-privacy et, plus particulièrement, l'accès aux données de communication électroniques auprès de fournisseurs de service de communications électroniques.

S'il y a peu de décisions rendues annuellement par la C.J.U.E. ou le Tribunal en matière de protection des données, elles sont souvent très denses.

As far as the Court of Justice of the European Union is concerned, some judgments concern questions of competence, admissibility of requests, but also the direct applicability of a European regulation. In addition, a long-awaited ruling by the Data Protection Authority analyzed in depth the powers of the supervisory authority, particularly in the context of cross-border processing, with the intervention of the concept of "lead supervisory authority". Another judgment dealt with the essential concepts of personal data, lawfulness of processing and applicability of Article 10, but also of "establishment" and minimization. A ruling also concerns the e-privacy directive and, more specifically, access to electronic communication data from electronic communication service providers.

Although there are few decisions rendered annually by the CJEU or the Court, they are often very dense.

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

A. L'articulation entre la protection des droits fondamentaux par l'Union européenne et par le Conseil de l'Europe

Le respect du droit de l'Union européenne par un État membre constitue un objectif légitime d'intérêt général d'un poids considérable[2].

La Convention n'interdit pas aux États de transférer leur pouvoir souverain à une organisation internationale telle que l'Union européenne. L'action étatique entreprise en conformité avec de telles obligations juridiques est justifiée dès lors que l'organisation en question est considérée comme protégeant les droits fondamentaux, tant en ce qui concerne les garanties substantielles offertes que les mécanismes de contrôle de leur respect, d'une manière qui peut être considérée comme au moins équivalente à celle prévue par la Convention. Par « équivalent », la Cour entend « comparable », toute exigence d'une protection « identique » de l'organisa-

[2] Cour eur. D.H., décision du 9 novembre 2021, *Willems c. Les Pays-Bas*, n° 57294/16, § 24.

tion pourrait aller à l'encontre de l'intérêt de la coopération internationale recherchée[3].

La Cour a déjà reconnu que la protection des droits fondamentaux offerte par l'Union européenne était en principe équivalente à celle offerte par le système de la Convention[4].

L'application de cette présomption de protection équivalente est soumise à deux conditions. La première est que l'ingérence litigieuse doit avoir constitué une obligation juridique internationale stricte pour l'État défendeur, à l'exclusion de toute marge de manœuvre de la part des autorités nationales. La deuxième condition est le déploiement de tout le potentiel du mécanisme de surveillance prévu par le droit de l'Union européenne[5].

La présomption de conformité à la Convention peut être renversée si, dans les circonstances d'un cas particulier, la protection des droits fondamentaux était manifestement déficiente[6].

La condition du plein déploiement du mécanisme de contrôle doit être appliquée sans formalisme excessif et en tenant compte des caractéristiques spécifiques du mécanisme de contrôle en question. Ce faisant, elle n'impose pas à la juridiction nationale de demander à la Cour de justice de l'Union européenne de se prononcer dans tous les cas sans exception, y compris dans les cas où aucune question réelle et sérieuse ne se pose quant à la protection des droits fondamentaux par le droit de l'Union européenne, ou dans ceux où la Cour de justice de l'Union européenne a déjà indiqué précisément comment les dispositions applicables du droit de l'Union européenne doivent être interprétées d'une manière compatible avec les droits fondamentaux[7].

B. Protection de l'identité

1. *Le droit à l'identité sexuelle*

Le droit au respect de la vie privée englobe l'identification sexuelle comme un aspect de l'identité personnelle. Cela concerne tous les individus, y compris les personnes transgenres, qu'elles souhaitent ou non commencer un traitement de conversion sexuelle agréé par les autorités[8].

[3] *Ibid.*, § 26.
[4] *Ibid.*, § 27.
[5] *Ibid.*, § 28.
[6] *Ibid.*, § 29.
[7] *Ibid.*, § 34.
[8] Cour eur. D.H., 19 janvier 2021, *X et Y c. Roumanie*, n[os] 2145/16 et 20607/16, § 106.

Le droit à l'identité sexuelle est un des aspects les plus importants de la vie privée. Dans ce domaine, les États contractants jouissent d'une marge d'appréciation restreinte[9].

La Cour ne met pas en cause le choix des législateurs de confier à l'autorité judiciaire plutôt qu'à l'autorité administrative les décisions en matière de changement de registre d'état civil des personnes transsexuelles[10].

La préservation du principe de l'indisponibilité de l'état des personnes, de la garantie de la fiabilité et de la cohérence de l'état civil et, plus largement, de l'exigence de sécurité juridique relève de l'intérêt général et justifie la mise en place de procédures rigoureuses dans le but notamment de vérifier les motivations profondes d'une demande de changement légal d'identité[11].

Le refus des autorités internes de reconnaître juridiquement la réassignation sexuelle faute d'une intervention chirurgicale de conversion sexuelle est une atteinte injustifiée au droit au respect de la vie privée[12].

2. *Reconnaissance des parents d'intention*

Le refus de reconnaître les parents d'intention dans une gestation pour autrui est une ingérence dans le droit au respect de la vie familiale de ces parents et de l'enfant[13].

3. *Ordre d'attribution des noms de famille*

Des références d'ordre général à des traditions présupposées ou attitudes sociales majoritaires ayant cours dans un pays donné ne suffisent pas à justifier une différence de traitement fondée sur le sexe[14].

Si la règle voulant que le nom du père soit attribué en premier en cas de désaccord des parents peut se révéler nécessaire en pratique et n'est pas forcément en contradiction avec la Convention, l'impossibilité d'y déroger est excessivement rigide et discriminatoire envers les femmes[15].

Si la sécurité juridique peut être manifestée par le choix de placer le nom du père en premier, elle peut aussi bien être manifestée par le nom de la mère[16].

---

[9] *Ibid.*, § 148.
[10] *Ibid.*, § 153.
[11] *Ibid.*, § 158.
[12] *Ibid.*, § 167.
[13] Cour eur. D.H., arrêt du 18 mai 2021, *Valdis Fjolnisdottir et autres c. Icelande*, n° 71552/17, § 63.
[14] Cour eur. D.H., arrêt du 26 octobre 2021, *Leon Madrid c. Espagne*, n° 30306/13, § 66.
[15] *Ibid.*, § 68.
[16] *Ibid.*, § 69.

4. *Changement du nom de famille*

Le choix ou le changement du nom tombe dans le champ d'application de l'article 8 étant donné que le nom concerne la vie privée et familiale de l'individu[17].

Des restrictions légales à la possibilité de changer de nom peuvent se justifier dans l'intérêt public, par exemple afin d'assurer un enregistrement exact de la population, sauvegarder les moyens d'une identification personnelle ou relier à une famille les porteurs d'un nom donné[18].

Le nom, en tant qu'élément d'individualisation principal d'une personne au sein de la société, appartient au noyau dur des considérations relatives au droit au respect de la vie privée et familiale[19].

C. Prescription de l'action en recherche de paternité

Les procédures relatives à la paternité tombent incontestablement sous l'empire de l'article 8. En effet, ce dernier reconnaît à chacun le droit de connaître ses origines et de les voir légalement établies[20].

En matière de prescription de l'action en recherche de paternité, la Cour examine plusieurs éléments[21] :

- si les circonstances justifiant une demande en recherche de paternité étaient réunies avant ou après l'expiration du délai de prescription ;
- s'il existe des recours lorsque l'action est prescrite (et qui permettent, par exemple, la réouverture du délai) ou des exceptions lorsqu'une personne prend connaissance de la réalité biologique après l'expiration du délai de prescription.

Elle distingue selon que la personne n'a eu aucune possibilité de connaître les faits des cas où la personne savait ou avait des raisons de supposer qui était son père mais n'a pris aucune mesure pour engager la procédure dans le délai[22].

La Cour distingue aussi entre les situations dans lesquelles les délais sont absolus et rigides et celles où les délais peuvent être prolongés quand les faits pertinents ne sont pas connus avant l'expiration des délais. Dans le premier cas, il y a violation de l'article 8 si le délai est appliqué sans prendre en compte le fait de savoir si l'enfant a eu connaissance des circonstances se rapportant à l'identité de son père. Dans le deuxième cas, la Cour regarde si la personne a agi avec diligence pour

[17] Cour eur. D.H., arrêt du 16 novembre 2021, *Kyazim c. Bulgarie*, n° 39356/17, § 15.
[18] *Ibid.*, § 33.
[19] *Ibid.*, § 39.
[20] Cour eur. D.H., arrêt du 19 octobre 2021, *Lavanchy c. Suisse*, n° 69997/17, § 30 (cette affaire fait l'objet d'un renvoi devant la Grande Chambre).
[21] *Ibid.*, § 33.
[22] *Ibid.*

bénéficier de la possibilité d'introduire la procédure en établissement de paternité après l'expiration des délais de prescription[23].

D. Droit d'accès

1. *Accès au dossier d'un enfant par la personne l'ayant pris en charge*

Le processus décisionnel qui débouche sur une mesure d'ingérence doit être équitable et respecter les intérêts protégés par l'article 8[24].

En ce qui concerne l'accès aux données personnelles détenues par des autorités publiques, la question de l'accès à ses origines et de la connaissance de l'identité de ses parents biologiques n'est pas de même nature que celle de l'accès au dossier personnel établi sur un enfant pris en charge ou celle de la recherche des preuves d'une paternité alléguée[25].

2. *Informations à fournir aux parents lors d'une autopsie réalisée contre leur gré*

Il ne peut pas être exclu que le droit au respect de la vie privée et familiale couvre des situations post-mortem[26]. L'autopsie d'un nouveau-né décédé réalisée contre les objections de ses parents est une ingérence dans le droit au respect de la vie privée et familiale ainsi que dans celui de manifester sa religion sous l'angle de l'article 9[27].

La marge d'appréciation de l'État est normalement restreinte lorsqu'est en jeu un aspect particulièrement important de la vie ou de l'identité d'un individu. Toutefois, la marge d'appréciation sera plus large en l'absence de consensus entre les États membres du Conseil de l'Europe sur l'importance relative des intérêts en jeu ou sur la meilleure façon de les protéger. Habituellement, l'État se voit reconnaître une large marge d'appréciation quand il doit trouver un équilibre entre des intérêts privés et publics concurrents ou entre des droits protégés par la Convention[28].

Les droits protégés par les articles 8 et 9 ne sont pas absolus et n'imposent pas aux États de reconnaître un droit absolu de pouvoir s'opposer aux autopsies[29].

---

[23] *Ibid.*, § 34.
[24] Cour eur. D.H., arrêt du 27 mai 2021, *Jessica Marchi c. Italie*, n° 54978/17, § 41.
[25] *Ibid.*, § 108.
[26] Cour eur. D.H., arrêt du 20 juillet 2021, *Polat c. Autriche*, n° 12886/16, § 48. La Cour a rappelé que la manière d'inhumer un mort est un aspect essentiel des pratiques religieuses et tombe dans le champ de l'article 9. Dès lors, cette disposition s'applique au grief selon lequel une autopsie a été réalisée contre les convictions religieuses des parents.
[27] *Ibid.*, § 53.
[28] *Ibid.*, § 78.
[29] *Ibid.*, § 84.

Le droit d'accès aux informations relatives à la vie privée et familiale d'une personne soulève une question au titre de l'article 8[30]. Dans ce contexte, le grief concernant l'obligation d'un hôpital public de fournir des informations sur l'autopsie d'un enfant à sa mère tombe dans la sphère du droit au respect de la vie privée et familiale[31]. Dans le cas d'une autopsie réalisée contre le gré des parents, l'hôpital avait une obligation encore plus grande de leur fournir une information sur ce qui avait été fait lors de l'autopsie et sur ce qui serait fait avec le corps de leur enfant[32].

3. *Obligation d'informer les proches d'un décès*

Lorsqu'une personne disparaît en étant sous la garde de l'État et dans des circonstances mettant sa vie en danger, une enquête officielle efficace doit être menée sur cette disparition[33].

Lorsqu'une personne décède à l'insu de ses proches mais à la connaissance de l'État, ce dernier a l'obligation positive, en vertu de l'article 8, de prévenir les proches afin qu'ils puissent, entre autres, organiser une sépulture convenable[34].

E. Protection des données relatives à la santé

Le stockage systématique et les autres utilisations d'informations relatives à la vie privée d'un individu par les autorités publiques ont des implications importantes pour les intérêts protégés par l'article 8 et constituent donc une ingérence dans les droits protégés par celui-ci. C'est d'autant plus vrai lorsque le traitement concerne des catégories d'informations très intimes et sensibles, notamment des informations relatives à la santé physique ou mentale d'une personne identifiable[35].

Compte tenu de l'importance fondamentale de la protection des données pour l'exercice effectif du droit au respect de la vie privée, la marge d'appréciation dont disposent les États membres pour concevoir leurs cadres législatifs et administratifs respectifs dans ce domaine est plutôt limitée[36].

Le fait que l'information soit publique n'enlève pas nécessairement la protection de l'article 8 notamment lorsque la personne concernée n'a pas divulgué l'information ou autorisé sa divulgation. En effet, même en ce qui concerne une nouvelle diffusion d'« informations publiques », l'intérêt de la publication de ces informations devait être mis en balance avec des considérations liées à la vie privée[37].

---

30 *Ibid.*, § 93.
31 *Ibid.*, § 95.
32 *Ibid.*, § 115.
33 Cour eur. D.H., arrêt du 31 août 2021, *Vassiliou et autres c. Chypre*, n° 58699/15, § 82.
34 *Ibid.*, § 95.
35 Cour eur. D.H., arrêt du 14 décembre 2021, *E.B. c. La République de Moldavie*, n° 41542/13, § 22.
36 *Ibid.*, § 23.
37 *Ibid.*, § 24.

Il en est ainsi parce que le respect de la vie privée consiste également à empêcher toute nouvelle intrusion. Ainsi, même si l'information en question était déjà connue du public, une nouvelle diffusion de cette « information publique » doit aussi être mise en balance avec le droit à la vie privée de la personne concernée[38].

Le stockage et les autres utilisations de données sensibles à propos de la santé d'une personne sont nécessairement couverts par la protection de l'article 8[39].

F. Divulgation par des autorités fiscales de données de contribuables défaillants

1. *Applicabilité de l'article 8*

Le nom, l'adresse personnelle et le numéro d'identification fiscale (en tant qu'informations concernant une personne physique identifiée ou identifiable) constituent des « données à caractère personnel » au sens de l'article 2 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[40].

Selon la jurisprudence constante de la Cour, les considérations liées à la vie privée entrent en jeu dans les situations où des informations ont été recueillies sur une personne bien précise, où des données à caractère personnel ont été traitées ou utilisées, et où les éléments en question ont été rendus publics d'une manière ou dans une mesure excédant ce à quoi les intéressés pouvaient raisonnablement s'attendre[41].

La protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. Le droit interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cette disposition[42].

L'article 8 consacre ainsi un droit à une forme d'auto-détermination informationnelle qui autorise les personnes à invoquer leur droit à la vie privée en ce qui concerne des données qui, bien que neutres, sont collectées, traitées et diffusées, selon des formes ou modalités telles que leurs droits au titre de l'article 8 puissent être mis en jeu[43].

[38] *Ibid.*
[39] *Ibid.*, § 25.
[40] Cour eur. D.H., arrêt du 12 janvier 2021, *L.B. c. Hongrie*, n° 36345/16, § 19.
[41] *Ibid.*, § 22.
[42] *Ibid.*
[43] *Ibid.*

Donner des précisions sur les revenus imposables provenant du travail et d'autres sources, ainsi que du patrimoine net imposable de personnes, relève clairement de la vie privée de celles-ci[44].

Le manquement d'un contribuable à ses obligations fiscales est un comportement qui peut être enregistré ou rapporté publiquement[45]. Néanmoins, compte tenu du fait que les données publiées contenaient des informations sur la situation économique du contribuable, la Cour considère que les données publiées par l'autorité fiscale relevaient de la vie privée du contribuable. Dans ce contexte, peu importe que les données publiées aient concerné des impôts impayés sur des activités professionnelles[46].

Par ailleurs, il n'est pas contesté que la mesure en cause impliquait la publication de l'adresse personnelle du contribuable, laquelle, conformément à la jurisprudence de la Cour, constitue une donnée ou un renseignement d'ordre personnel qui relève de la vie privée et qui bénéficie, à ce titre, de la protection accordée à celle-ci[47].

2. *Sur l'existence d'une ingérence*

La publication ou l'utilisation par une autorité publique de données relatives à la vie privée d'un individu constitue une atteinte à l'article 8, § 1er[48].

En l'espèce, les informations en cause ayant été rendues accessibles à des tiers, la publication sur le site de l'autorité fiscale de données qui désignaient le requérant comme un contribuable défaillant puis comme un grand fraudeur fiscal et indiquaient dans le détail le montant précis de ses arriérés d'impôts et dettes fiscales, son numéro d'identification fiscale et son adresse personnelle, s'analyse en une ingérence dans la vie privée de l'intéressé au sens de l'article 8[49].

3. *Sur la justification de l'ingérence*

Pour déterminer la proportionnalité d'une mesure générale, la Cour doit commencer par étudier les choix législatifs à l'origine de la mesure. La qualité de l'examen parlementaire et judiciaire de la nécessité de la mesure réalisé au niveau national revêt une importance particulière à cet égard, y compris pour ce qui est de l'application de la marge d'appréciation pertinente[50].

---

[44] *Ibid.*
[45] *Ibid.*, § 23.
[46] *Ibid.*
[47] *Ibid.*, § 24.
[48] *Ibid.*, § 42.
[49] *Ibid.*, § 43.
[50] *Ibid.*, § 48.

La question centrale n'est pas de savoir s'il aurait fallu adopter des règles moins restrictives, ni même de savoir si l'État peut prouver que sans l'interdiction l'objectif légitime visé ne pourrait pas être atteint. Il s'agit plutôt de déterminer si, lorsqu'il a adopté la mesure générale litigieuse et arbitré entre les intérêts en présence, le législateur a agi dans le cadre de sa marge d'appréciation[51].

Les autres facteurs à prendre en compte pour apprécier la compatibilité d'un dispositif législatif entraînant l'imposition de mesures restrictives en l'absence de tout examen individualisé du comportement d'une personne, sont la gravité de la mesure en question et le point de savoir si le dispositif législatif est encadré de manière suffisamment stricte pour répondre d'une manière proportionnée au besoin social impérieux auquel il cherche à répondre[52]. La manière dont une mesure générale a été appliquée aux faits d'une cause donnée permet de se rendre compte de ses répercussions pratiques et est donc pertinente pour l'appréciation de sa proportionnalité[53].

Une ample latitude est d'ordinaire laissée à l'État pour prendre des mesures d'ordre général en matière économique ou sociale[54]. La marge d'appréciation est de façon générale également ample lorsque l'État doit ménager un équilibre entre des intérêts privés et publics concurrents ou différents droits protégés par la Convention[55].

La Cour tient également compte du rôle fondamental que joue la protection des données à caractère personnel pour l'exercice du droit au respect de la vie privée consacré par l'article 8[56]. La protection accordée aux données à caractère personnel dépend d'un certain nombre de facteurs, dont la nature du droit en cause garanti par la Convention, son importance pour la personne concernée, la nature de l'ingérence et la finalité de celle-ci[57]. Selon l'arrêt *S. et Marper*, la marge d'appréciation d'un État est d'autant plus restreinte que le droit en cause est important pour garantir à l'individu la jouissance effective des droits fondamentaux ou d'ordre « intime » qui lui sont reconnus[58]. Lorsqu'un aspect particulièrement important de l'existence ou de l'identité d'un individu se trouve en jeu, la marge laissée à l'État est d'ordinaire restreinte[59].

Dans son appréciation, la Cour tient dûment compte du contexte spécifique dans lequel les informations en cause ont été rendues publiques[60]. Elle trouve important de souligner que la mesure contestée s'inscrivait dans le cadre de la politique

[51] *Ibid.*
[52] *Ibid.*
[53] *Ibid.*
[54] *Ibid.*, § 49.
[55] *Ibid.*
[56] *Ibid.*, § 50.
[57] *Ibid.*
[58] *Ibid.*
[59] *Ibid.*
[60] *Ibid.*, § 52.

fiscale générale de l'État[61]. Il convient de relever ici le rôle essentiel des impôts pour financer l'appareil d'État mais aussi pour mettre en œuvre la politique économique et sociale de l'État dans un sens plus large[62]. La Cour reconnaît qu'il est difficile d'établir si la publication des données des contribuables défaillants permet réellement de lutter contre la fraude fiscale et la perte de recettes qui en découle pour l'État[63]. Le Gouvernement affirme que tel est le cas, tandis que le requérant soutient le contraire. La Cour estime qu'il n'est pas déraisonnable que l'État juge nécessaire de protéger l'intérêt économique général en assurant la perception des recettes publiques au moyen d'un contrôle des citoyens visant à dissuader les contribuables de manquer à leurs obligations fiscales[64].

Outre l'intérêt économique du pays dans son ensemble au bon fonctionnement de son système fiscal, le Gouvernement mentionne également la protection des intérêts économiques de personnes privées, à savoir les partenaires commerciaux potentiels[65]. La Cour ne voit aucune raison de remettre en question l'idée que toute personne a un intérêt spécifique à obtenir des informations relatives au respect de leurs obligations fiscales par ceux avec lesquels elle entend établir des relations économiques afin de déterminer, en fin de compte, s'il est opportun de s'y engager, en particulier lorsque l'évasion fiscale persiste pendant une période prolongée[66]. L'accès à de telles informations ayant également une incidence sur la concurrence et le fonctionnement de l'économie, la Cour est disposée à admettre que la divulgation de la liste des personnes redevables d'un montant important d'impôts avait une valeur informative pour le public sur une question d'intérêt général et ne concernait pas une question purement privée ni n'avait pour seul objet de satisfaire la curiosité du public[67].

Le choix du législateur de rendre publique l'identité de personnes ayant manqué à leurs obligations fiscales dans le but d'améliorer la discipline de paiement et de protéger les intérêts commerciaux des tiers, en contribuant ainsi à l'économie générale, n'est pas manifestement dépourvu de base raisonnable[68].

La Cour a tenu compte des critères suivants[69] :

- la publication ne concernait que les grands fraudeurs fiscaux ;
- la durée du manquement aux obligations fiscales ;
- le retrait de la liste dès que les impôts étaient payés ;
- les données publiées permettaient un contrôle du public sur la fraude fiscale ;
- une combinaison d'identifiants était nécessaire pour assurer l'exactitude et l'efficacité du dispositif.

---

61 *Ibid.*
62 *Ibid.*
63 *Ibid.*
64 *Ibid.*
65 *Ibid.*, § 53.
66 *Ibid.*
67 *Ibid.*
68 *Ibid.*, § 54.
69 *Ibid.*, §§ 54-60.

La Cour poursuit en relevant que les communications en ligne et leur contenu risquent bien plus que la presse de porter atteinte à l'exercice et à la jouissance des droits et libertés fondamentaux, en particulier du droit au respect de la vie privée[70].

Plus précisément, la publication d'informations concernant des impôts impayés expose le contribuable à un contrôle du public qui s'accroît en proportion de l'étendue de la publicité. La publication des données à caractère personnel du requérant sur le site de l'autorité fiscale les a rendues accessibles à quiconque se connectait à Internet, y compris à des personnes se trouvant dans un autre pays[71].

D'un autre côté, l'accès des données concernées à un large public était nécessaire pour l'efficacité du dispositif. Tout en reconnaissant l'importance des droits d'une personne ayant fait l'objet d'une publication disponible sur Internet, ces droits doivent aussi être mis en balance avec le droit du public à s'informer. En l'espèce, le but et l'effet principal de la publication en cause étaient d'informer le public, et la raison principale pour laquelle ces données ont été publiées en ligne était de rendre les informations aisément disponibles et accessibles aux personnes concernées, indépendamment de leur lieu de résidence[72].

La portée et l'incidence potentielles d'une déclaration publiée sur un site destiné à un lectorat réduit ne sont certainement pas les mêmes que dans le cas d'une déclaration publiée sur une page web grand public ou très visitée[73].

En l'espèce, le seul fait que l'accès à la liste en cause n'était pas restreint ne signifie pas nécessairement que cette liste attirait une forte attention du public : en particulier, quiconque souhaitait accéder aux informations en question devait tout d'abord se rendre sur le site de l'autorité fiscale, puis trouver la liste des contribuables défaillants ou des fraudeurs fiscaux, et enfin rechercher les informations désirées[74].

Par ailleurs, la Cour doute que la liste des contribuables défaillants et des fraudeurs fiscaux, publiée en hongrois sur le site de l'autorité fiscale, ait pu attirer l'attention du public – dans le monde entier – au-delà des personnes concernées. En revanche, plus que toute autre, la publication sur un portail consacré aux questions fiscales garantissait la diffusion des informations d'une manière raisonnablement calculée pour n'atteindre que ceux qui y avaient un intérêt particulier, tout en évitant leur divulgation à ceux qui n'y avaient aucun intérêt[75].

[70] *Ibid.*, § 62.
[71] *Ibid.*, § 63.
[72] *Ibid.*, § 64.
[73] *Ibid.*, § 66.
[74] *Ibid.*, § 67.
[75] *Ibid.*, § 68.

La Cour juge également pertinent de souligner que le site de l'autorité fiscale ne fournissait au public aucun moyen d'humilier les personnes concernées, par exemple en publiant des commentaires en dessous des listes en question[76].

Pour la Cour, dans les circonstances de l'espèce, rendre publiques les informations en cause ne saurait être considéré comme une grave intrusion dans la sphère personnelle de la personne concernée. Il n'apparaît pas que la publication de ses données à caractère personnel ait fait peser sur sa vie privée une charge bien plus lourde que ce qui était nécessaire pour servir l'intérêt légitime de l'État[77].

Compte tenu du contexte spécifique dans lequel les informations en cause ont été publiées, du fait que leur publication a été conçue pour garantir la disponibilité et l'accessibilité des informations dans l'intérêt général, et de l'effet limité de cette publication sur la vie quotidienne du requérant, la Cour considère que cette publication relevait de la marge d'appréciation de l'État défendeur[78].

G. Protection contre la cyberviolence

La notion de vie privée inclut l'intégrité physique et psychologique d'une personne que les États ont l'obligation de protéger, même quand le danger provient de particuliers[79]. Les enfants et les autres personnes vulnérables, en particulier, ont droit à une protection efficace[80].

Les actes de cyberviolence, de cyberharcèlement et d'usurpation d'identité malveillante ont été classés comme des formes de violence à l'égard des femmes et des enfants susceptibles de porter atteinte à leur intégrité physique et psychologique en raison de leur vulnérabilité[81].

La Cour rappelle qu'elle a déjà souligné que « le cyberharcèlement est actuellement reconnu comme un aspect de la violence à l'égard des femmes et des filles et peut prendre diverses formes, telles que les cyber-violations de la vie privée… et la prise, le partage et la manipulation d'informations et d'images, y compris intimes » et que dans le contexte de la violence domestique, les partenaires intimes sont souvent les auteurs probables des actes de cyberharcèlement ou de surveillance[82].

[76] *Ibid.*, § 69.
[77] *Ibid.*, § 70.
[78] *Ibid.*, § 71.
[79] Cour eur. D.H., arrêt du 14 septembre 2021, *Volodina c. Russie (n° 2)*, n° 40419/19, § 47.
[80] *Ibid.*, § 47.
[81] *Ibid.*, § 48.
[82] *Ibid.*

La violence en ligne, ou cyberviolence, est étroitement liée à la violence hors ligne, ou « dans la vie réelle », et doit être considérée comme une autre facette du phénomène complexe de la violence domestique[83].

Les divulgations d'informations personnelles, en ce compris sur l'orientation sexuelle, affectent la vie privée de la personne concernée, de même que les abus et les menaces en ligne et hors ligne. L'article 8 est donc applicable[84].

Le fait que la photographie du requérant ainsi que ses adresses de domicile et de travail ont également été rendues publiques, que certaines personnes se sont présentées sur son lieu de travail et que des menaces explicites ont été envoyées sur son profil Facebook signifie que ces commentaires peuvent être considérés comme constituant une véritable menace et, en tant que tels, un discours de haine, dont les victimes doivent être protégées par le droit pénal[85].

Cela suppose que des mesures efficaces soient prises pour identifier et poursuivre les auteurs de ces actes. Toutefois, compte tenu des difficultés liées au maintien de l'ordre dans les sociétés modernes, une obligation positive doit être interprétée de manière à ne pas imposer une charge impossible ou disproportionnée aux autorités[86].

Les États ont l'obligation positive d'établir et d'appliquer effectivement un système sanctionnant toutes les formes de violence domestique et d'offrir des garanties suffisantes aux victimes[87].

L'obligation positive s'applique à toutes les formes de violence domestique, qu'elles se produisent hors ligne ou en ligne[88].

Cette obligation positive comprend notamment :

– l'obligation d'établir et d'appliquer en pratique un cadre juridique adéquat offrant une protection contre la violence des particuliers ;
– l'obligation de prendre les mesures raisonnables afin de prévenir un risque réel et immédiat de violence récurrente dont les autorités avaient ou auraient dû avoir connaissance ;
– l'obligation de mener une enquête effective sur les actes de violence.

La Cour rappelle que les obligations positives de l'État de sauvegarder l'intégrité physique ou psychologique d'un individu peuvent s'étendre aux questions rela-

[83] *Ibid.*, § 49.
[84] Cour eur. D.H., décision du 6 juillet 2021, *Giuliano c. Hongrie*, n° 45305/16, § 27.
[85] *Ibid.*, § 28.
[86] *Ibid.*
[87] Cour eur. D.H., arrêt du 14 septembre 2021, *Volodina c. Russie (n° 2)*, n° 40419/19, § 49.
[88] *Ibid.*

tives à l'efficacité d'une enquête pénale même lorsque la responsabilité pénale des agents de l'État n'est pas en cause[89].

En ce qui concerne les actes qui portent atteinte à l'intégrité psychologique d'un individu, l'obligation d'un cadre juridique adéquat n'exige pas toujours la mise en place d'une disposition pénale couvrant l'acte spécifique. Le cadre juridique pourrait également être constitué de recours de droit civil susceptibles d'offrir une protection suffisante, éventuellement combinés avec des recours procéduraux tels que l'octroi d'une injonction[90].

Tant l'intérêt public que les intérêts de la protection des victimes vulnérables contre les infractions portant atteinte à leur intégrité physique ou psychique exigent la disponibilité d'un recours permettant d'identifier et de traduire en justice l'auteur de l'infraction. La procédure civile, qui aurait pu constituer un recours approprié dans des situations de moindre gravité, n'aurait pas permis d'atteindre ces objectifs en l'espèce[91].

Les autorités de l'État ont la responsabilité de fournir des mesures de protection adéquates aux victimes de violence domestique, sous la forme d'une dissuasion efficace contre les atteintes graves à leur intégrité physique et psychologique[92].

Pour être efficace, une enquête doit être rapide et approfondie. Les autorités doivent prendre toutes les mesures raisonnables pour obtenir des preuves concernant l'incident, y compris des preuves médico-légales. Une diligence particulière est requise dans le traitement des cas de violence domestique, et la nature spécifique de la violence domestique doit être prise en compte dans la conduite de la procédure interne[93].

Le principe d'efficacité signifie que les autorités nationales ne doivent en aucun cas être prêtes à laisser impunies les souffrances physiques ou psychologiques infligées. Ce principe est essentiel pour maintenir la confiance et le soutien de la population dans l'État de droit et pour éviter toute apparence de tolérance ou de collusion des autorités à l'égard des actes de violence[94].

89 *Ibid.*
90 *Ibid.*, § 51.
91 *Ibid.*, § 57.
92 *Ibid.*, § 58.
93 *Ibid.*, § 62.
94 *Ibid.*, § 67.

H. Protection des données dans les procédures judiciaires

1. *Stigmatisation d'un témoin dans un jugement*

La notion de vie privée est un large concept qui recouvre un certain nombre d'aspects relatifs à l'identité personnelle en ce compris l'intégrité physique et psychologique d'une personne. Le droit à la protection de la réputation est compris dans le droit au respect de la vie privée dès lors que la réputation est une partie de l'identité personnelle et de l'intégrité psychologique[95].

Pour que l'article 8 entre en jeu, l'attaque à l'honneur et à la réputation doit atteindre un certain degré de gravité et doit avoir été réalisée de manière à porter atteinte à la jouissance personnelle du droit au respect de la vie privée[96].

À cet égard, la notion de « vie privée » n'exclut pas en principe les activités de nature professionnelle ou commerciale puisque c'est au cours de leur vie professionnelle que la majorité des personnes ont une occasion significative de développer des relations avec le monde extérieur. Une atteinte à la réputation d'un individu qui entrave sa capacité à exercer une activité professionnelle choisie peut donc avoir des effets conséquents sur la jouissance du droit au respect de sa « vie privée » au sens de l'article 8[97].

Par conséquent, la description négative du comportement d'une personne dans une décision judiciaire faisant autorité peut, par la manière dont elle le stigmatisait, avoir un impact majeur sur sa situation personnelle et professionnelle, ainsi que sur son honneur et sa réputation[98].

Dans le contexte spécifique des procédures judiciaires, il incombe avant tout au tribunal de veiller à ce que les droits de l'article 8 des personnes témoignant soient protégés de manière adéquate[99].

Le fait de ne pas avoir informé, interrogé, convoqué ou notifié de toute autre manière une personne d'une plainte à son encontre avant qu'elle ne soit identifiée dans un jugement, couplé au fait de ne pas lui avoir accordé l'anonymat, a violé l'article 8 de la Convention car l'ingérence dans la vie privée de la personne concernée n'était pas assortie de garanties effectives et adéquates[100].

---

[95] Cour eur. D.H., arrêt du 22 juin 2021, *S.W. c. Royaume-Uni*, n° 87/18, § 45.
[96] *Ibid.*, § 46.
[97] *Ibid.*
[98] *Ibid.*
[99] *Ibid.*, § 61.
[100] *Ibid.*

2. *Divulgation de messages électroniques dans le cadre de procédures judiciaires*

La notion de « vie privée » est une notion large, non susceptible d'une définition exhaustive, qui recouvre l'intégrité physique et morale de la personne et peut donc englober de multiples aspects de l'identité d'un individu, tels l'identification et l'orientation sexuelle, le nom, ou des éléments se rapportant au droit à l'image. Elle comprend des informations personnelles dont un individu peut légitimement attendre qu'elles ne soient pas publiées sans son consentement. Cependant, pour que l'article 8 de la Convention entre en ligne de compte, l'atteinte à la réputation personnelle doit présenter un certain niveau de gravité et avoir été effectuée de manière à causer un préjudice à la jouissance personnelle du droit au respect de la vie privée[101].

Des messages électroniques échangés par une personne avec des correspondants masculins sur un site de rencontres occasionnelles sont des messages personnels dont un individu peut légitimement attendre qu'ils ne soient pas dévoilés sans son consentement, et dont la divulgation peut entraîner un sentiment très fort d'intrusion dans la « vie privée » et la « correspondance » visées à l'article 8. La gravité de l'atteinte à la jouissance personnelle du droit au respect à la vie privée dénoncée en l'espèce ne faisant pas de doute, la Cour conclut que de tels messages relèvent bien du champ d'application de cette disposition[102].

3. *Divulgation de l'état de santé en audience publique*

La protection des données à caractère personnel, et notamment des données médicales, revêt une importance fondamentale pour la jouissance par une personne de son droit au respect de sa vie privée et familiale tel que garanti par l'article 8. Par conséquent, le droit interne doit prévoir des garanties appropriées pour empêcher toute communication ou divulgation de données personnelles sur la santé qui serait incompatible avec les garanties de l'article 8[103].

La personne convoquée à comparaître devant un tribunal et qui demande un ajournement pour des raisons de santé peut s'attendre à ce que le certificat médical produit à cet effet fasse l'objet d'un examen ; il aurait dès lors dû demander que cela se fasse à huis clos[104].

En l'espèce, la Cour a retenu les éléments suivants :

– la divulgation n'est intervenue qu'une seule fois ;
– l'information n'a été reprise dans aucune décision ou jugement mais seulement dans l'enregistrement de l'audience ;

[101] Cour eur. D.H., arrêt du 7 septembre 2021, *M.P. c. Portugal*, n° 27516/14, § 33.
[102] *Ibid.*, § 34.
[103] Cour eur. D.H., décision du 14 septembre 2021, *Henryk Stoklosa c. Pologne*, n° 68562/14, § 39.
[104] *Ibid.*, § 43.

– la divulgation ne concerne qu'une affection mineure et passagère ;
– les intérêts des autres parties au procès et le besoin d'assurer le bon déroulement du procès ont été considérés comme étant d'une plus grande importance que l'intérêt de la personne à la protection de la confidentialité de ses données médicales.

I. Protection contre la surveillance (« ciblée »)

1. *Généralités*

La surveillance secrète est une ingérence grave dans le droit au respect de la vie privée d'une personne. En conséquence, l'autorisation judiciaire qui sert de base à cette surveillance ne peut pas être rédigée en des termes si vagues qu'elle laisse place à des spéculations et à des suppositions quant à son contenu et, surtout, quant à la personne à l'égard de laquelle la mesure est appliquée[105].

Quel que soit le système de surveillance en cause, il faut des garanties adéquates et suffisantes contre les abus. Cette appréciation ne revêt qu'un caractère relatif ; elle dépend de toutes les circonstances de la cause, comme[106] :

– la nature, l'étendue et la durée des mesures ;
– les raisons requises pour les ordonner ;
– les autorités compétentes pour les permettre, les exécuter et les contrôler ;
– le type de recours disponible en droit interne.

L'enregistrement des images a un caractère de gravité plus important que l'enregistrement des sons[107].

L'interception de communications privées au moyen d'appareils de radiotransmission et d'enregistrements vidéo et audio, ainsi que la transcription des données obtenues et leur éventuelle utilisation dans le cadre de poursuites pénales, s'analysent en une « ingérence d'une autorité publique » dans l'exercice du droit au respect de sa vie privée[108].

Dans le contexte particulier des mesures de surveillance telles que les interceptions de communications, la « prévisibilité » commande que le droit interne soit suffisamment clair pour indiquer à tous de manière adéquate en quelles circonstances et sous quelles conditions la puissance publique est habilitée à recourir à pareilles mesures. En outre, la loi doit définir l'étendue et les modalités d'exercice du pouvoir d'appréciation accordé aux autorités compétentes avec une clarté suffisante pour fournir à l'individu une protection adéquate contre l'arbitraire[109].

---

105 Cour eur. D.H., arrêt du 22 juillet 2021, *Azer Ahmadov c. Azebaijan*, n° 3409/10, § 71.
106 Cour eur. D.H., arrêt du 18 mai 2021, *Zamfirescu c. Roumanie*, n° 14132/14, § 55.
107 *Ibid.*, § 52.
108 Cour eur. D.H., décision du 15 juin 2021, *Falzarano c. Italie*, n° 73357/14, § 25 ; arrêt du 30 septembre 2021, *Gladkiy et autres c. Russie*, n° 57143/11, § 8.
109 Cour eur. D.H., décision du 15 juin 2021, *Falzarano c. Italie*, n° 73357/14, § 28.

Dans sa jurisprudence relative aux mesures de surveillance dans le cadre des enquêtes pénales, la Cour a déterminé les garanties minimales suivantes contre les abus de pouvoir que la loi doit renfermer[110] :

- la nature des infractions susceptibles de donner lieu à un mandat d'interception ;
- la définition des catégories de personnes susceptibles d'être mises sur écoute ;
- la fixation d'une limite à la durée d'exécution de la mesure ;
- la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies ;
- les précautions à prendre pour la communication des données à d'autres parties ;
- et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements.

En ce qui concerne la vidéosurveillance sur le lieu de travail, l'attente en matière de protection de la vie privée que le salarié peut raisonnablement avoir demeure forte dans les espaces de travail fermés tels que les bureaux[111].

2. *Écoutes téléphoniques*

Les conversations téléphoniques sont couvertes par les notions de « vie privée » et de « correspondance » au sens de l'article 8[112].

Les interceptions téléphoniques et la mise sur écoute sont des ingérences dans le droit au respect de la vie privée[113], en ce compris leur utilisation dans le contexte de procédures disciplinaires[114].

L'utilisation, non autorisée par le droit interne, dans le cadre de procédures disciplinaires, d'enregistrements de conversation téléphonique réalisés dans le cadre de procédures pénales, est une ingérence non prévue par la loi dans l'exercice du droit au respect de la vie privée[115].

3. *Interception et enregistrement de conversations téléphoniques entre un avocat et son client*

Des garanties procédurales spécifiques sont nécessaires lorsqu'il s'agit de protéger la confidentialité des communications entre avocats et clients (comme la destruction effective de ces enregistrements), même si la conversation ne consistait

[110] *Ibid.*, § 29.
[111] Cour eur. D.H., arrêt du 18 mai 2021, *Zamfirescu c. Roumanie*, n° 14132/14, § 52.
[112] Cour eur. D.H., arrêt du 15 juin 2021, *Eksioglu et Mosturoglu c. Turquie*, n^{os} 2006/13 et 10857/13, § 51.
[113] Cour eur. D.H., arrêt du 18 mai 2021, *Zamfirescu c. Roumanie*, n° 14132/14, § 60.
[114] Cour eur. D.H., arrêt du 15 juin 2021, *Eksioglu et Mosturoglu c. Turquie*, n^{os} 2006/13 et 10857/13, § 51.
[115] Cour eur. D.H., arrêt du 18 mai 2021, *Zamfirescu c. Roumanie*, n° 14132/14, § 161 ; arrêt du 15 juin 2021, *Eksioglu et Mosturoglu c. Turquie*, n^{os} 2006/13 et 10857/13, §§ 52-53.

pas en un conseil juridique. En effet, toutes les communications entre eux sont privées et confidentielles et ce, même si l'avocat n'est pas encore formellement mandaté par son client[116].

4. *Surveillance secrète dans le contexte d'enquêtes pénales*

Les mesures de surveillance secrète, y compris l'enregistrement vidéo et audio des communications, constituent des ingérences dans l'exercice du droit au respect de la vie privée. Il incombe aux juridictions internes de procéder à un contrôle juridictionnel effectif de la légalité et de la « nécessité dans une société démocratique » des mesures de surveillance contestées et d'offrir des garanties suffisantes contre l'arbitraire au sens de l'article 8, § 2[117].

Il est de jurisprudence constante que le refus des autorités nationales de divulguer une autorisation de surveillance aux personnes concernées sans raison valable, prive ces dernières de toute possibilité de faire contrôler la légalité des mesures de surveillance et leur « nécessité dans une société démocratique » et que cela constitue une violation de l'article 8[118].

5. *Vidéosurveillance secrète en l'absence d'autorisation judiciaire*

L'exigence d'une autorisation judiciaire préalable pour les opérations de vidéosurveillance secrètes est une garantie procédurale importante contre les ingérences arbitraires dans la vie privée. Une fois que cette garantie est mise en place, les autorités judiciaires doivent fournir des raisons pertinentes et suffisantes pour justifier l'autorisation de procéder à des opérations secrètes[119].

6. *Opération de surveillance par des services secrets*

Il est de jurisprudence constante que les mesures de surveillance secrète et le stockage, le traitement et l'utilisation de données à caractère personnel tombent dans le champ de la notion de vie privée[120].

Étant donné que la mise en œuvre concrète des mesures de surveillance secrète n'est pas soumise au contrôle des personnes concernées ou du public en général, il est contraire au principe de la primauté du droit que la marge d'appréciation accordée par la loi au pouvoir exécutif soit exprimée 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 suffisam-

[116] Cour eur. D.H., arrêt du 16 novembre 2021, *Vasilev c. Bulgarie*, n° 7610/15, §§ 89-90.
[117] Cour eur. D.H., arrêt du 8 juillet 2021, *Borodokin c. Russie*, n° 63614/11, § 6.
[118] *Ibid.*, § 7.
[119] Cour eur. D.H., arrêt du 8 juillet 2021, *Berlizev c. Russie*, n° 43571/12, § 40.
[120] Cour eur. D.H., arrêt du 20 juillet 2021, *Zoltan Varga c. Slovaquie*, n° 58361/12 et 2 autres, § 144.

ment de clarté, compte tenu de l'objectif légitime de la mesure en question, afin d'offrir à l'individu une protection adéquate contre toute ingérence arbitraire[121].

J. Protection contre la surveillance (« en masse »)

1. *Généralités*

La Cour a mis en avant que[122] :

> « Pour chaque individu, le volume de données de communication actuellement disponible est normalement supérieur au volume de données de contenu, car chaque contenu s'accompagne de multiples données de communication. Si le contenu d'une communication, crypté ou non, peut ne rien révéler d'utile sur son expéditeur ou son destinataire, les données de communication associées, en revanche, peuvent révéler un grand nombre d'informations personnelles, telles que l'identité et la localisation de l'expéditeur et du destinataire, ou encore l'équipement par lequel la communication a été acheminée. De plus, toute intrusion occasionnée par l'acquisition de données de communication associées est démultipliée par l'interception en masse, car ces données peuvent désormais faire l'objet d'analyses et de recherches qui permettent de brosser un portrait intime de la personne concernée par le suivi de ses activités sur les réseaux sociaux, de ses déplacements, de ses navigations sur Internet ainsi que de ses habitudes de communication, et par la connaissance de ses contacts ».

L'interception en masse est un processus graduel dans lequel l'intensité de l'ingérence dans l'exercice des droits protégés par l'article 8 augmente au fur et à mesure que le processus avance. Les étapes du processus d'interception en masse peuvent être décrites comme suit[123] :

- interception et rétention initiale des communications et des données de communication associées (c'est-à-dire des données de trafic qui se rapportent aux communications interceptées) ;
- application de sélecteurs spécifiques aux communications retenues et aux données de communication associées ;
- examen par des analystes des communications sélectionnées et des données de communication associées ;
- rétention subséquente des données et utilisation du « produit final », notamment partage de ces données avec des tiers.

Au cours de la première étape, les services de renseignement interceptent en masse des communications électroniques (ou des « paquets » de communications électroniques). Ces communications sont celles d'un grand nombre de personnes,

[121] *Ibid.*, § 151.
[122] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 256 ; *Big Brother Watch et autres c. Royaume-Uni*, n[os] 58170/13, 62322/14 et 24960/15, § 342.
[123] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 239 ; *Big Brother Watch et autres c. Royaume-Uni*, n[os] 58170/13, 62322/14 et 24960/15, § 325.

dont la plupart ne présentent absolument aucun intérêt pour les services de renseignement. Certaines communications peu susceptibles de présenter un intérêt pour le renseignement peuvent être éliminées à ce stade[124].

La recherche initiale, qui est en grande partie automatisée, intervient lors de la seconde étape : différents types de sélecteurs, y compris des « sélecteurs forts » (tels qu'une adresse de courrier électronique) et/ou des requêtes complexes, sont appliqués aux paquets de communications retenus et aux données de communication associées. À ce stade, il est possible que le processus commence à cibler des individus par l'utilisation de sélecteurs forts[125].

Lors de la troisième étape, les éléments interceptés sont examinés pour la première fois par un analyste[126].

Enfin, la quatrième étape est celle où les services de renseignement utilisent concrètement les éléments interceptés. Les éléments retenus peuvent alors être inclus dans un rapport de renseignement, communiqués à d'autres services de renseignement du pays, ou même transmis à des services de renseignement étrangers[127].

L'article 8 s'applique à chacune des étapes décrites ci-dessus. L'intensité de l'ingérence dans l'exercice des droits protégés par l'article 8 augmente au fur et à mesure que le processus d'interception en masse avance[128].

2. *Sur l'existence d'une ingérence*

Le simple fait de conserver des données relatives à la vie privée d'un individu s'analyse en une ingérence au sens de l'article 8. La nécessité de disposer de garanties se fait d'autant plus sentir lorsqu'il s'agit de protéger les données à caractère personnel soumises à un traitement automatique. Le fait que les données retenues soient conservées sous une forme codée intelligible uniquement à l'aide de l'informatique et ne pouvant être interprétée que par un nombre restreint de personnes ne saurait avoir d'incidence sur cette conclusion. En définitive, c'est à la fin du processus, lorsque des informations relatives à une personne en particulier sont analysées ou que le contenu des communications est examiné par un analyste, que la présence de garanties est plus que jamais nécessaire[129].

---

[124] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 240 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 326.
[125] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 241 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 327.
[126] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 242 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, §328.
[127] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 243 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 329.
[128] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 244 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 330.
[129] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 244 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 330.

3. *Sur la prévisibilité de l'ingérence*

En matière de surveillance secrète, la « prévisibilité » ne peut se comprendre de la même façon que dans la plupart des autres domaines. Dans le contexte particulier des mesures de surveillance secrète, telle l'interception de communications, la « prévisibilité » ne saurait signifier qu'un individu doit se trouver à même de prévoir quand les autorités sont susceptibles de recourir à ce type de mesures de manière à ce qu'il puisse adapter sa conduite en conséquence. Cependant, le risque d'arbitraire apparaît avec netteté là où un pouvoir de l'exécutif s'exerce en secret. En matière de mesures de surveillance secrète, il est donc indispensable qu'existent des règles claires et détaillées, d'autant que les procédés techniques utilisables ne cessent de se perfectionner. Le droit interne doit être suffisamment clair pour indiquer à tous de manière adéquate en quelles circonstances et sous quelles conditions la puissance publique est habilitée à recourir à pareilles mesures[130].

En outre, la loi doit définir l'étendue et les modalités d'exercice du pouvoir d'appréciation accordé aux autorités compétentes avec une clarté suffisante pour fournir à l'individu une protection adéquate contre l'arbitraire[131].

En matière d'interception de communications dans le cadre d'enquêtes pénales, la loi doit au minimum prévoir les six éléments suivants pour prévenir les abus de pouvoir[132] :

- la nature des infractions susceptibles de donner lieu à un mandat d'interception ;
- la définition des catégories de personnes dont les communications sont susceptibles d'être interceptées ;
- la limite à la durée d'exécution de la mesure ;
- la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies ;
- les précautions à prendre pour la communication des données à d'autres parties ;
- les circonstances dans lesquelles les données interceptées peuvent ou doivent être effacées ou détruites.

Ces mêmes garanties minimales s'appliquent aussi dans les cas où l'interception était faite pour des raisons de sécurité nationale. Mais il faut en outre tenir compte des éléments suivants[133] :

- les modalités du contrôle de l'application de mesures de surveillance secrète ;

[130] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 247 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 333.
[131] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 247 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 333.
[132] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 249 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 335.
[133] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 249 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 335.

– l'existence éventuelle d'un mécanisme de notification ;
– et les recours prévus en droit interne.

4. *Sur le contrôle et la supervision des mesures de surveillance secrète*

Le contrôle et la supervision des mesures de surveillance secrète peuvent intervenir à trois stades : lorsqu'on ordonne la surveillance, pendant qu'on la mène ou après qu'elle ait cessé.

En ce qui concerne les deux premières phases, la nature et la logique mêmes de la surveillance secrète commandent d'exercer à l'insu de l'intéressé non seulement la surveillance comme telle, mais aussi le contrôle qui l'accompagne. Puisque la personne concernée sera donc nécessairement dans l'impossibilité d'introduire de son propre chef un recours effectif ou de prendre une part directe à quelque procédure de contrôle que ce soit, il est indispensable que les mécanismes existants procurent en eux-mêmes des garanties appropriées et équivalentes sauvegardant les droits de l'individu. En un domaine où les abus sont potentiellement si aisés dans des cas individuels et pourraient entraîner des conséquences préjudiciables pour la société démocratique tout entière, il est en principe souhaitable que le contrôle soit confié à un juge, car le contrôle juridictionnel offre les meilleures garanties d'indépendance, d'impartialité et de procédure régulière[134].

Au troisième stade, c'est-à-dire lorsque la surveillance a cessé, la question de la notification *a posteriori* de mesures de surveillance est un élément pertinent pour apprécier l'effectivité des recours judiciaires et donc l'existence de garanties effectives contre les abus des pouvoirs de surveillance. La personne concernée ne peut guère, en principe, contester rétrospectivement devant la justice la légalité des mesures prises à son insu, sauf si on l'avise de celles-ci ou si toute personne pensant avoir fait l'objet d'une surveillance a la faculté de saisir les tribunaux, ceux-ci étant compétents même si le sujet de la surveillance n'a pas été informé des mesures prises[135].

5. *Sur la nécessité de l'ingérence*

Pour ce qui est de la question de savoir si l'ingérence était « nécessaire dans une société démocratique » à la réalisation d'un but légitime, les autorités nationales disposent d'une ample marge d'appréciation pour choisir les moyens de sauvegarder au mieux la sécurité nationale[136].

---

[134] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 250 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 336.
[135] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 251 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 337.
[136] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 252 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 338.

Cette marge d'appréciation va toutefois de pair avec un contrôle européen portant à la fois sur la loi et sur les décisions qui l'appliquent. La Cour doit être convaincue de l'existence de garanties adéquates et effectives contre les abus car un système de surveillance secrète destiné à protéger la sécurité nationale (ou tout autre intérêt national essentiel) risque de saper, voire de détruire, les processus démocratiques sous couvert de les défendre. L'appréciation de cette question est fonction de toutes les circonstances de la cause, telles que par exemple[137] :

- la nature, la portée et la durée des mesures pouvant être prises ;
- les raisons requises pour les ordonner ;
- les autorités compétentes pour les permettre, les exécuter et les contrôler ;
- et le type de recours fourni par le droit interne.

La Cour vérifie si les procédures de supervision de la décision et de la mise en œuvre de mesures restrictives sont de nature à circonscrire « l'ingérence » à ce qui est « nécessaire dans une société démocratique »[138].

6. *Distinction entre interceptions ciblées et interceptions en masse*

La Cour opère une distinction entre les interceptions ciblées et les interceptions en masse[139]. Elle souligne, notamment, que[140] :

> « Comme tout système d'interception, l'interception en masse recèle à l'évidence un potentiel considérable d'abus susceptibles de porter atteinte au droit des individus au respect de leur vie privée. Certes, l'article 8 de la Convention n'interdit pas de recourir à l'interception en masse afin de protéger la sécurité nationale ou d'autres intérêts nationaux essentiels contre des menaces extérieures graves, et les États jouissent d'une ample marge d'appréciation pour déterminer de quel type de régime d'interception ils ont besoin à cet effet, cependant la latitude qui leur est accordée pour la mise en œuvre de ce régime doit être plus restreinte et un certain nombre de garanties doivent être mises en place ».

[137] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 253 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 339.
[138] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 253 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 339.
[139] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 257 et s. ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 343 et s.
[140] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 261 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 347.

7. *Principes applicables aux interceptions en masse*

La Cour considère qu'il y a lieu d'adapter les principes applicables aux interceptions ciblées aux interceptions en masse[141]. Elle note tout d'abord qu'il est difficile d'appliquer aux interceptions en masse les deux garanties suivantes[142] :

- la nature des infractions susceptibles de donner lieu à un mandat d'interception ;
- la définition des catégories de personnes dont les communications sont susceptibles d'être interceptées.

Toutefois, elle considère que le droit interne doit quand même contenir des règles détaillées prévoyant les circonstances dans lesquelles les autorités peuvent avoir recours à de telles mesures. Le cadre juridique devrait, en particulier, énoncer avec suffisamment de clarté les motifs pour lesquels une interception en masse pourrait être autorisée et les circonstances dans lesquelles les communications d'un individu pourraient être interceptées[143].

Les quatre autres garanties minimales demeurent par contre tout à fait pertinentes pour les interceptions en masse[144] :

- la limite à la durée d'exécution de la mesure ;
- la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies ;
- les précautions à prendre pour la communication des données à d'autres parties ;
- les circonstances dans lesquelles les données interceptées peuvent ou doivent être effacées ou détruites.

8. *Sur le contrôle et la supervision des interceptions en masse : le principe des « garanties de bout en bout »*

Dans le contexte de l'interception en masse, la Cour rappelle que la supervision et le contrôle des mesures revêtent une importance d'autant plus grande que le risque d'abus est inhérent à ce type d'interception et que le besoin légitime d'opérer dans le secret signifie inévitablement que, pour des raisons tenant à la

[141] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 261 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 347.
[142] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 262 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 348. La Cour indique aussi que l'exigence d'un « soupçon raisonnable » était moins pertinente en matière d'interceptions en masse que dans le cadre d'une enquête portant sur une cible précise ou une infraction identifiable.
[143] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 262 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 348.
[144] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 262 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 348.

sécurité nationale, les États ne sont souvent pas libres de divulguer des informations sur le fonctionnement du système en cause[145].

Afin de réduire autant que possible le risque d'abus du pouvoir d'interception en masse, le processus doit être encadré par des « garanties de bout en bout », c'est-à-dire qu'au niveau national, la nécessité et la proportionnalité des mesures prises doivent être appréciées à chaque étape du processus, que les activités d'interception en masse doivent être soumises à l'autorisation d'une autorité indépendante dès le départ (dès la définition de l'objet et de l'étendue de l'opération) et que les opérations doivent faire l'objet d'une supervision et d'un contrôle indépendant opéré *a posteriori*. Ces facteurs sont, de l'avis de la Cour, des garanties fondamentales, qui constituent la pierre angulaire de tout régime d'interception en masse conforme aux exigences de l'article 8[146].

Si l'autorisation judiciaire constitue une « importante garantie contre l'arbitraire », la Cour indique qu'il ne s'agit toutefois pas d'une « exigence nécessaire ». L'interception en masse doit néanmoins être autorisée par un organe indépendant, c'est-à-dire un organe indépendant du pouvoir exécutif[147].

Afin de constituer une garantie effective contre les abus, l'organe indépendant chargé d'accorder les autorisations doit être informé à la fois du but poursuivi par l'interception et des canaux de transmission ou des voies de communication susceptibles d'être interceptés. Cela lui permettra d'apprécier la nécessité et la proportionnalité de l'opération d'interception en masse ainsi que de vérifier si la sélection des canaux est nécessaire et proportionnée aux buts pour lesquels les activités d'interception sont menées[148].

Compte tenu des caractéristiques de l'interception en masse, du grand nombre de sélecteurs employés et du besoin inhérent de flexibilité dans le choix des sélecteurs, qui peut en pratique s'exprimer par des combinaisons techniques de chiffres et de lettres, la Cour accepte d'admettre qu'inclure tous les sélecteurs dans l'autorisation ne serait probablement pas faisable en pratique. Toutefois, étant donné que le choix des sélecteurs et des termes de recherche détermine les communications susceptibles d'être examinées par un analyste, l'autorisation devrait à tout le moins indiquer les types ou catégories de sélecteurs à utiliser[149].

---

[145] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 263 ; *Big Brother Watch et autres c. Royaume-Uni*, n^{os} 58170/13, 62322/14 et 24960/15, § 349.
[146] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 264 ; *Big Brother Watch et autres c. Royaume-Uni*, n^{os} 58170/13, 62322/14 et 24960/15, § 350.
[147] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 265 ; *Big Brother Watch et autres c. Royaume-Uni*, n^{os} 58170/13, 62322/14 et 24960/15, § 351.
[148] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 266 ; *Big Brother Watch et autres c. Royaume-Uni*, n^{os} 58170/13, 62322/14 et 24960/15, § 352.
[149] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 268 ; *Big Brother Watch et autres c. Royaume-Uni*, n^{os} 58170/13, 62322/14 et 24960/15, § 354.

Par ailleurs, des garanties renforcées devraient s'appliquer lorsque les services de renseignement emploient des sélecteurs forts se rapportant à des personnes identifiables. Les services de renseignement devraient être tenus de justifier – au regard des principes de nécessité et de proportionnalité – l'utilisation de chaque sélecteur fort, et cette justification devrait être consignée scrupuleusement et soumise à une procédure d'autorisation interne préalable comportant une vérification distincte et objective de la conformité de la justification avancée aux principes susmentionnés[150].

Chaque stade du processus d'interception en masse[151] doit également être soumis à la supervision d'une autorité indépendante, et cette supervision devrait être suffisamment solide pour circonscrire « l'ingérence » à ce qui est « nécessaire dans une société démocratique »[152].

L'organe de supervision doit, en particulier, être en mesure d'apprécier la nécessité et la proportionnalité de la mesure prise, en tenant dûment compte du degré d'intrusion dans l'exercice par les personnes susceptibles d'être affectées de leurs droits protégés par la Convention. Afin de faciliter cette supervision, les services de renseignement doivent tenir des archives détaillées à chaque étape du processus[153].

Enfin, toute personne qui soupçonne que ses communications ont été interceptées par les services de renseignement doit disposer d'un recours effectif permettant de contester la légalité de l'interception soupçonnée ou la conformité à la Convention du régime d'interception. Dans le contexte des interceptions ciblées, la Cour a considéré à plusieurs reprises que la notification ultérieure des mesures de surveillance était un facteur à prendre en compte pour apprécier le caractère effectif des recours judiciaires et donc l'existence de garanties effectives contre les abus des pouvoirs de surveillance. Elle a toutefois admis que la notification n'était pas nécessaire si le système de recours internes permettait à toute personne soupçonnant que ses communications étaient ou avaient été interceptées de saisir les tribunaux, c'est-à-dire lorsque ceux-ci sont compétents même si l'intéressé n'a pas été informé de l'interception de ses communications[154].

[150] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 269 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 355.
[151] Notamment l'autorisation initiale et ses éventuels renouvellements, la sélection des canaux de transmission, le choix et l'application de sélecteurs et de termes de recherche, l'utilisation, la conservation, la transmission à des tiers et la suppression des éléments interceptés.
[152] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 270 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 356.
[153] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 270 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 356.
[154] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 271 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 357.

Un recours qui ne dépend pas de la notification de l'interception à la personne concernée peut également constituer un recours effectif dans le contexte de l'interception en masse[155].

Les pouvoirs dont dispose l'autorité et les garanties procédurales qu'elle offre sont des éléments à prendre en compte pour apprécier l'effectivité du recours. Par conséquent, en l'absence de toute obligation de notification, il est impératif que le recours relève de la compétence d'un organe qui, sans être nécessairement judiciaire, soit indépendant de l'exécutif, assure l'équité de la procédure et offre, dans la mesure du possible, une procédure contradictoire. Les décisions de cet organe doivent être motivées et juridiquement contraignantes, notamment pour ce qui est d'ordonner la cessation d'une interception irrégulière et la destruction des éléments interceptés obtenus et/ou conservés de manière illégale[156].

9. *Les huit éléments requis pour les interceptions en masse*

Pour déterminer si l'État a agi dans les limites de sa marge d'appréciation, la Cour vérifie si le cadre juridique national fixe clairement les huit éléments suivants[157] :

- les motifs pour lesquels l'interception en masse peut être autorisée ;
- les circonstances dans lesquelles les communications d'un individu peuvent être interceptées ;
- la procédure d'octroi d'une autorisation ;
- les procédures à suivre pour la sélection, l'examen et l'utilisation des éléments interceptés ;
- les précautions à prendre pour la communication de ces éléments à d'autres parties ;
- les limites posées à la durée de l'interception et de la conservation des éléments interceptés, et les circonstances dans lesquelles ces éléments doivent être effacés ou détruits ;
- les procédures et modalités de supervision, par une autorité indépendante, du respect des garanties énoncées ci-dessus, et les pouvoirs de cette autorité en cas de manquement ;
- les procédures de contrôle indépendant *a posteriori* du respect des garanties et les pouvoirs conférés à l'organe compétent pour traiter les cas de manquement.

[155] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 272 ; *Big Brother Watch et autres c. Royaume-Uni*, n^{os} 58170/13, 62322/14 et 24960/15, § 358.
[156] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 273 ; *Big Brother Watch et autres c. Royaume-Uni*, n^{os} 58170/13, 62322/14 et 24960/15, § 359.
[157] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 275 ; *Big Brother Watch et autres c. Royaume-Uni*, n^{os} 58170/13, 62322/14 et 24960/15, § 361.

10. *La transmission des résultats de l'interception en masse à un autre État ou à une organisation internationale*

La transmission, par un État, d'informations obtenues au moyen d'une interception en masse, à des États étrangers ou à des organisations internationales, doit être limitée aux éléments recueillis et conservés d'une manière conforme à la Convention, et être soumise aux garanties supplémentaires suivantes et qui concernent le transfert lui-même[158] :

- les circonstances dans lesquelles pareil transfert peut avoir lieu doivent être clairement énoncées dans le droit interne ;
- l'État qui transfère les informations doit s'assurer que l'État destinataire a mis en place, pour la gestion des données, des garanties de nature à prévenir les abus et les ingérences disproportionnées. L'État destinataire doit, en particulier, garantir la conservation sécurisée des données et restreindre leur divulgation à d'autres parties. Cela ne signifie pas nécessairement qu'il doive garantir une protection comparable à celle de l'État qui transfère les informations, ni qu'une assurance doive être donnée avant chaque transfert ;
- des garanties renforcées sont nécessaires lorsqu'il est clair que les éléments transférés appellent une confidentialité particulière – par exemple s'il s'agit de communications journalistiques confidentielles ;
- le transfert d'informations à des partenaires de renseignement étrangers doit également être soumis à un contrôle indépendant.

11. *Le régime des données de communication associées*

L'interception et la conservation des données de communication associées, ainsi que les recherches effectuées sur celles-ci, doivent être analysées au regard des mêmes garanties que celles applicables au contenu des communications[159].

Cela étant, même si l'interception des données de communication associées est normalement autorisée en même temps que l'interception du contenu des communications, une fois qu'elles ont été obtenues ces données peuvent faire l'objet d'un traitement différent par les services de renseignement. Compte tenu de la nature différente des données de communication associées et des différentes façons dont elles sont utilisées par les services de renseignement, la Cour est d'avis qu'il n'est pas nécessaire que les dispositions juridiques régissant le traitement des données de communication associées soient identiques en tous points à celles régissant le traitement du contenu des communications (pour autant que les garanties requises soient respectées)[160].

---

[158] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 276 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 362.
[159] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 277 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 363.
[160] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Centrum för Rättvisa c. Suède*, § 278 ; *Big Brother Watch et autres c. Royaume-Uni*, n^os^ 58170/13, 62322/14 et 24960/15, § 364. Sur la question de la violation de l'article 10, voyez les n^os^ 428 à 458.

12. *Sur la réception de renseignements provenant de services de renseignement étrangers*

L'interception de communications par des services de renseignement étrangers n'engage pas la responsabilité d'un État destinataire et ne relève pas de sa juridiction au sens de l'article 1 de la Convention, même si l'interception a été réalisée à sa demande. En particulier, l'interception de communications par des services de renseignement étrangers ne relève de la juridiction de l'État destinataire que si celui-ci exerce son autorité ou son contrôle sur ces services[161].

Par contre, il peut y avoir ingérence dans les droits garantis par l'article 8 au stade de la demande initiale et de la réception, la conservation, l'examen et l'utilisation des éléments interceptés par les services de renseignements de l'État destinataire[162].

En conséquence[163] :

- les demandes d'éléments interceptés adressées aux États non contractants doivent avoir une base en droit interne, être accessibles à la personne concernée et prévisibles quant à leurs effets ;
- l'échange de renseignements doit être encadré par des normes claires et précises indiquant à tous de manière suffisante en quelles circonstances et sous quelles conditions les autorités sont habilitées à formuler de telles demandes et offrant des garanties effectives contre l'utilisation de ce pouvoir à des fins de contournement du droit interne et/ou des obligations conventionnelles des États.

Dès la réception des éléments interceptés, l'État destinataire doit avoir mis en place des garanties suffisantes pour leur examen, leur utilisation, leur conservation, leur transmission à des tiers, leur effacement et leur destruction[164].

Ces garanties, qui ont d'abord été énoncées par la Cour dans sa jurisprudence relative à l'interception de communications par les États contractants, s'appliquent également à la réception, par un État contractant, d'éléments interceptés demandés à un service de renseignement étranger[165].

De plus, dès lors que les États ne sont pas toujours en mesure de savoir si des éléments reçus de services de renseignement étrangers sont le produit d'une interception, la Cour considère que les mêmes règles doivent s'appliquer à l'en-

[161] Cour eur. D.H. (GC), arrêt du 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, n[os] 58170/13, 62322/14 et 24960/15, §§ 495-496.
[162] *Ibid.*, § 496.
[163] *Ibid.*, § 497.
[164] *Ibid.*, § 498.
[165] *Ibid.*

semble des éléments reçus de services de renseignement étrangers qui pourraient être le produit d'une interception[166].

Enfin, tout régime autorisant des services de renseignements à demander à des États non contractants de procéder à une interception ou de leur transmettre des éléments interceptés doit être soumis à une supervision indépendante et doit également prévoir la possibilité d'un contrôle *a posteriori* indépendant[167].

K. Protection contre la surveillance en prison

1. *Surveillance de la correspondance reçue par un prisonnier*

L'évaluation du droit d'un détenu condamné au respect de sa correspondance requiert de tenir compte des exigences ordinaires et raisonnables de l'emprisonnement. En ce sens, une certaine mesure de contrôle de la correspondance des détenus est nécessaire et n'est pas en soi incompatible avec la Convention[168].

2. *Protection de la correspondance entre un avocat et son client*

La correspondance avec un avocat, quelle qu'en soit la finalité, se voit appliquer un régime privilégié en vertu de l'article 8. Il en résulte que les autorités pénitentiaires ne peuvent ouvrir une lettre échangée entre un détenu et son avocat que si elles ont des motifs plausibles de penser qu'il y figure un élément illicite non révélé par les moyens normaux de détection. Elles ne peuvent toutefois pas la lire. Il y a lieu de fournir des garanties appropriées pour empêcher la lecture de ce type de lettres, qui consistent par exemple en l'ouverture de l'enveloppe en présence du détenu[169]. Il faut toutefois rappeler que la confidentialité de la correspondance entre un détenu et son défenseur constitue un droit fondamental pour un individu et touche directement aux droits de la défense. C'est pourquoi une dérogation à ce principe ne peut être autorisée que dans des cas exceptionnels et doit s'entourer de garanties adéquates et suffisantes contre les abus[170].

3. *Contrôle des communications téléphoniques en prison*

La détention, comme toute autre mesure privative de liberté, entraîne des limitations inhérentes à la correspondance. Il n'est pas contesté que les communications téléphoniques sont couvertes par les notions de « vie privée » et de « correspondance »[171].

166 *Ibid.*
167 *Ibid.*, § 499. Voyez, pour le surplus, les opinions séparées.
168 Cour eur. D.H., décision du 18 mai 2021, *Maricak c. Slovaquie*, n° 45558/15, § 37.
169 Cour eur. D.H., arrêt du 6 avril 2021, *Kale c. Turquie*, n° 46992/11, § 20 ; arrêt du 6 avril 2021, *Inan c. Turquie*, n° 46154/10, § 23.
170 Cour eur. D.H., arrêt du 6 avril 2021, *Inan c. Turquie*, n° 46154/10, § 24.
171 Cour eur. D.H., arrêt du 29 juin 2021, *Resin c. Russie*, n° 9798/12 et 4 autres, § 94.

Il est essentiel pour le droit au respect de la vie privée et de la correspondance d'un détenu que les autorités lui permettent ou, le cas échéant, l'aident à maintenir des contacts avec le monde extérieur[172].

La surveillance des conversations téléphoniques d'un détenu avec ses représentants devant les juridictions internes et la Cour est une ingérence dans ses droits au titre de l'article 8[173].

Ne permet pas d'assurer une protection juridique contre les ingérences arbitraires des autorités publiques dans le droit du requérant au respect de sa correspondance, le cadre juridique en matière de communications téléphoniques qui prévoit la surveillance de toutes les conversations téléphoniques des détenus en termes généraux sans faire de distinction entre les différentes catégories de communications téléphoniques ni établir la durée ou la portée de la mesure, les raisons qui peuvent justifier son application ou les modalités de son exercice et qui ne prévoit non plus de contrôle indépendant de la portée et de la durée des mesures de censure[174].

4. *Interdiction de communiquer avec ses proches*

Les personnes détenues continuent à jouir de tous leurs droits et libertés, à l'exception du droit à la liberté. L'emprisonnement ne prive pas le détenu des droits conférés par la Convention, en ce compris le droit au respect de la vie familiale[175].

La détention, comme toute autre mesure privant une personne de sa liberté, entraîne des limitations inhérentes à sa vie privée et familiale. Toutefois, le droit d'un détenu au respect de sa vie familiale implique que les autorités pénitentiaires l'aident à maintenir des contacts avec sa famille proche[176].

Toute restriction aux droits d'un détenu doit être justifiée dans chaque cas, bien que cette justification puisse être trouvée dans les considérations de sécurité, en particulier la prévention du crime et du désordre, qui découlent inévitablement des circonstances de l'emprisonnement. En outre, l'approche de l'évaluation de la proportionnalité des mesures étatiques prises par rapport aux « objectifs punitifs » a évolué ces dernières années, l'accent devant désormais être mis davantage sur la nécessité de trouver un juste équilibre entre la punition et la réinsertion des détenus. La réadaptation, c'est-à-dire la réintégration dans la société d'une personne condamnée, est nécessaire dans toute communauté qui a fait de la dignité humaine sa pièce maîtresse. L'article 8 de la Convention impose à

[172] *Ibid.*, § 95.
[173] *Ibid.*, § 96.
[174] *Ibid.*, § 99.
[175] Cour eur. D.H., arrêt du 19 octobre 2021, *Danilevich c. Russie*, n° 31469/08, § 45.
[176] *Ibid.*, § 46.

l'État d'aider, dans la mesure du possible, les détenus à créer et à maintenir des liens avec des personnes extérieures à la prison afin de favoriser leur réinsertion sociale[177].

L'article 8 ne garantit pas aux prisonniers le droit de passer des appels téléphoniques, notamment si la correspondance écrite est possible[178].

La Cour distingue entre l'application d'un régime pénitentiaire spécial pendant l'enquête, lorsque des mesures peuvent raisonnablement être considérées comme nécessaires pour atteindre l'objectif légitime poursuivi, et l'application prolongée d'un tel régime, dont la nécessité doit être évaluée avec le plus grand soin par les autorités compétentes[179].

Une interdiction totale des communications téléphoniques avec les proches est inacceptable et un minimum d'appels téléphoniques doit être autorisé. Aucune restriction supplémentaire ne devrait être imposée aux personnes condamnées à perpétuité en comparaison avec les autres détenus en ce qui concerne les possibilités de maintenir un contact utile avec leurs familles et leurs proches[180].

5. *Vidéosurveillance permanente*

Le placement d'une personne sous vidéosurveillance permanente pendant sa détention est une ingérence grave dans son droit au respect de sa vie privée. Il y a violation de l'article 8 lorsque le droit national n'est pas suffisamment clair, précis ou détaillé et n'offre pas de protection appropriée contre les ingérences arbitraires des autorités dans le droit des détenus au respect de leur vie privée, et que le droit national ne présuppose aucun exercice de mise en balance et ne permet pas à une personne d'obtenir un contrôle juridictionnel de la proportionnalité de son placement sous vidéosurveillance permanente par rapport aux intérêts en jeu dans la protection de sa vie privée[181].

---

177 *Ibid.*, § 47.
178 *Ibid.*, §§ 48-49.
179 *Ibid.*, § 50.
180 *Ibid.*, § 60.
181 Cour eur. D.H., arrêt du 29 avril 2021, *Vasilyev et autres c. Russie*, n° 19289/17 et 22 autres, § 7; arrêt du 29 avril 2021, *Zokirov et autres c. Russie*, n° 3494/17 et 24 autres, § 7; arrêt du 2 décembre 2021, *Gromovoy et Shaydullov c. Russie*, n^{os} 24857/15 et 36001/20, § 7. Voy. aussi: Cour eur. D.H., arrêt du 29 avril 2021, *Lygin et autres c. Russie*, n° 27637/17 et 11 autres, § 7; arrêt du 29 avril 2021, *Firsov et autres c. Russie*, n° 66799/17 et 14 autres, § 7; arrêt du 10 juin 2021, *Galstyan et Medvedev c. Russie*, n^{os} 50796/12 et 38594/18, § 12; *Yarosha et autres c. Russie*, n° 42659/16 et 7 autres, § 7; *Bubnov et autres c. Russie*, n° 52138/17 et 8 autres, § 7; *Kosourov et autres c. Russie*, n° 60283/17 et 3 autres, § 7; *Sukhanskiy et autres c. Russie*, n° 14125/18 et 5 autres, § 7; *Fetisov et autres c. Russie*, n° 25032/18 et 11 autres, § 7; arrêt du 5 octobre 2021, *Koval et autres c. Russie*, n° 29627/10 et 8 autres, § 222; arrêt du 28 octobre 2021, *Alekseyev et autres c. Russie*, n° 42856/16 et 8 autres, § 7; *Yelovskiy et Chakryan c. Russie*, n^{os} 3336/16 et 20490/20, § 7; arrêt du 2 décembre 2021, *Malygin et autres c. Russie*, n° 1011/14 et 3 autres, § 18.

L. Perquisitions et saisies d'équipements informatiques et électroniques

Dans le contexte des perquisitions et des saisies, le droit interne doit offrir une certaine protection à l'individu contre les ingérences arbitraires. Il doit être suffisamment clair dans ses termes pour donner aux citoyens une indication adéquate quant aux circonstances et aux conditions dans lesquelles les autorités publiques sont habilitées à recourir à de telles mesures[182].

Par ailleurs, la Cour a reconnu l'importance de garanties procédurales spécifiques lorsqu'il s'agit de protéger la confidentialité des échanges entre les avocats et leurs clients[183] d'autant qu'une atteinte au secret professionnel des avocats peut avoir des répercussions sur la bonne administration de la justice et donc sur les droits garantis par l'article 6 de la Convention. Les autorités doivent avoir une raison impérieuse pour s'immiscer dans le secret des communications d'un avocat ou dans ses documents de travail[184].

La Convention n'interdit pas d'imposer aux avocats certaines obligations susceptibles de concerner leurs relations avec leurs clients. C'est notamment le cas lorsqu'il existe des preuves crédibles de la participation d'un avocat à une infraction, ou dans le cadre de la lutte contre certaines pratiques. À ce titre, il est toutefois indispensable d'encadrer strictement de telles mesures, car l'avocat occupe une position essentielle dans l'administration de la justice et peut, en vertu de son rôle d'intermédiaire entre les justiciables et les tribunaux, être qualifié d'auxiliaire de justice[185].

M. Registres de police et casiers judiciaires

1. *Registre de police*

La conservation de données relatives à la vie privée tombe dans le champ de l'article 8, § 1er[186].

La collecte et le stockage par la police de données relatives à un individu en particulier constituent une ingérence dans la vie privée de cette personne[187].

La conservation des données à caractère personnel d'un individu au motif de son appartenance à une communauté religieuse particulière est une ingérence dans sa vie privée telle que protégée par l'article 8 lu à la lumière de l'article 9[188].

---

182 Cour eur. D.H., arrêt du 16 novembre 2021, *Sargava c. Estonie*, n° 698/19, § 87.
183 *Ibid.*, § 88.
184 Cour eur. D.H., arrêt du 21 janvier 2021, *Kadura et Smaliy c. Ukraine*, nos 42753/14 et 43860/14, § 142.
185 Cour eur. D.H., arrêt du 16 novembre 2021, *Sargava c. Estonie*, n° 698/19, § 89.
186 Cour eur. D.H., arrêt du 28 septembre 2021, *Kuropyatnik c. Russie*, n° 64403/11, § 35.
187 *Ibid.*, § 40.
188 *Ibid.*

2. *Casier judiciaire*

Tant la conservation que la diffusion d'informations relatives à la vie privée d'un individu relèvent de l'article 8, § 1er[189].

Conformément à la jurisprudence constante de la Cour, même des informations publiques peuvent relever de la vie privée lorsqu'elles sont systématiquement collectées et conservées dans des fichiers détenus par les autorités[190].

Des informations telles que le casier judiciaire d'une personne, lorsqu'elles sont systématiquement collectées et conservées dans un fichier détenu par les agents de l'État, tombent dans le champ de la « vie privée » au sens de l'article 8, § 1er [191].

Le fait de rendre accessible à des tiers des informations relatives aux condamnations antérieures d'une personne constitue une ingérence dans le droit au respect de la vie privée de celle-ci[192].

La divulgation de renseignements sur casier judiciaire d'une personne dans un certificat de casier judiciaire constitue aussi une ingérence dans le droit au respect de la vie privée de cette personne[193].

Les lacunes des dispositions relatives à la conservation des données contenues dans le casier judiciaire peuvent être corrigées par le renforcement des garanties applicables à la divulgation de ces données[194].

Il y a un intérêt manifeste à ce que les personnes qui postulent à un emploi dans des domaines sensibles puissent savoir à l'avance quelles condamnations seront divulguées dans certificat de casier judiciaire[195].

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

1. *Protection de la réputation*

Le droit à la protection de la réputation est un droit protégé par l'article 8 en tant qu'élément du droit au respect de la vie privée[196].

189 Cour eur. D.H., arrêt du 30 novembre 2021, *X. c. La République de Moldavie*, n° 43529/13, § 26.
190 *Ibid.*, § 26.
191 *Ibid.*, § 27.
192 *Ibid.*, § 29.
193 Cour eur. D.H., arrêt du 30 mars 2021, *M.C. c. Royaume-Uni*, n° 51220/13, § 46.
194 *Ibid.*, § 48.
195 *Ibid.*, § 53.
196 Cour eur. D.H., décision du 4 février 2021, *De Carvalho Basso c. Portugal*, nos 73053/14 et 33075/17, § 42 ; arrêt du 9 février 2021, *Sagdic c. Turquie*, n° 9142/16, § 25 ; arrêt du 21 septembre 2021, *Milosavljevic c. Serbie (n° 2)*, n° 47274/19, §§ 55 et 67 ; arrêt du 30 novembre 2021, *Tiriac c. Roumanie*, n° 51107/16, § 60.

La réputation d'une personne fait partie de son identité personnelle et de son intégrité morale, et elle relève de la vie privée même si les critiques dont la personne fait l'objet sont exprimées dans le cadre d'un débat public[197]. Les mêmes considérations s'appliquent à l'honneur d'une personne[198].

Pour que l'article 8 trouve à s'appliquer, 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[199] et ce, tant pour la réputation en général qu'en ce qui concerne la réputation professionnelle[200].

L'article 8 ne peut pas être invoqué pour se plaindre d'une atteinte à la réputation qui est la conséquence prévisible de ses propres actes, comme, par exemple, la commission d'une infraction pénale[201]. Toutefois, une condamnation pénale ne prive pas la personne condamnée de son droit à l'oubli, *a fortiori* si cette condamnation est devenue caduque. En effet, même si une personne peut acquérir une certaine notoriété lors d'un procès, l'intérêt du public pour l'infraction et, par conséquent, la notoriété de la personne, peut diminuer avec le temps. Ainsi, après un certain temps, les personnes qui ont été condamnées ont intérêt à ne plus être confrontées à leurs actes, en vue de leur réintégration dans la société. Cela peut être particulièrement vrai lorsqu'une personne condamnée a été définitivement libérée[202].

2. *Protection des données*

Lorsqu'il y a eu compilation de données sur une personne en particulier, traitement ou utilisation de données à caractère personnel ou publication d'une manière ou à un degré dépassant ce qui est normalement prévisible, des considérations relatives à la vie privée apparaissent. La protection des données à caractère personnel revêt une importance fondamentale pour la jouissance par une personne de son droit au respect de sa vie privée et familiale. Le droit interne doit offrir des garanties appropriées pour empêcher toute utilisation des données à caractère personnel qui serait incompatible avec les garanties de cet article. L'article 8 prévoit ainsi le droit à une forme d'autodétermination informationnelle, permettant aux individus d'invoquer leur droit à la vie privée à l'égard de données qui, bien que neutres, sont collectées, traitées et diffusées collectivement et sous

197 Cour eur. D.H., arrêt du 9 février 2021, *Sagdic c. Turquie*, n° 9142/16, § 25 ; arrêt du 14 décembre 2021, *Samoylova c. Russie*, n° 49108/11, § 60.
198 Cour eur. D.H., arrêt du 9 février 2021, *Sagdic c. Turquie*, n° 9142/16, § 25.
199 Cour eur. D.H., décision du 4 février 2021, *De Carvalho Basso c. Portugal*, n°s 73053/14 et 33075/17, § 43 (voyez-en une application au § 58) ; arrêt du 9 février 2021, *Sagdic c. Turquie*, n° 9142/16, § 25 ; arrêt du 25 mars 2021, *Matalas c. Grèce*, n° 1864/18, § 39 ; arrêt du 27 juillet 2021, *SIC (Sociedade independente de comunicaçao) c. Portugal*, n° 29856/13, § 60 ; arrêt du 21 septembre 2021, *Milosavljevic c. Serbie (n° 2)*, n° 47274/19, § 55 ; arrêt du 30 novembre 2021, *Tiriac c. Roumanie*, n° 51107/16, § 60.
200 Cour eur. D.H., arrêt du 30 novembre 2021, *Tiriac c. Roumanie*, n° 51107/16, § 60.
201 Cour eur. D.H., arrêt du 25 mars 2021, *Matalas c. Grèce*, n° 1864/18, § 39 ; arrêt du 14 octobre 2021, *M.L. c. Slovaquie*, n° 34159/17, § 38.
202 Cour eur. D.H., arrêt du 14 octobre 2021, *M.L. c. Slovaquie*, n° 34159/17, § 38.

une forme ou d'une manière telle que leurs droits au titre de l'article 8 peuvent être engagés[203].

La notion de « vie privée » englobe les informations personnelles dont les individus peuvent légitimement s'attendre à ce qu'elles ne soient pas publiées sans leur consentement. La Cour a précédemment jugé que les données collectées, traitées et publiées par des sociétés privées, fournissant des détails sur les revenus imposables gagnés et non gagnés ainsi que sur le patrimoine net imposable, concernaient la « vie privée » de ces personnes, nonobstant le fait que, en vertu du droit national, ces données pouvaient être accessibles, selon certaines règles, au public[204].

Le nom complet d'une personne relève de la « vie privée » au sens de l'article 8, § 1er, de la Convention. L'adresse du domicile d'une personne relève également de la « vie privée »[205].

3. *Distinction entre une personne « ordinaire » et une personnalité « publique »*

Il faut distinguer les particuliers des personnes agissant dans un contexte public en tant que personnalités politiques ou personnalités publiques. Les limites de la critique acceptable sont plus larges à l'égard d'un homme politique, visé en cette qualité, qu'à l'égard d'un particulier inconnu du public. Ce principe s'applique non seulement aux hommes politiques, mais aussi à toute personne faisant partie de la sphère publique, que ce soit par ses actions ou par sa position. Toutefois, si le fait de relater des faits réels concernant la vie privée d'hommes politiques ou d'autres personnes publiques peut être admissible dans certaines circonstances, même les personnes connues du public ont des attentes légitimes en matière de protection et de respect de leur vie privée[206].

Comme pour les hommes politiques, les limites de la critique admissible sont plus larges pour les fonctionnaires agissant dans l'exercice de leurs fonctions officielles que pour les simples particuliers. Cependant, on ne saurait dire que des fonctionnaires s'exposent sciemment à un contrôle attentif de leurs faits et gestes exactement comme les hommes politiques[207].

---

203 Cour eur. D.H., arrêt du 14 décembre 2021, *Samoylova c. Russie*, n° 49108/11, § 60.
204 *Ibid.*, § 62.
205 *Ibid.*, § 63.
206 Voyez : Cour eur. D.H., arrêt du 30 novembre 2021, *Tiriac c. Roumanie*, n° 51107/16, § 85 ; décision du 4 février 2021, *De Carvalho Basso c. Portugal*, nos 73053/14 et 33075/17, § 50 ; arrêt du 7 décembre 2021, *Danes et autres c. Roumanie*, n° 44332/16 et 2 autres, § 49 ; arrêt du 14 décembre 2021, *Samoylova c. Russie*, n° 49108/11, § 75.
207 Cour eur. D.H., arrêt du 9 février 2021, *Sagdic c. Turquie*, n° 9142/16, § 33. Voy. aussi le cas de l'arrêt du 16 novembre 2021, *Vacean c. Roumanie*, n° 47695/14, § 42, la décision du 30 novembre 2021, *Harbuz c. Roumanie*, n° 73064/17, § 14, et l'arrêt du 14 décembre 2021, *Samoylova c. Russie*, n° 49108/11, § 75.

4. *Le rôle de la presse, ses droits et obligations*

La presse joue un rôle éminent dans une société démocratique : si elle ne doit pas franchir certaines limites, tenant notamment à la protection de la réputation et aux droits d'autrui ainsi qu'à la nécessité d'empêcher la divulgation d'informations confidentielles, il lui incombe néanmoins 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 ». Les journalistes doivent cependant agir de bonne foi, sur la base de faits exacts, et fournir des informations « fiables et précises » dans le respect de l'éthique journalistique[208].

En effet, la protection que l'article 10 offre aux journalistes est subordonnée à la condition qu'ils agissent de bonne foi de manière à fournir des informations exactes et dignes de crédit dans le respect des principes d'un journalisme responsable. Le concept de journalisme responsable, activité professionnelle protégée par l'article 10, est une notion qui ne couvre pas uniquement le contenu des informations recueillies et/ou diffusées par des moyens journalistiques, mais aussi la licéité du comportement des journalistes. Le fait qu'un journaliste ait enfreint la loi doit être pris en compte, mais il n'est pas déterminant pour établir s'il a agi de manière responsable[209].

Une distorsion de la réalité, opérée de mauvaise foi, peut parfois transgresser les limites de la critique acceptable : 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. Ainsi, la mission d'information comporte nécessairement des devoirs et des responsabilités ainsi que 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 livrer ces personnes à la vindicte publique[210].

Il doit exister des motifs spécifiques pour relever les médias de l'obligation ordinaire qui leur incombe de vérifier que les déclarations factuelles qu'ils publient à l'égard de particuliers ne sont pas diffamatoires. À cet égard, entrent spécialement en jeu la nature et le degré de la diffamation en cause et la question de savoir à quel point le média peut raisonnablement considérer ses sources comme crédibles pour ce qui est des allégations qu'il entend publier[211].

---

[208] Cour eur. D.H., arrêt du 9 février 2021, *Sagdic c. Turquie*, n° 9142/16, § 26 ; arrêt du 14 décembre 2021, *Samoylova c. Russie*, n° 49108/11, § 76.
[209] Cour eur. D.H., arrêt du 9 février 2021, *Sagdic c. Turquie*, n° 9142/16, § 27.
[210] *Ibid.*, § 28.
[211] *Ibid.*, § 39.

Malgré le rôle essentiel qui revient aux médias dans une société démocratique, les journalistes ne sauraient en principe être déliés, par la protection que leur offre l'article 10, de leur devoir de respecter les lois pénales de droit commun[212].

Dans le cadre d'une requête introduite sous l'angle de l'article 10, la Cour vérifie en outre le mode d'obtention des informations et leur véracité ainsi que la gravité de la sanction imposée aux journalistes ou aux éditeurs[213].

Lorsqu'elle contribue au débat public sur des questions d'intérêt légitime et qu'elle agit de bonne foi, la presse devrait normalement être autorisée à s'appuyer sur le contenu des rapports officiels sans avoir à entreprendre des recherches indépendantes. Cela signifie que les journalistes doivent être libres de rendre compte d'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[214].

5. *La mise en la balance du droit au respect de la vie privée et du droit à la liberté d'expression*

Conformément à la jurisprudence établie de longue date de la Cour, les critères pertinents à prendre en considération dans la mise en balance du droit au respect de la vie privée et du droit à la liberté d'expression sont les suivants[215] :

- 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.

6. *Nécessité de distinguer entre déclarations de fait et jugements de valeur*

Il faut distinguer entre déclarations de fait et jugements de valeur. La matérialité des déclarations de fait peut se prouver ; en revanche, les jugements de valeur ne se prêtant pas à une démonstration de leur exactitude, l'obligation de les prouver est impossible à remplir et porte atteinte à la liberté d'opinion elle-même. Cependant, 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 liti-

[212] *Ibid.*, § 41.
[213] Cour eur. D.H., arrêt du 25 mars 2021, *Matalas c. Grèce*, n° 1864/18, § 41. À propos de la sévérité de la sanction, voyez not. l'arrêt du 21 septembre 2021, *Milosavljevic c. Serbie (n° 2)*, n° 47274/19, §§ 69-70, et l'arrêt du 14 décembre 2021, *Samoylova c. Russie*, n° 49108/11, § 74.
[214] Cour eur. D.H., arrêt du 14 décembre 2021, *Samoylova c. Russie*, n° 49108/11, § 89.
[215] Cour eur. D.H., arrêt du 9 février 2021, *Sagdic c. Turquie*, n° 9142/16, § 29 ; arrêt du 25 mars 2021, *Matalas c. Grèce*, n° 1864/18, § 41 ; arrêt du 16 novembre 2021, *Vacean c. Roumanie*, n° 47695/14, § 36 ; arrêt du 30 novembre 2021, *Tiriac c. Roumanie*, n° 51107/16, § 74 ; arrêt du 7 décembre 2021, *Danes et autres c. Roumanie*, n° 44332/16 et 2 autres, § 35 ; arrêt du 14 décembre 2021, *Samoylova c. Russie*, n° 49108/11, § 74.

gieux ; à défaut, ce jugement de valeur pourrait se révéler 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[216].

7. *Contribution à un débat d'intérêt général*

En ce qui concerne la contribution à un débat d'intérêt général, la Cour rappelle que l'article 10, § 2, laisse peu de place aux restrictions au discours politique ou au débat sur des questions d'intérêt public. La marge d'appréciation des États est donc réduite lorsqu'il s'agit d'un débat sur une question d'intérêt public. Pour savoir si une publication concernant la vie privée d'un individu n'est pas destinée à satisfaire uniquement la curiosité d'un certain lectorat, mais porte également sur un sujet d'importance générale, il convient d'apprécier la publication dans son ensemble et d'examiner si, compte tenu du contexte dans lequel elle apparaît, elle se rapporte à une question d'intérêt public[217].

À cet égard, la Cour précise que l'intérêt public concerne les questions qui touchent le public à un point tel qu'il peut légitimement s'y intéresser, qui attirent son attention ou qui le concernent de manière significative, notamment en ce qu'elles affectent le bien-être des citoyens ou la vie de la communauté. Il en va de même pour les questions susceptibles de susciter une controverse considérable, qui concernent une question sociale importante ou qui impliquent un problème sur lequel le public aurait intérêt à être informé[218].

La contribution de la presse à un débat d'intérêt public ne se limite pas à l'actualité ou à des débats préexistants. Certes, la presse est un vecteur de diffusion des débats sur des questions d'intérêt public, mais elle a également pour rôle de révéler et de porter à la connaissance du public des informations susceptibles de susciter un tel intérêt et de donner lieu à un tel débat au sein de la société[219].

8. *Contenu, forme et répercussion des publications*

En ce qui concerne le contenu, la forme et les répercussions des publications, la Cour rappelle que les journalistes ont la responsabilité première de protéger les individus, y compris les personnalités publiques, contre toute intrusion dans leur vie privée. Les choix qu'ils font à cet égard doivent être fondés sur les règles

[216] Cour eur. D.H., arrêt du 9 février 2021, *Sagdic c. Turquie*, n° 9142/16, § 29 ; arrêt du 25 mars 2021, *Matalas c. Grèce*, n° 1864/18, § 47 (voy. aussi le § 51). Voy. aussi les arrêts des 21 septembre 2021, *Milosavljevic c. Serbie (n° 2)*, n° 47274/19, § 63 ; 6 novembre 2021, *Vacean c. Roumanie*, n° 47695/14, § 37 ; 30 novembre 2021, *Tiriac c. Roumanie*, n° 51107/16, § 78 ; 7 décembre 2021, *Danes et autres c. Roumanie*, n° 44332/16 et 2 autres, § 39.
[217] Cour eur. D.H., arrêt du 30 novembre 2021, *Tiriac c. Roumanie*, n° 51107/16, § 81 ; arrêt du 7 décembre 2021, *Danes et autres c. Roumanie*, n° 44332/16 et 2 autres, § 43.
[218] Cour eur. D.H., arrêt du 30 novembre 2021, *Tiriac c. Roumanie*, n° 51107/16, § 82.
[219] *Ibid.*, § 76.

éthiques et les codes de conduite de leur profession. Même si les journalistes jouissent de la liberté de choisir, parmi les informations qui leur parviennent, celles qu'ils vont traiter et la manière dont ils vont le faire, cette liberté n'est pas dénuée de responsabilités[220]. Par ailleurs, les personnes qui prennent part à un débat public sur un sujet d'intérêt général sont autorisées à recourir à un certain degré d'exagération, voire de provocation, ou en d'autres termes à faire des déclarations quelque peu immodérées[221].

Le cas échéant, il faut tenir compte de l'ampleur de la diffusion des articles litigieux sur l'Internet ainsi que l'accessibilité de ces articles et leur impact sur la personne concernée. La Cour rappelle à cet égard que les communications en ligne et leur contenu risquent assurément bien plus que dans la presse [classique] de porter atteinte à l'exercice et à la jouissance des droits et libertés fondamentaux, en particulier du droit au respect de la vie privée[222].

9. *Publication d'images*

La notion de « vie privée » est un concept large qui s'étend à un certain nombre d'aspects liés à l'identité personnelle, tels que le nom ou l'image d'une personne, et inclut en outre l'intégrité physique et psychologique d'une personne. Ce concept comprend aussi le droit de vivre à l'abri des regards indiscrets[223].

L'image d'une personne constitue l'un des principaux attributs de sa personnalité, car elle révèle les caractéristiques uniques de cette personne et la distingue des autres. Le droit de chaque personne à la protection de son image présuppose le droit de contrôler l'utilisation de cette image. S'il implique dans la plupart des cas la possibilité de refuser la publication de l'image, il couvre également le droit de la personne de s'opposer à l'enregistrement, la conservation et la reproduction de l'image[224].

Les critères pertinents à prendre en considération dans la mise en balance du droit au respect de la vie privée et du droit à la liberté d'expression sont les suivants[225] :

- 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 ;
- les circonstances dans lesquelles les photographies ont été prises[226].

220 *Ibid.*, § 92 ; arrêt du 7 décembre 2021, *Danes et autres c. Roumanie*, n° 44332/16 et 2 autres, § 56.
221 Cour eur. D.H., arrêt du 30 novembre 2021, *Tiriac c. Roumanie*, n° 51107/16, § 97.
222 Cour eur. D.H., arrêt du 16 novembre 2021, *Vacean c. Roumanie*, n° 47695/14, § 52.
223 Cour eur. D.H., arrêt du 1er juillet 2021, *Hajovsky c. Slovaquie*, n° 7796/16, § 29.
224 *Ibid.*, § 29.
225 *Ibid.*, § 30 ; arrêt du 14 octobre 2021, *M.L. c. Slovaquie*, n° 34159/17, § 35.
226 Voy. not. les §§ 45 et 46 à 49 de l'arrêt du 1er juillet 2021, *Hajovsky c. Slovaquie*, n° 7796/16.

Bien que la liberté d'expression comprenne la publication de photographies, il s'agit néanmoins d'un domaine dans lequel la protection des droits et de la réputation d'autrui revêt une importance particulière, car les photographies peuvent contenir des informations très personnelles, voire intimes, sur un individu et sa famille[227].

Une attention particulière doit être accordée à la contribution apportée par les photographies ou les articles à un débat d'intérêt général. À cet égard, il faut distinguer entre le fait de rapporter des faits (même controversés) susceptibles de contribuer à un débat dans une société démocratique, et le fait de rapporter des détails de la vie privée d'un individu qui n'exerce pas de fonctions officielles. Alors que dans le premier cas, la presse exerce son rôle vital de « chien de garde » dans une démocratie en communiquant des informations et des idées sur des questions d'intérêt public, elle ne le fait pas dans le second cas. Lorsque la situation ne relève d'aucun débat politique ou public et que les photographies publiées et les commentaires qui les accompagnent portent exclusivement sur des détails de la vie privée de la personne dans le seul but de satisfaire la curiosité d'un lectorat particulier, la liberté d'expression appelle une interprétation plus étroite[228].

10. *Déclarations dénigrantes*

Conformément à la jurisprudence de la Cour en matière de déclarations dénigrantes à l'encontre de fonctionnaires faites dans le cadre de plaintes écrites adressées aux autorités, la Cour examine la proportionnalité de l'ingérence en prenant en compte[229] :

- la nature et le mode exact de communication des déclarations ;
- le contexte respectif dans lequel elles ont été faites ;
- la mesure dans laquelle elles ont affecté la personne concernée ;
- la sévérité des sanctions infligées.

Ce raisonnement s'applique également aux cas de diffamation résultant de déclarations contenues dans des documents privés entre particuliers et qui n'étaient pas destinées par leur auteur à être diffusées publiquement mais qui ont été portées à la connaissance d'un nombre restreint de personnes[230].

[227] Cour eur. D.H., arrêt du 1er juillet 2021, *Hajovsky c. Slovaquie*, n° 7796/16, § 31.
[228] *Ibid.*
[229] Cour eur. D.H., arrêt du 25 mars 2021, *Matalas c. Grèce*, n° 1864/18, § 42.
[230] *Ibid.*, § 46.

11. *Divulgation de données privées lors d'une émission télévisée*

La notion de « vie privée » au sens de l'article 8, § 1er, est un concept large qui ne se prête pas à une définition exhaustive. Il comprend le droit de vivre à l'abri des regards indiscrets[231].

12. *Divulgation de courriers électroniques*

Conformément à la jurisprudence constante de la Cour, il faut prendre en considération les critères pertinents suivants dans le cadre de la mise en balance de l'article 8 et de l'article 10[232] :

- la contribution à un débat d'intérêt public ;
- le degré de notoriété de la personne concernée ;
- le sujet du reportage ;
- le comportement préalable de la personne concernée ;
- le contenu, la forme et les conséquences de la publication.

Le seul fait que des courriers électroniques aient été obtenus par un tiers, en violation de la loi, ne saurait priver l'éditeur (ou les journalistes) de la protection de l'article 10[233], d'autant que la publication de ces courriers n'est pas une infraction pénale.

La présentation d'un article de presse et le style utilisé relèvent d'une décision éditoriale, sur laquelle ni la Cour ni les juridictions nationales n'ont à porter de jugement[234].

Si la liberté journalistique n'est pas illimitée et que la presse ne doit pas dépasser certaines limites, même la diffusion de conversations téléphoniques enregistrées secrètement ou de matériel provenant d'une caméra cachée peut être protégée par l'article 10 si une question d'intérêt général est en jeu[235].

13. *Compatibilité des sanctions pénales*

L'imposition d'une peine d'emprisonnement dans les cas de diffamation ne peut être compatible avec la liberté d'expression que dans des circonstances exceptionnelles – notamment lorsque d'autres droits fondamentaux ont été gravement atteints, comme, par exemple, dans le cas de discours de haine ou d'incitation à la violence[236].

---

231 Cour eur. D.H., arrêt du 14 décembre 2021, *Samoylova c. Russie*, n° 49108/11, § 59.
232 Cour eur. D.H., décision du 12 octobre 2021, *Speer c. Allemagne*, n° 35244/15, § 22.
233 *Ibid.*, § 28.
234 *Ibid.*, § 31.
235 *Ibid.*
236 Cour eur. D.H., arrêt du 25 mars 2021, *Matalas c. Grèce*, n° 1864/18, § 59.

Jean Herveg et Jean-Marc Van Gyseghem

O. Protection des données et l'Internet

1. *Désindexation (déréférencement) d'un article accessible sur l'Internet*

Il faut distinguer entre la désindexation et le retrait permanent ou l'effacement d'articles d'information publiés par la presse[237].

2. *Le droit à l'oubli et les archives accessibles sur l'Internet*

Dans le cadre de l'examen d'une publication initiale, la Cour a fixé depuis longtemps les principes pertinents qui doivent guider l'appréciation de la nécessité d'une ingérence. Il s'agit de prendre en considération dans le contexte de la mise en balance du droit à la liberté d'expression et du droit au respect de la vie privée les critères suivants[238] :

- la contribution à un débat d'intérêt général ;
- la notoriété de la personne visée et l'objet du reportage ;
- le comportement antérieur de la personne concernée ;
- le mode d'obtention des informations et leur véracité ;
- le contenu, la forme et les répercussions de la publication ;
- et la gravité de la mesure imposée.

Selon la jurisprudence constante de la Cour, la condition de la « nécessité dans une société démocratique » requiert de déterminer si l'ingérence correspond à un besoin social impérieux et, en particulier, si les motifs fournis par les autorités nationales pour la justifier sont pertinents et suffisants et si la mesure est proportionnée au but légitime poursuivi[239].

Sur le terrain de l'article 10, les États contractants disposent d'une certaine marge d'appréciation pour juger de la nécessité et de l'ampleur d'une ingérence dans la liberté d'expression protégée par cette disposition. Toutefois, cette marge va de pair avec un contrôle européen portant à la fois sur la loi et sur les décisions qui l'appliquent, même quand elles émanent d'une juridiction indépendante. Dans l'exercice de son pouvoir de contrôle, la Cour n'a pas pour tâche de se substituer aux juridictions nationales, mais il lui incombe de vérifier, à la lumière de l'ensemble de l'affaire, si les décisions qu'elles ont rendues en vertu de leur pouvoir d'appréciation se concilient avec les dispositions invoquées de la Convention[240].

La Cour rappelle qu'au rôle premier de la presse s'ajoute une fonction accessoire mais néanmoins d'une importance certaine, qui consiste à constituer des archives

[237] Cour eur. D.H., arrêt du 25 novembre 2021, *Biancardi c. Italie*, n° 77419/16, § 59.
[238] Cour eur. D.H., arrêt du 22 juin 2021, *Hurbain c. Belgique*, n° 57292/16, § 94 (cette affaire fait l'objet d'un renvoi devant la Grande Chambre).
[239] *Ibid.*, § 95.
[240] *Ibid.*, § 96.

à partir d'informations déjà publiées et à les mettre à la disposition du public. La mise à disposition d'archives sur l'Internet contribue grandement à la préservation et à l'accessibilité de l'actualité et des informations. Les archives numériques constituent en effet une source précieuse pour l'enseignement et les recherches historiques, notamment en ce qu'elles sont immédiatement accessibles au public et généralement gratuites[241]. Par conséquent, les droits d'une personne ayant fait l'objet d'une publication disponible sur l'Internet doivent donc être mis en balance avec le droit du public à s'informer sur des événements du passé et de l'histoire contemporaine, notamment à l'aide des archives numériques de la presse[242].

L'obligation d'examiner à un stade ultérieur la licéité du maintien en ligne d'un reportage à la suite d'une demande de la personne concernée, et qui implique une mise en balance de tous les intérêts en jeu, comporte le risque que la presse s'abstienne de conserver des reportages dans ses archives en ligne ou qu'elle omette des éléments individualisés dans des reportages susceptibles de faire ultérieurement l'objet d'une telle demande[243].

La Cour indique qu'elle est également consciente du fait que la modification de la version archivée d'un article porte atteinte à l'intégrité des archives, qui en constitue l'essence même. Les juridictions internes doivent donc être particulièrement vigilantes lorsqu'elles font droit à une demande d'anonymisation ou de modification de la version électronique d'un article archivé pour les besoins du droit au respect de la vie privée[244].

Cela étant dit, le droit de maintenir des archives en ligne à la disposition du public n'est pas un droit absolu. Il doit être mis en balance avec les autres droits en présence. Dans ce cadre, de l'avis de la Cour, les critères qui doivent être pris en compte quand est concernée la mise en ligne ou le maintien à disposition d'une publication archivée sont en principe les mêmes que ceux utilisés par la Cour dans le cadre d'une publication initiale. Certains d'entre eux peuvent toutefois revêtir plus ou moins de pertinence eu égard aux circonstances de l'espèce et au passage du temps[245].

En ce qui concerne la forme de la publication, la Cour rappelle que les sites internet sont des outils d'information et de communication qui se distinguent particulièrement de la presse écrite, notamment quant à leur capacité à emmagasiner et à diffuser l'information, et que les communications en ligne et leur contenu risquent bien plus que des publications sur support papier de porter atteinte à l'exercice et à la jouissance des droits et libertés fondamentaux, en particulier du droit au respect de la vie privée[246].

---

241 *Ibid.*, § 100.
242 *Ibid.*, § 101.
243 *Ibid.*, § 102.
244 *Ibid.*, § 103.
245 *Ibid.*, § 104.
246 Cour eur. D.H., arrêt du 22 juin 2021, *Hurbain c. Belgique*, n° 57292/16, § 115.

La Cour considère que la reproduction de matériaux tirés de la presse écrite et celle de matériaux tirés de l'Internet peuvent être soumises à des régimes différents. Il en va de même en ce qui concerne les archives papier et les archives numériques. La portée de ces dernières est en effet beaucoup plus importante et les conséquences sur la vie privée des personnes nommées d'autant plus graves, ce qui est encore amplifié par les moteurs de recherche[247].

En ce qui concerne le degré de diffusion de la version archivée de la publication, la Cour tient compte du fait que la consultation d'archives nécessite une démarche active de recherche par l'introduction de mots-clés sur le site des archives du journal[248].

À l'instar de la Cour de justice de l'Union européenne, la Cour admet que des obligations différentes peuvent être appliquées aux moteurs de recherche et aux éditeurs à l'origine de l'information litigieuse. Il est également vrai que c'est avant tout en raison des moteurs de recherche que les informations sur les personnes tenues à disposition par les médias concernés peuvent facilement être repérées par les internautes. Il ne peut toutefois pas être perdu de vue que le fait pour un journal de mettre en ligne un article sur son site web a déjà, en tant que tel, des répercussions sur la visibilité des informations litigieuses[249].

La Cour a précisé qu'elle n'impose pas une obligation pour les médias de vérifier leurs archives de manière systématique et permanente. Sans préjudice de leur devoir de respecter la vie privée lors de la publication initiale d'un article, il s'agit pour eux, en ce qui concerne l'archivage de l'article, de procéder à une vérification et donc à une mise en balance des droits en jeu seulement en cas de demande expresse à cet effet[250].

3. *Injonction de retirer et de ne plus publier sur l'Internet des enregistrements illicites*

La Cour a rappelé les critères à prendre en considération lors de la mise en balance du droit au respect de la vie privée et du droit au respect de la liberté d'expression (et de la liberté de la presse en particulier) :

- 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.

[247] *Ibid.*, § 116.
[248] *Ibid.*, § 117.
[249] *Ibid.*
[250] *Ibid.*, § 134.

Dans le cadre d'une requête introduite sous l'angle de l'article 10, la Cour vérifie en outre le mode d'obtention des informations et leur véracité ainsi que la gravité de la sanction imposée aux journalistes ou aux éditeurs[251].

La Cour rappelle que la protection offerte aux journalistes par l'article 10 est subordonnée à la condition qu'ils agissent de bonne foi de manière à fournir des informations exactes et dignes de crédit dans le respect des principes d'un journalisme responsable[252].

Elle rappelle encore que les journalistes qui exercent leur liberté d'expression assument « des devoirs et des responsabilités ». La Convention ne garantit pas une liberté d'expression sans aucune restriction, même quand il s'agit de rendre compte dans la presse de questions sérieuses d'intérêt général. Ainsi, malgré le rôle essentiel qui revient aux médias dans une société démocratique, les journalistes ne sauraient en principe être déliés de leur devoir de respecter les lois pénales de droit commun au motif que l'article 10 leur offrirait une protection inattaquable. En d'autres termes, un journaliste auteur d'une infraction ne peut pas se prévaloir d'une immunité pénale (et dont ne bénéficient pas les autres personnes qui exercent leur droit à la liberté d'expression) du seul fait que l'infraction en question aurait été commise dans l'exercice de ses fonctions journalistiques[253].

Les atteintes à la vie privée résultant d'une intrusion dans l'intimité des individus commises par des dispositifs techniques d'écoutes, de vidéo ou de photographies clandestines doivent faire l'objet d'une protection particulièrement attentive[254].

Dans certaines circonstances, une personne, même connue du public, peut se prévaloir d'une « espérance légitime » de protection et de respect de sa vie privée. L'appartenance d'un individu à la catégorie des personnalités publiques ne saurait, *a fortiori* lorsqu'elles n'exercent pas de fonctions officielles, autoriser les médias à transgresser les principes déontologiques et éthiques qui devraient s'imposer à eux ni légitimer des intrusions dans la vie privée[255].

La Cour rappelle que les sites Internet sont des outils d'information et de communication qui se distinguent particulièrement de la presse écrite, notamment quant à leur capacité à emmagasiner et à diffuser l'information, et que les communications en ligne et leur contenu risquent bien plus que la presse écrite [classique] de porter atteinte à l'exercice et à la jouissance des droits et libertés fondamentaux, en particulier du droit au respect de la vie privée[256].

---

[251] Cour eur. D.H., arrêt du 14 janvier 2021, *Société éditrice de Mediapart et autres c. France*, n[os] 281/15 et 34445/15, § 76.
[252] *Ibid.*, § 77.
[253] *Ibid.*, §§ 77, 83 et 87.
[254] *Ibid.*, § 84.
[255] *Ibid.*, § 87.
[256] *Ibid.*, § 88.

4. *Blocage de l'accès à des contenus sur l'Internet*

La possibilité pour les individus de s'exprimer sur Internet constitue un outil sans précédent d'exercice de la liberté d'expression. Grâce à leur accessibilité ainsi qu'à leur capacité à conserver et à diffuser de grandes quantités de données, les sites Internet contribuent grandement à améliorer l'accès du public à l'actualité et, de manière générale, à faciliter la communication de l'information. Cependant, les avantages de ce média s'accompagnent d'un certain nombre de risques. Des propos clairement illicites, notamment des propos diffamatoires, haineux ou appelant à la violence, peuvent être diffusés comme jamais auparavant dans le monde entier, en quelques secondes, et parfois demeurer en ligne pendant fort longtemps[257].

Est légitime l'exigence d'un traitement rapide par les autorités internes d'une demande de blocage d'accès à un contenu en ligne pour empêcher au plus vite la diffusion d'informations fausses et diffamatoires et de contenus portant atteinte à la vie privée et qui sont publiés sur les sites internet[258].

Dans des cas ordinaires de diffamation, qui ne relèvent pas d'un discours de haine et de menaces directes à l'intégrité physique d'une personne, un système de retrait sur notification, accompagné de procédures efficaces permettant une réaction rapide, telle qu'une procédure de blocage d'accès, peut constituer un outil approprié de mise en balance des droits et des intérêts de tous les intéressés[259].

La mesure de blocage d'accès à un contenu Internet pour une durée indéterminée risque de constituer une atteinte disproportionnée aux libertés de presse et d'expression dans bien des cas. Cette mesure doit être employée exceptionnellement dans des circonstances bien définies, à savoir lorsque l'atteinte au droit au respect de la vie privée est évidente et constatable de prime abord. Mais au vu des dangers qu'elles posent, de telles restrictions doivent s'inscrire dans un cadre légal particulièrement strict quant à la délimitation de l'interdiction et efficace quant au contrôle juridictionnel contre les abus éventuels[260].

5. *Obligation de divulguer l'identité des personnes ayant posté des commentaires sur un forum d'un site d'informations sur Internet*

La notion de « source » journalistique vise « toute personne qui fournit des informations à un journaliste »[261].

[257] Cour eur. D.H., arrêt du 18 mai 2021, *Savci Cengel c. Turquie*, n° 30697/19, § 35.
[258] *Ibid.*, § 37.
[259] *Ibid.*, § 37.
[260] *Ibid.*, § 41.
[261] Cour eur. D.H., arrêt du 7 décembre 2021, *Standard Verlagsgesellschaft m.b.H. c. Autriche*, n° 39378/15, § 65.

L'expression « informations permettant d'identifier une source » inclut, dans la mesure où elles sont susceptibles de conduire à l'identification d'une source, à la fois « les circonstances factuelles de l'acquisition d'informations auprès d'une source par un journaliste » et « le contenu non publié des informations fournies par une source à un journaliste »[262].

Les commentaires postés sur le forum par les lecteurs d'un portail d'information, tout en constituant des opinions et donc des informations, sont clairement adressés au public et non à un journaliste. En conséquence, les auteurs des commentaires ne peuvent pas être considérés comme une source pour un journaliste. Toutefois, une ingérence dans l'article 10 peut également se produire autrement qu'en ordonnant la divulgation d'une source journalistique[263].

La Cour ne doute pas qu'une obligation de divulguer les données des auteurs de commentaires en ligne pourrait les dissuader de contribuer au débat et, partant, entraîner un effet dissuasif parmi les utilisateurs actifs dans les forums en général. Cela affecte également, indirectement, le droit à la liberté de la presse de la société qui héberge le forum en tant qu'entreprise de médias. Elle note que cette entreprise de médias invite les utilisateurs à commenter ses articles afin de faire avancer la discussion sur son travail journalistique. Pour atteindre cet objectif, elle permet aux auteurs des commentaires d'utiliser des noms d'utilisateur. Lors de leur inscription au forum, les utilisateurs sont informés que leurs données ne seront pas vues publiquement et ne seront divulguées que si la loi l'exige. Le règlement des forums stipule que certains contenus ne seront pas acceptés, que les commentaires seront filtrés par un système de mots-clés, qu'ils pourront être soumis à un examen manuel et qu'ils seront supprimés s'ils ne sont pas conformes au règlement[264].

La Cour ne perd pas de vue la facilité, la portée et la rapidité de la diffusion d'informations sur Internet, ainsi que la persistance de ces informations une fois divulguées, qui peuvent considérablement aggraver les effets d'un discours illicite par rapport aux médias traditionnels. Elle est donc d'accord sur le fait que la Convention ne prévoit pas un droit absolu à l'anonymat sur Internet[265].

En même temps, la Cour est consciente de l'intérêt des utilisateurs d'Internet à ne pas divulguer leur identité. L'anonymat est depuis longtemps un moyen d'éviter des représailles ou une attention non désirée. En tant que tel, il est susceptible de favoriser la libre circulation des opinions, des idées et des informations de manière importante, y compris, notamment, sur Internet. Cela peut donc indirectement servir aussi les intérêts d'une entreprise de médias[266].

262 *Ibid.*
263 *Ibid.*, § 71.
264 *Ibid.*, § 74.
265 *Ibid.*, § 75.
266 *Ibid.*, § 76.

Différents degrés d'anonymat sont possibles sur l'Internet. Un utilisateur d'Internet peut être anonyme pour le grand public tout en étant identifiable par un fournisseur de services par le biais d'un compte ou de données de contact qui peuvent être soit non vérifiées, soit soumises à une certaine forme de vérification. Un fournisseur de services peut également autoriser un degré élevé d'anonymat pour ses utilisateurs, auquel cas ceux-ci ne sont pas tenus de s'identifier du tout et ne peuvent être retrouvés (dans une mesure limitée) qu'à travers les informations conservées par les fournisseurs d'accès à l'Internet. La divulgation de ces informations nécessite généralement une injonction des autorités d'enquête ou judiciaires et est soumise à des conditions restrictives. Elle peut néanmoins être requise dans certains cas afin d'identifier et de poursuivre les auteurs[267].

Dans le cas d'espèce, l'entreprise de médias offrait un certain degré d'anonymat aux utilisateurs du forum et cet anonymat n'aurait pas été effectif si l'entreprise ne pouvait pas le défendre par ses propres moyens[268].

Bien que l'anonymat sur Internet soit une valeur importante, celle-ci doit céder à l'occasion à d'autres impératifs légitimes, tels que la prévention des troubles ou de la criminalité ou la protection des droits et libertés d'autrui[269].

Dans l'affaire qui lui était soumise, la Cour a souligné le fait que les intérêts en jeu ne comprenaient pas seulement le droit des plaignants de protéger leur réputation et le droit de la société requérante à la liberté de la presse, mais aussi le rôle de cette dernière dans la protection des données à caractère personnel des auteurs de commentaires et de leur liberté d'exprimer publiquement leurs opinions[270].

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

A. Primauté du droit de l'Union

La Cour, saisie sur question préjudicielle de la Cour constitutionnelle lettone portait sur la primauté du droit de l'Union sur les législations nationales dans une affaire qui sera plus amplement relatée ci-dessous, rappelle que « l'interprétation que la Cour donne des règles du droit de l'Union, dans l'exercice de la compétence que lui confère l'article 267 TFUE, éclaire et précise la signification et la portée de ces règles, telles qu'elles doivent ou auraient dû être comprises et appliquées depuis le moment de leur entrée en vigueur. Ce n'est qu'à titre exceptionnel que la Cour peut, par application d'un principe général de sécurité juridique inhé-

[267] *Ibid.*, § 77.
[268] *Ibid.*, § 78.
[269] *Ibid.*, § 91.
[270] *Ibid.*, § 92.

rent à l'ordre juridique de l'Union, être amenée à limiter la possibilité pour tout intéressé d'invoquer une disposition qu'elle a interprétée en vue de mettre en cause des relations juridiques établies de bonne foi. Pour qu'une telle limitation puisse être décidée, il est nécessaire que deux critères essentiels soient réunis, à savoir la bonne foi des milieux intéressés et le risque de troubles graves (arrêts du 6 mars 2007, *Meilicke*, C-292/04, EU:C:2007:132, points 34 et 35 ; du 22 janvier 2015, *Balazs*, C-401/13 et C-432/13, EU:C:2015:26, points 49 et 50, ainsi que du 29 septembre 2015, *Gmina Wrocław*, C-276/14, EU:C:2015:635, points 44 et 45) »[271]. Et d'ajouter qu'« une telle limitation ne peut être admise, selon la jurisprudence constante de la Cour, que dans l'arrêt même qui statue sur l'interprétation sollicitée. En effet, il faut nécessairement un moment unique de détermination des effets dans le temps de l'interprétation sollicitée que donne la Cour d'une disposition du droit de l'Union. Le principe qu'une limitation ne peut être admise que dans l'arrêt même qui statue sur l'interprétation sollicitée garantit l'égalité de traitement des États membres et des autres justiciables face à ce droit et remplit par là même les exigences découlant du principe de sécurité juridique (arrêt du 6 mars 2007, *Meilicke*, C-292/04, EU:C:2007:132, points 36 et 37 ; voy., en ce sens, arrêts du 23 octobre 2012, *Nelson e.a.*, C-581/10 et C-629/10, EU:C:2012:657, point 91, ainsi que du 7 novembre 2018, *O'Brien*, C-432/17, EU:C:2018:879, point 34) »[272].

La Cour conclut son raisonnement en précisant que « par conséquent, les effets dans le temps d'une décision rendue par la Cour sur renvoi préjudiciel ne sauraient dépendre de la date de prononcé de l'arrêt par lequel la juridiction de renvoi statue définitivement sur l'affaire au principal, ni même de l'appréciation par celle-ci de la nécessité de préserver les effets juridiques de la réglementation nationale en cause [et qu']en vertu du principe de primauté du droit de l'Union, il ne saurait, en effet, être admis que des règles de droit national, fussent-elles d'ordre constitutionnel, portent atteinte à l'unité et à l'efficacité de ce droit (voy., en ce sens, arrêts du 26 février 2013, *Melloni*, C-399/11, EU:C:2013:107, point 59, ainsi que du 29 juillet 2019, *Pelham e.a.*, C-476/17, EU:C:2019:624, point 78). À supposer même que des considérations impérieuses de sécurité juridique soient de nature à conduire, à titre exceptionnel, à une suspension provisoire de l'effet d'éviction exercé par une règle de droit de l'Union directement applicable à l'égard du droit national contraire à celle-ci, les conditions d'une telle suspension ne peuvent être déterminées que par la Cour (voy., en ce sens, arrêt du 8 septembre 2010, *Winner Wetten*, C-409/06, EU:C:2010:503, points 61 et 67) »[273].

B. Effet immédiat ou direct d'un règlement

Dans cette même affaire, riche en demandes préjudicielles, la Cour a rappelé qu'« en vertu de l'article 288, deuxième alinéa, TFUE, un règlement est obliga-

[271] C.J.U.E., 22 juin 2021, *B. c. Latvijas Republikas Saeima*, C-439/19, point 132.
[272] *Ibid.*, point 133.
[273] *Ibid.*, points 134 et 135.

toire dans tous ses éléments et qu'il est directement applicable dans tout État membre, de telle sorte que ses dispositions ne nécessitent, en principe, aucune mesure d'application des États membres. À cet égard, il convient de rappeler que, selon une jurisprudence bien établie de la Cour, en vertu de l'article 288 TFUE et en raison même de la nature des règlements et de leur fonction dans le système des sources du droit de l'Union, les dispositions des règlements ont, en général, un effet immédiat dans les ordres juridiques nationaux, sans qu'il soit besoin, pour les autorités nationales, de prendre des mesures d'application. Néanmoins, certaines de ces dispositions peuvent nécessiter, pour leur mise en œuvre, l'adoption de mesures d'application par les États membres (arrêt du 15 mars 2017, *Al Chodor*, C-528/15, EU:C:2017:213, point 27 et jurisprudence citée) »[274].

C. Compétence du Tribunal

Par un arrêt du 19 octobre 2021[275], le Tribunal rappelle qu'il est compétent pour connaître des recours introduits « à l'encontre des seuls actes des institutions, des organes ou des organismes de l'Union ». Il s'agissait d'un recours introduit par une dame de nationalité italienne contre un décret-loi italien pris dans le cadre de la lutte contre la Covid-19 et, plus particulièrement, relatif à un cadre pour la délivrance, la vérification et l'acceptation du certificat Covid numérique de l'Union européenne afin de faciliter la libre circulation des ressortissants de l'Union.

C'est évidemment, à bon droit, que le Tribunal se déclare dans cette affaire incompétent pour connaître du recours.

D. Recevabilité devant la C.J.U.E.

Dans une cause opposant Facebook à l'Autorité de protection des données belge qui sera plus amplement reprise ci-dessous, la Cour rappelle une des conditions de recevabilité d'une question préjudicielle. Ainsi, elle déclare irrecevable une des questions préjudicielles au motif que la « question posée n'a aucun rapport avec la réalité ou l'objet du litige au principal et concerne un problème hypothétique. Par conséquent, cette question doit être déclarée irrecevable »[276].

En effet et dès lors que, « selon une jurisprudence constante, les questions portant sur le droit de l'Union bénéficient d'une présomption de pertinence, le refus de la Cour de statuer sur une question préjudicielle posée par une juridiction nationale n'est possible que s'il apparaît de manière manifeste que l'interprétation d'une règle de l'Union sollicitée n'a aucun rapport avec la réalité ou l'objet du litige au principal, lorsque le problème est de nature hypothétique ou encore lorsque la

[274] C.J.U.E., 15 juin 2021, *Facebook Ireland Ltd, Facebook Inc, Facebook Belgium BVBA c. Gegevensbeschermingsautoriteit*, points 109 et 110.
[275] Trib., 19 janvier 2021, *Guglielmina Natale c. Italie*, T-469/21.
[276] C.J.U.E., 15 juin 2021, *Facebook Ireland Ltd, Facebook Inc, Facebook Belgium BVBA c. Gegevensbeschermingsautoriteit*, point 118.

Cour ne dispose pas des éléments de fait et de droit nécessaires pour répondre de façon utile aux questions qui lui sont posées (arrêts du 16 juin 2015, *Gauweiler e.a.*, C-62/14, EU:C:2015:400, point 25, ainsi que du 7 février 2018, *American Express*, C-304/16, EU:C:2018:66, point 32) »[277].

E. Règlement n° 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD)

1. *Champ d'application matériel du RGPD*

Dans un arrêt rendu le 22 juin 2021[278], la Cour se prononce sur une série de questions préjudicielles posées par la Cour constitutionnelle lituanienne. Il s'agissait d'un dossier relatif à un conducteur lituanien qui contestait la légalité d'une législation lettone « prévoyant l'accès du public aux données à caractère personnel relatives aux points de pénalité imposées pour des infractions routières »[279]. Pour être plus précis, la législation lettone prévoit l'imposition de points de pénalité aux conducteurs de véhicules qui ont commis une infraction routière et auxquels une sanction, pécuniaire ou autre, a été infligée. Ces points sont inscrits par un organisme public, la CSDD, au registre national des véhicules et de leurs conducteurs le jour de l'expiration du délai de recours contre la décision infligeant cette sanction. De plus, cette sanction relève du droit administratif visant à sensibiliser les conducteurs concernés, en les incitant à adopter un mode de conduite plus sûr, et non à les sanctionner une seconde fois. Cependant, le conducteur peut se voir interdit de conduite lorsqu'un certain nombre de points de pénalités est atteint[280].

La Cour se pose, dans un premier temps, la question du champ d'application du RGPD afin de déterminer si le traitement dont question y entrait. Elle a l'occasion de rappeler que le RGPD prévoit des exceptions à la définition très large de ce champ d'application ; exceptions qui doivent « recevoir une interprétation stricte (voy., en ce sens, arrêts du 9 juillet 2020, *Land Hessen*, C-272/19, EU:C:2020:535, point 68, ainsi que du 16 juillet 2020, *Facebook Ireland et Schrems*, C-311/18, EU:C:2020:559, point 84) »[281]. Or il ressort de la lecture conjointe de l'article 2, paragraphe 2, sous a), du RGPD et de l'article 2, paragraphe 2, sous b), du RGPD ainsi que du considérant 16, que le RGPD « ne s'applique pas aux traitements de données à caractère personnel dans le contexte des "activités qui ne relèvent pas du champ d'application du droit de l'Union, telles que les activités relatives à la

[277] *Ibid.*, point 115.
[278] C.J.U.E., 22 juin 2021, *B. c. Latvijas Republikas Saeima*, C-439/19, point 2.
[279] *Ibid.*
[280] *Ibid.*, point 58.
[281] *Ibid.*, point 62.

sécurité nationale" ainsi que des "activités ayant trait à la politique étrangère et de sécurité commune de l'Union" »[282]. La Cour en conclut, après avoir effectué un parallèle avec l'article 3 de la directive 95/46 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données abrogée par le RGPD et sa jurisprudence antérieure, que « doit être considéré comme ayant pour seul objet d'exclure du champ d'application dudit règlement les traitements de données à caractère personnel effectués par les autorités étatiques dans le cadre d'une activité qui vise à préserver la sécurité nationale ou d'une activité pouvant être rangée dans la même catégorie, de telle sorte que le seul fait qu'une activité soit propre à l'État ou à une autorité publique ne suffit pas pour que cette exception soit automatiquement applicable à une telle activité (voy., en ce sens, arrêt du 9 juillet 2020, *Land Hessen*, C-272/19, EU:C:2020:535, point 70) »[283]. Il en découle que « les activités qui ont pour but de préserver la sécurité nationale visées à l'article 2, paragraphe 2, sous a), du RGPD couvrent, en particulier, ainsi que l'a également relevé en substance M. l'avocat général aux points 57 et 58 de ses conclusions, celles ayant pour objet de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société »[284]. La Cour conclut de manière logique que « les activités relatives à la sécurité routière ne poursuivent pas un tel objectif et ne sauraient, en conséquence, être rangées dans la catégorie des activités ayant pour but la préservation de la sécurité nationale, visées à l'article 2, paragraphe 2, sous a), du RGPD »[285].

Par ailleurs, la Cour s'interroge sur l'articulation entre le RGPD et la directive 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel 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, et à la libre circulation de ces données. En effet, la cause s'inscrit dans des compétences de police routière et l'article 2, paragraphe 2, sous d), du RGPD prévoit que ce dernier ne s'applique pas au traitement de données à caractère personnel effectué « 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 »[286]. Cette exception est liée au fait que ces finalités font l'objet d'une législation européenne plus spécifique, à savoir la directive 2016/680. Or, il s'avère que la notion d'autorités compétentes « doit être comprise en lien avec la protection des données à caractère personnel dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière, compte tenu des aménagements qui peuvent s'avérer nécessaires, à cet égard, en raison de la nature spécifique de ces domaines. En outre, le considérant 11 de cette directive précise que le RGPD s'applique au traitement de données à caractère personnel qui serait

[282] *Ibid.*, point 63.
[283] *Ibid.*, point 66.
[284] *Ibid.*, point 67.
[285] *Ibid.*, point 68.
[286] Article 2, paragraphe 2, sous d), du RGPD.

effectué par une "autorité compétente", au sens de l'article 3, paragraphe 7, de ladite directive, mais à d'autres fins que celles prévues dans celle-ci »[287]. Or, en l'espèce, et pour ce qui concerne la communication au public des informations relatives aux points de pénalité effectuée par la CSDD, cette dernière ne peut être considérée comme autorité compétence au sens de l'article 3, 7, de la directive 2016/80. En conséquence, le RGPD trouve à s'appliquer dès lors que ce traitement ne peut relever de l'exception visée par l'article 2, 2, sous d), du RGPD.

2. *Notion d'établissement*

Dans une cause opposant Facebook à l'Autorité de protection des données belge qui sera plus amplement reprise ci-dessous, la Cour analyse la notion d'établissement visé à l'article 3, 1, du RGPD et dont l'applicabilité territoriale du règlement dépend. En effet, cet article prévoit que le RGPD « s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union »[288]. Et le considérant 22 du règlement de préciser que « l'établissement suppose l'exercice effectif et réel d'une activité au moyen d'un dispositif stable. La forme juridique retenue pour un tel dispositif, qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard ».

Sur la base de ces deux éléments, la Cour confirme que « conformément à l'article 3, paragraphe 1, du règlement nº 2016/679, le champ d'application territoriale de ce règlement est déterminé, sous réserve des hypothèses visées aux paragraphes 2[289] et 3[290] de cet article, par la condition que le responsable du traitement ou le sous-traitant pour le traitement transfrontalier dispose d'un établissement sur le territoire de l'Union »[291].

3. *Notion de donnée à caractère personnel*

Dans l'affaire concernant la communication d'informations relatives aux points de pénalité prévue par la législation lituanienne vue ci-dessus, la Cour s'interroge également sur la notion de donnée à caractère personnel et, plus particulièrement,

---

287 C.J.U.E., 22 juin 2021, *B. c. Latvijas Republikas Saeima*, C-439/19, point 70.

288 C.J.U.E., 15 juin 2021, *Facebook Ireland Ltd, Facebook Inc, Facebook Belgium BVBA c. Gegevensbeschermingsautoriteit*, point 81.

289 Ndr. : « 2. Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées :
a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; ou
b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union ».

290 Ndr. : « 3. Le présent règlement s'applique au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'Union mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public ».

291 C.J.U.E., 15 juin 2021, *Facebook Ireland Ltd, Facebook Inc, Facebook Belgium BVBA c. Gegevensbeschermingsautoriteit*, point 83.

si une telle qualification pouvait être donnée aux points de pénalité en cas d'infraction routière. Force est de constater, dans le chef de la Cour, que les « informations relatives aux points de pénalité, qui se rapportent à une personne physique identifiée, sont des "données à caractère personnel", au sens de l'article 4, point 1, du RGPD, et que leur communication par la CSDD à des tiers constitue un "traitement", au sens de l'article 4, point 2, du RGPD »[292].

Dans une cause concernant l'enregistrement d'adresse IP par un fournisseur de services de médias en ligne, la Cour a rappelé qu'une telle information doit être considérée comme « une donnée à caractère personnel, au sens de l'article 4, point 1, du règlement n° 2016/679, lorsqu'il dispose de moyens légaux lui permettant de faire identifier la personne concernée grâce aux informations supplémentaires dont dispose le fournisseur d'accès à Internet de cette personne (arrêt du 19 octobre 2016, *Breyer*, C-582/14, EU:C:2016:779, point 49) »[293].

4. *Applicabilité de l'article 10 du RGPD*

Toujours dans la cause concernant la communication d'informations relatives aux points de pénalité, la question de l'applicabilité de l'article 10 du RGPD s'est posée. En effet, les informations relatives aux points de pénalité dont la communication est effectuée par la CSDD constituent-elles des données à caractère personnel « relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes ». Dans l'affirmative, leur traitement ne pourrait s'effectuer que sous le contrôle de l'autorité publique sauf « si le traitement est autorisé par le droit de l'Union ou par le droit d'un État membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées »[294].

Dans son analyse, la Cour rappelle que « ledit article 10 vise à assurer une protection accrue à l'encontre de traitements qui, en raison de la sensibilité particulière des données en cause, sont susceptibles de constituer 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 (voy., en ce sens, arrêt du 24 septembre 2019, *GC e.a. (Déréférencement de données sensibles)*, C-136/17, EU:C:2019:773, point 44) »[295]. Elle précise en outre que « dès lors que les données auxquelles se réfère l'article 10 du RGPD portent sur des comportements qui entraînent la désapprobation de la société, l'octroi d'un accès à de telles données est susceptible de stigmatiser la personne concernée et de constituer ainsi une ingérence grave dans sa vie privée ou professionnelle »[296]. En l'espèce, la Cour relève que l'accès à l'information relative aux points de pénalité « permet au public de savoir si une personne déterminée a commis des infrac-

[292] C.J.U.E., 22 juin 2021, *B. c. Latvijas Republikas Saeima*, C-439/19, point 60.
[293] C.J.U.E., *Mircom International Content Management & Consulting (M.I.C.M.) Limited c. Telenet BVBA*, C-597/19, point 102.
[294] C.J.U.E., 22 juin 2021, *B. c. Latvijas Republikas Saeima*, C-439/19, point 73.
[295] *Ibid.*, point 74.
[296] *Ibid.*, point 75.

tions routières et, dans l'affirmative, d'en déduire la gravité et la fréquence de ces infractions. Un tel régime de communication de points de pénalité revient, dès lors, à donner accès à des données à caractère personnel relatives aux infractions routières »[297].

Il convient cependant de s'interroger sur la question de déterminer si cet accès constitue un traitement de données à caractère personnel relatives à des infractions au sens de l'article 10 du RGPD ; en effet, cette « notion renvoie exclusivement aux infractions pénales, ainsi qu'il résulte notamment de la genèse du RGPD »[298]. En effet, il ressort des « travaux préparatoires » du RGPD[299] que « si le Parlement européen avait proposé d'inclure dans cet article les termes de sanctions administratives (*J.O.*, 2017, C 378, p. 430), cette proposition n'a pas été retenue ». En conséquence, « il doit être considéré que le législateur de l'Union, en omettant délibérément d'inclure l'adjectif "administratif" à l'article 10 du RGPD, a entendu réserver la protection accrue prévue par cette disposition au seul domaine pénal »[300].

La Cour ajoute cependant que la qualification de certaines sanctions de « sanctions administratives » ne les fait pas sortir automatiquement du champ d'application de l'article 10 et ce afin de garantir une protection équivalente et homogène dans tous les États membres[301]. Cela est d'autant plus vrai pour la Cour qui reprend les conclusions de l'avocat général[302] que « le considérant 13 de la directive 2016/680 indique que la notion d'infraction pénale au sens de [cette] directive devrait être une notion autonome du droit de l'Union conforme à l'interprétation de la Cour de justice de l'Union européenne »[303]. Il en découle donc que « la notion d'"infraction pénale", décisive pour déterminer l'applicabilité de l'article 10 du RGPD à des données à caractère personnel relatives aux infractions routières, telles que celles en cause au principal, requiert, dans toute l'Union, une interprétation autonome et uniforme, qui doit être recherchée en tenant compte de l'objectif poursuivi par cette disposition et du contexte dans lequel celle-ci s'insère, sans que soit déterminante à cet égard la qualification donnée par l'État membre concerné à ces infractions, cette qualification pouvant être différente d'un pays à l'autre (voy., en ce sens, arrêt du 14 novembre 2013, *Baláž*, C-60/12, EU:C:2013:733, points 26 et 35) »[304].

La Cour rappelle ensuite sa jurisprudence selon laquelle :

> « 87 [...] trois critères sont pertinents pour apprécier le caractère pénal d'une infraction. Le premier est la qualification juridique de l'infraction en droit

[297] *Ibid.*, point 76.
[298] *Ibid.*, point 77.
[299] *Ibid.*
[300] *Ibid.*, point 78.
[301] *Ibid.*, point 83.
[302] *Ibid.*, conclusions de l'avocat général, point 84.
[303] *Ibid.*, point 84.
[304] *Ibid.*, point 85.

> interne, le deuxième, la nature même de l'infraction et, le troisième, le degré de sévérité de la sanction que risque de subir l'intéressé (voy., en ce sens, arrêts du 5 juin 2012, *Bonda*, C-489/10, EU:C:2012:319, point 37 ; du 20 mars 2018, *Garlsson Real Estate e.a.*, C-537/16, EU:C:2018:193, point 28, ainsi que du 2 février 2021, *Consob*, C-481/19, EU:C:2021:84, point 42).
>
> 88. Même pour des infractions qui ne sont pas qualifiées de "pénales" par le droit national, un tel caractère peut néanmoins découler de la nature même de l'infraction en question et du degré de sévérité des sanctions que celle-ci est susceptible d'entraîner (voy., en ce sens, arrêt du 20 mars 2018, *Garlsson Real Estate e.a.*, C-537/16, EU:C:2018:193, points 28 et 32).
>
> 89. S'agissant du critère relatif à la nature même de l'infraction, il implique de vérifier si la sanction en cause poursuit, notamment, une finalité répressive, sans que la seule circonstance qu'elle poursuit également une finalité préventive soit de nature à lui ôter sa qualification de sanction pénale. En effet, il est dans la nature même des sanctions pénales qu'elles tendent tant à la répression qu'à la prévention de comportements illicites. En revanche, une mesure qui se limite à réparer le préjudice causé par l'infraction concernée ne présente pas une nature pénale (voy., en ce sens, arrêts du 5 juin 2012, *Bonda*, C-489/10, EU:C:2012:319, point 39, ainsi que du 20 mars 2018, *Garlsson Real Estate e.a.*, C-537/16, EU:C:2018:193, point 33). Or, il est constant que l'attribution des points de pénalité pour des infractions routières, tout comme les amendes ou autres sanctions que la commission de ces infractions peut entraîner, n'ont pas seulement pour objet de réparer des préjudices éventuellement causés par lesdites infractions mais poursuivent également une finalité répressive.
>
> 90. En ce qui concerne le critère relatif au degré de sévérité des sanctions que la commission de ces mêmes infractions peut entraîner, il importe de relever, tout d'abord, que seules des infractions routières d'une certaine gravité comportent l'attribution de points de pénalité et que, partant, de telles infractions sont susceptibles d'entraîner des sanctions d'une certaine sévérité. Ensuite, l'imposition de points de pénalité se rajoute généralement à la sanction infligée en cas de commission d'une telle infraction, ce qui est d'ailleurs le cas, ainsi qu'il a été relevé au point 58 du présent arrêt, de la législation en cause au principal. Enfin, la cumulation desdits points entraîne, en elle-même, des conséquences juridiques, telles que l'obligation de passer un examen, voire une interdiction de conduire »[305]. ■

Elle précise également que cette jurisprudence « est corroborée par la jurisprudence de la Cour européenne des droits de l'homme selon laquelle, nonobstant la tendance à la "décriminalisation" des infractions routières dans certains États, ces infractions doivent généralement, eu égard à la finalité à la fois préventive et répressive des sanctions infligées et du degré de sévérité que celles-ci peuvent atteindre, être considérées comme étant de nature pénale (voy., en ce sens, Cour eur. D.H., 21 février 1984, *Öztürk c. Allemagne*, CE:ECHR:1984:0221JUD

[305] *Ibid.*, points 87-90.

000854479, §§ 49 à 53 ; 29 juin 2007, *O'Halloran et Francis c. Royaume-Uni*, CE:ECHR:2007:0629JUD 001580902, §§ 33 à 36, ainsi que 4 octobre 2016, *Rivard c. Suisse*, CE:ECHR:2016:1004JUD 002156312, §§ 23 et 24) »[306].

Il en découle donc, dans la cause des points de pénalité, que l'attribution de points de pénalité liée à des infractions routières entre dans la notion d'infractions visée à l'article 10 du RGPD et donc que ces données requièrent la protection accrue prévue à cet article 10.

5. *Base de licéité*

a. Articulation entre les articles 6 et 10 ainsi que 6 et 9 du RGPD

L'articulation entre les articles 6, 9 et 10 du RGPD a soulevé des questions quant à savoir si les articles 6 et 9 ainsi que 6 et 10 devaient s'appliquer de manière cumulative ou, au contraire, de manière autonome.

Toujours dans cet arrêt relatif aux points de pénalité liée à des infractions routières, la Cour va dans le sens d'une application cumulative. Cela ressort du point 99 de l'arrêt[307] dans lequel la Cour fait choix d'une base de licéité dans l'article 6, à savoir le caractère nécessaire « à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement »[308] pour ce qui concerne la communication à des tiers d'informations relatives aux points de pénalité par la CSDD, puis précise que, dès lors que « les données à caractère personnel relatives aux points de pénalité imposés aux conducteurs de véhicules pour des infractions routières relèvent de l'article 10 du RGPD, leur traitement est soumis aux restrictions additionnelles prévues à cette disposition »[309].

La Cour ajoute, par ailleurs, que l'on doit également tenir compte, outre les bases de licéité, des conditions posées par l'article 5, 1, sous c), du RGPD, à savoir que les « données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) », pour examiner la conformité d'une législation nationale au RGPD.

b. Article 6, 1, f), du RGPD (intérêt légitime)

Dans l'arrêt concernant le traitement d'adresse IP vu ci-dessus, la Cour rappelle que l'article 6, 1, f, du RGPD (intérêt légitime), « prévoit trois conditions cumulatives pour qu'un traitement de données à caractère personnel soit licite, à savoir,

306 *Ibid.*, point 91.
307 *Ibid.*, point 99.
308 *Ibid.*
309 *Ibid.*, point 100.

premièrement, la poursuite d'un intérêt légitime par le responsable du traitement ou par un tiers, deuxièmement, la nécessité du traitement des données à caractère personnel pour la réalisation de l'intérêt légitime poursuivi et, troisièmement, la condition que les intérêts ou les libertés et les droits fondamentaux de la personne concernée par la protection des données ne prévalent pas (voy., en ce sens, en ce qui concerne l'article 7, sous f), de la directive 95/46, arrêt du 4 mai 2017, *Rīgas satiksme*, C-13/16, EU:C:2017:336, point 28) »[310].

En termes d'« intérêt légitime », la Cour considère que « l'intérêt du responsable du traitement ou d'un tiers à obtenir une donnée à caractère personnel concernant une personne qui a prétendument porté atteinte à sa propriété afin de l'assigner en justice pour obtenir réparation constitue un intérêt légitime. Cette analyse est confortée par l'article 9, paragraphe 2, sous e) et f), du règlement n° 2016/679 qui prévoit que l'interdiction du traitement de certains types de données à caractère personnel qui révèle notamment des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ne s'applique pas lorsque le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée ou est nécessaire notamment à la constatation, à l'exercice ou à la défense d'un droit en justice [voy. en ce sens, en ce qui concerne l'article 8, paragraphe 2, sous e), de la directive 95/46, arrêt du 4 mai 2017, *Rīgas satiksme*, C-13/16, EU:C:2017:336, point 29] »[311]. Pour illustrer cela, elle reprend l'exemple du recouvrement de créance énoncé par l'avocat général.

> « S'agissant de la condition relative à la nécessité du traitement des données à caractère personnel pour la réalisation de l'intérêt légitime poursuivi, il y a lieu de rappeler que les dérogations et les restrictions au principe de la 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). Cette condition pourrait, en l'occurrence, être remplie dès lors que, ainsi que M. l'avocat général l'a relevé au point 97 de ses conclusions, l'identification du détenteur de la connexion n'est souvent possible que sur la base de l'adresse IP et des informations fournies par le fournisseur d'accès à Internet »[312].

> « Enfin, concernant la condition relative à la pondération des droits et des intérêts opposés en cause, elle dépend, en principe, des circonstances concrètes du cas particulier (arrêt du 4 mai 2017, *Rīgas satiksme*, C-13/16, EU:C:2017:336, point 31 et jurisprudence citée). Il revient à la juridiction de renvoi d'apprécier ces circonstances particulières. À cet égard, les mécanismes permettant de trouver un juste équilibre entre les différents droits et intérêts en présence sont inscrits dans le règlement 2016/679 lui-même (voy., par analogie, arrêt

[310] C.J.U.E., *Mircom International Content Management & Consulting (M.I.C.M.) Limited c. Telenet BVBA*, C-597/19, point 106.
[311] *Ibid.*, point 108.
[312] *Ibid.*, point 110.

> du 29 janvier 2008, *Promusicae*, C-275/06, EU:C:2008:54, point 66 et jurisprudence citée) »[313].

S'agissant de données IP qui semblent également entrer dans le champ d'application de la directive 2002/58/CE du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive e-privacy), « pour qu'un traitement, tel que l'enregistrement des adresses IP des personnes dont les connexions Internet ont été utilisées pour le téléversement de segments de fichiers contenant des œuvres protégées sur des réseaux de pair à pair (*peer-to-peer*), aux fins de déposer une demande de divulgation des noms et des adresses postales des détenteurs de ces adresses IP, puisse être considéré comme licite en satisfaisant aux conditions prévues par le [RGPD], il faut qu'il soit, en particulier, vérifié si ce traitement satisfait aux dispositions susvisées de la directive 2002/58, cette dernière concrétisant, pour les utilisateurs des moyens de communication électroniques, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel (voy., en ce sens, arrêt du 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 109) »[314].

6. *Principe de minimisation*

À nouveau et dans le prolongement de l'analyse des articles 6 et 10 du RGPD dans l'affaire des points de pénalité en Lettonie, la Cour rappelle que la législation nationale doit également être analysée au regard du principe de proportionnalité et que l'on doit « vérifier en particulier si, eu égard à la gravité de l'ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel causée par ladite communication [accès du public au registre reprenant les points de pénalité], celle-ci apparaît justifiée, et notamment proportionnée, aux fins de la réalisation des objectifs poursuivis »[315]. En l'espèce, la Cour a considéré que « compte tenu, d'une part, de la sensibilité des données en question et de la gravité de ladite ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel des personnes concernées ainsi que, d'autre part, du fait que, eu égard aux constatations effectuées [...], il n'apparaît pas que l'objectif de l'amélioration de la sécurité routière ne puisse pas raisonnablement être atteint de manière aussi efficace par d'autres moyens moins attentatoires, la nécessité, pour assurer cet objectif, d'un tel régime de communication de données à caractère personnel relatives aux points de pénalité imposés pour des infractions routières ne saurait être considérée comme étant établie (voy., par analogie, arrêt du 9 novembre 2010, *Volker und Markus Schecke et Eifert*, C-92/09 et C-93/09, EU:C:2010:662, point 86) »[316].

[313] *Ibid.*, points 111 et 112.
[314] *Ibid.*, point 118.
[315] C.J.U.E., 22 juin 2021, *B. c. Latvijas Republikas Saeima*, C-439/19, point 106.
[316] *Ibid.*, point 113.

7. *Compétence des autorités de protection des données nationales*

a. Mécanismes de contrôle de cohérence.

Dans une affaire opposant Facebook à l'Autorité de protection des données belge, la Cour est amenée à analyser les compétences des autorités de contrôle des données nationales mais également la notion d'« autorité de contrôle chef de file » visée à l'article 58 du RGPD.

Le Président de la Commission pour la protection de la vie privée[317], devenue depuis lors l'Autorité de protection des données (APD), avait attrait Facebook en cessation devant le tribunal de première instance néerlandophone de Bruxelles. Il était reproché à cette dernière « une "violation grave et à grande échelle, par Facebook, de la législation en matière de protection de la vie privée" consistant en la collecte par ce réseau social en ligne d'informations sur le comportement de navigation tant des détenteurs d'un compte Facebook que des non-utilisateurs des services Facebook au moyen de différentes technologies, telles que les cookies, les modules sociaux (par exemple, les boutons "J'aime" ou "Partager") ou encore les pixels. Ces éléments permettaient au réseau social concerné d'obtenir certaines données d'un internaute consultant une page d'un site Internet les contenant, telles que l'adresse de cette page, l'"adresse IP" du visiteur de ladite page ainsi que la date et l'heure de la consultation concernée »[318]. Le tribunal a donné raison à l'APD ; décision contre laquelle Facebook a interjeté appel devant la cour d'appel e Bruxelles. Elle y soutenait les thèses selon lesquelles l'action de l'APD serait irrecevable pour les faits antérieurs au 25 mai 2018 et que « l'APD n'aurait pas de compétence et ne disposerait pas d'un droit d'intenter cette action compte tenu du mécanisme de "guichet unique" désormais prévu en application des dispositions du règlement nº 2016/679. En effet, sur la base de ces dispositions, seul le Data Protection Commissioner (Commissaire à la protection des données, Irlande) serait compétent pour intenter une action en cessation à l'encontre de Facebook Ireland, cette dernière étant la seule responsable du traitement des données à caractère personnel des utilisateurs du réseau social concerné dans l'Union »[319]. Si la Cour a fait droit à l'irrecevabilité de l'action pour les faits antérieurs au 25 mai 2018, elle a cependant posé des questions préjudicielles à la C.J.U.E. concernant le principe de « guichet unique ».

À la question de savoir si une autorité de protection de données n'étant pas chef de file au sens de l'article 56, 1, du RGPD pouvait intenter une action devant une

[317] Pour rappel, la Commission n'avait pas de personnalité juridique de sorte qu'elle ne pouvait agir en justice que par le biais de son président dans les limites prévues par la loi.
[318] C.J.U.E., 15 juin 2021, *Facebook Ireland Ltd, Facebook Inc, Facebook Belgium BVBA c. Gegevensbeschermingsautoriteit*, point 30.
[319] *Ibid.*, point 35.

juridiction nationale, la Cour a rappelé que « d'une part, à la différence de la directive 95/46, qui avait été adoptée sur le fondement de l'article 100 A du traité CE, concernant l'harmonisation du marché commun, la base juridique du [RGPD] est l'article 16 TFUE, lequel consacre le droit de toute personne à la protection des données à caractère personnel et autorise le Parlement européen et le Conseil de l'Union européenne à fixer des règles relatives à la protection des personnes physiques à l'égard du traitement de ces données par les institutions, organes et organismes de l'Union, ainsi que par les États membres, dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation desdites données. D'autre part, le considérant 1 de ce règlement affirme que "[l]a protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental" et rappelle que l'article 8, paragraphe 1, de la Charte ainsi que l'article 16, paragraphe 1, TFUE prévoient le droit de toute personne à la protection des données à caractère personnel la concernant »[320]. Cela impose donc que les autorités compétentes des États membres doivent « assurer un niveau élevé de protection des droits garantis à l'article 16 TFUE et à l'article 8 de la Charte »[321]. De plus, rappelle la Cour, « ainsi que l'énonce le considérant 4 de ce règlement, celui-ci respecte tous les droits fondamentaux et observe les libertés et les principes reconnus dans la Charte »[322].

Sur la base de ces rappels, elle précise que les autorités de protection des données nationales sont investies de missions dont celle de contrôler l'application du RGPD mais également de coopérer « avec d'autres autorités de contrôle, y compris en partageant des informations, et de fournir une assistance mutuelle dans ce cadre en vue d'assurer une application cohérente [RGPD] et des mesures prises pour en assurer le respect, prévue à l'article 57, paragraphe 1, sous g), du [RGPD]. Parmi les pouvoirs conférés auxdites autorités de contrôle en vue de poursuivre ces missions, figurent divers pouvoirs d'enquête, prévus à l'article 58, paragraphe 1, du [RGPD], ainsi que le pouvoir de porter toute violation du RGPD] à l'attention des autorités judiciaires et, le cas échéant, d'ester en justice en vue de faire appliquer les dispositions [du RGPD], prévu à l'article 58, paragraphe 5, de ce dernier »[323].

Intervient alors le principe de « guichet unique » qui exige « une coopération loyale et efficace entre l'autorité de contrôle chef de file et les autres autorités de contrôle concernées »[324] et « l'autorité de contrôle chef de file ne peut ignorer les points de vue des autres autorités de contrôle concernées et toute objection pertinente et motivée formulée par l'une de ces dernières autorités a pour effet de

320 *Ibid.*, point 44.
321 *Ibid.*, point 45.
322 *Ibid.*, point 46.
323 *Ibid.*, point 48.
324 *Ibid.*, point 53.

bloquer, à tout le moins temporairement, l'adoption du projet de décision de l'autorité de contrôle chef de file »[325]. Ces principes de « guichet unique » et de « chef de file » n'empêchent cependant pas de connaître « une réclamation introduite auprès d'elle et qui concerne un traitement transfrontalier de données à caractère personnel ou une infraction éventuelle à ce règlement, si son objet concerne uniquement un établissement dans l'État membre dont elle relève ou affecte sensiblement des personnes concernées dans cet État membre uniquement »[326]. La Cour relève également une deuxième dérogation aux mécanismes de contrôle de la cohérence prévus par le RGPD ; dérogation qui consiste en une procédure d'urgence. « Cette procédure d'urgence permet, dans des circonstances exceptionnelles, lorsque l'autorité de contrôle concernée considère qu'il est urgent d'intervenir pour protéger les droits et les libertés des personnes concernées, d'adopter immédiatement des mesures provisoires visant à produire des effets juridiques sur son propre territoire et ayant une durée de validité déterminée qui n'excède pas trois mois, l'article 66, paragraphe 2, du règlement nº 2016/679 prévoyant de surcroît que, lorsqu'une autorité de contrôle a pris une mesure en vertu du paragraphe 1 et estime que des mesures définitives doivent être adoptées d'urgence, elle peut demander un avis d'urgence ou une décision contraignante d'urgence au Comité européen de la protection des données, en motivant sa demande d'avis ou de décision »[327]. Cette autorité de contrôle se prévalant de l'urgence doit cependant en informer le chef de file qui pourra décider si elle traitera ou non le cas. Il y a donc un système de priorité du chef de file sur les autres autorités de protection nationales impliquées dans le traitement transfrontalier de données à caractère personnel.

Cependant, « le mécanisme de "guichet unique" ne saurait en aucun cas aboutir à ce qu'une autorité de contrôle nationale, en particulier l'autorité de contrôle chef de file, n'assume pas la responsabilité qui lui incombe en vertu du règlement nº 2016/679 de contribuer à une protection efficace des personnes physiques contre des atteintes à leurs droits fondamentaux rappelés au point précédent du présent arrêt, sous peine d'encourager la pratique d'un forum shopping, notamment de la part des responsables de traitement, visant à contourner ces droits fondamentaux et l'application effective des dispositions de ce règlement les mettant en œuvre »[328].

La Cour termine son analyse en précisant que « l'exercice du pouvoir d'une autorité de contrôle d'un État membre de s'adresser aux juridictions de son État ne saurait être exclu lorsque, après avoir requis l'assistance mutuelle de l'autorité de contrôle chef de file, en vertu de l'article 61 du [RGPD], cette dernière ne lui fournit pas les informations demandées »[329]. La juridiction saisie devra donc « déterminer si les

[325] *Ibid.*
[326] *Ibid.*, point 58.
[327] *Ibid.*, point 59.
[328] *Ibid.*, point 68.
[329] *Ibid.*, point 71.

règles de répartition des compétences ainsi que les procédures et les mécanismes pertinents prévus par le [RGPD] ont été correctement appliqués »[330]. En conclusion, la Cour estime qu'« une autorité de contrôle d'un État membre qui, en vertu de la législation nationale adoptée en exécution de l'article 58, paragraphe 5 [du RGPD], a le pouvoir de porter toute prétendue violation dudit règlement à l'attention d'une juridiction de cet État membre et, le cas échéant, d'ester en justice peut exercer ce pouvoir en ce qui concerne un traitement de données transfrontalier, alors qu'elle n'est pas l'"autorité de contrôle chef de file", au sens de l'article 56, paragraphe 1, du même règlement, s'agissant de ce traitement de données, pour autant que ce soit dans l'une des situations où le [RGPD] confère à cette autorité de contrôle une compétence pour adopter une décision constatant que ledit traitement méconnaît les règles qu'il contient ainsi que dans le respect des procédures de coopération et de contrôle de la cohérence prévues par ce règlement »[331].

En complément à cette conclusion, la Cour précise également qu'« en cas de traitement de données transfrontalier, l'exercice du pouvoir d'une autorité de contrôle d'un État membre, autre que l'autorité de contrôle chef de file, d'intenter une action en justice, au sens de cette disposition, ne requiert pas que le responsable du traitement ou le sous-traitant pour le traitement transfrontalier de données à caractère personnel contre qui cette action est intentée dispose d'un établissement principal ou d'un autre établissement sur le territoire de cet État membre »[332]. En effet, « conformément à l'article 3, paragraphe 1, du [RGPD], le champ d'application territoriale de ce règlement est déterminé, sous réserve des hypothèses visées aux paragraphes 2 et 3 de cet article, par la condition que le responsable du traitement ou le sous-traitant pour le traitement transfrontalier dispose d'un établissement sur le territoire de l'Union »[333].

b. Transfert de données vers des pays tiers

Dans cette même affaire *Facebook contre Autorité de protection des données belge*, la Cour a analysé la question des pouvoirs d'une autorité de contrôle dans le cadre de transfert de données vers un pays tiers, c'est-à-dire un pays hors de l'Espace économique européen. La Cour précise que « cette question est soulevée dans le cadre d'un débat entre les parties portant sur le point de savoir si la juridiction de renvoi est compétente pour examiner l'action en cessation en tant qu'elle est intentée à l'encontre de Facebook Belgium, compte tenu du fait que, d'une part, au sein de l'Union, le siège social du groupe Facebook est situé en Irlande et que Facebook Ireland est le responsable exclusif de la collecte et du traitement

330 *Ibid.*, point 73.
331 *Ibid.*, point 75.
332 *Ibid.*, point 84.
333 *Ibid.*, point 83. La notion d'établissement a été analysée par ailleurs dans la contribution.

des données à caractère personnel pour l'ensemble du territoire de l'Union et, d'autre part, en vertu d'une répartition interne à ce groupe, l'établissement situé en Belgique aurait été créé, à titre principal, pour permettre audit groupe d'entretenir des relations avec les institutions de l'Union et, à titre accessoire, pour promouvoir les activités publicitaires et de marketing du même groupe destinées aux personnes résidant en Belgique »[334].

La Cour rappelle que « l'article 55, paragraphe 1, du [RGPD] établit la compétence de principe de chaque autorité de contrôle pour exercer les missions et les pouvoirs dont elle est investie, conformément à ce règlement, sur le territoire de l'État membre dont elle relève »[335] et que « s'agissant du pouvoir d'une autorité de contrôle d'un État membre d'intenter une action en justice, au sens de l'article 58, paragraphe 5, du [RGPD], il importe de rappeler, ainsi que M. l'avocat général l'a relevé au point 150 de ses conclusions, que cette disposition est formulée en des termes généraux et qu'elle ne précise pas les entités à l'encontre desquelles les autorités de contrôle devraient ou pourraient diriger une action en justice concernant toute violation de ce règlement »[336]. Elle conclut en considérant que « lorsque l'autorité de contrôle d'un État membre dispose de la compétence nécessaire à cet effet, en application des articles 55 et 56 du règlement nº 2016/679, elle peut exercer les pouvoirs qui lui sont conférés par ce règlement sur son territoire national, quel que soit l'État membre dans lequel le responsable du traitement ou son sous-traitant est établi »[337]. Cependant, ajoute-elle, l'on doit vérifier si le traitement de données à caractère personnel est effectué « dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union »[338]. Cette vérification doit tenir compte de l'objectif du RGPD qui est d'« assurer une protection efficace des libertés et des droits fondamentaux des personnes physiques, notamment leur droit à la protection de la vie privée et à la protection des données à caractère personnel, la condition selon laquelle le traitement de données à caractère personnel doit être effectué "dans le cadre des activités" de l'établissement concerné, ne saurait recevoir une interprétation restrictive (voy., par analogie, arrêt du 5 juin 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388, point 56 et jurisprudence citée) »[339].

Dans l'affaire *Facebook contre l'Autorité de protection des données*, la Cour considère que « les activités de l'établissement du groupe Facebook[340] situé en Belgique

[334] *Ibid.*, point 86.
[335] *Ibid.*, point 87.
[336] *Ibid.*, point 88.
[337] *Ibid.*, point 89.
[338] Article 3, 1, du RGPD.
[339] C.J.U.E., 15 juin 2021, *Facebook Ireland Ltd, Facebook Inc, Facebook Belgium BVBA c. Gegevensbeschermingsautoriteit*, point 91.
[340] Ndr. : « La Cour a relevé [...] que d'une part, un réseau social tel que Facebook génère une partie substantielle de ses revenus grâce, notamment, à la publicité qui y est diffusée et que l'activité exercée par l'établissement situé en Belgique est destinée à assurer, dans cet État membre, même si ce n'est que de manière accessoire, la promotion et la vente d'espaces publicitaires qui servent à rentabiliser les services Facebook. D'autre part, l'activité exercée à titre principal par Facebook Belgium, consistant à entretenir des relations avec les institutions de l'Union et à constituer

doivent être considérées comme étant indissociablement liées au traitement des données à caractère personnel en cause au principal, dont Facebook Ireland est le responsable s'agissant du territoire de l'Union. Partant, un tel traitement doit être regardé comme étant effectué "dans le cadre des activités d'un établissement du responsable du traitement", au sens de l'article 3, paragraphe 1, du règlement nº 2016/679 »[341]. La conséquence en est que « le pouvoir d'une autorité de contrôle d'un État membre, autre que l'autorité de contrôle chef de file, de porter toute prétendue violation de ce règlement à l'attention d'une juridiction de cet État et, le cas échéant, d'ester en justice, au sens de cette disposition, peut être exercé tant à l'égard de l'établissement principal du responsable du traitement qui se trouve dans l'État membre dont relève cette autorité qu'à l'égard d'un autre établissement de ce responsable, pour autant que l'action en justice vise un traitement de données effectué dans le cadre des activités de cet établissement et que ladite autorité soit compétente pour exercer ce pouvoir »[342].

F. La directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive e-privacy)

La Cour est saisie de questions préjudicielles dans le cadre d'une condamnation de privation de liberté prononcée par un tribunal de première instance estonien en 2017 sur la base de procès-verbaux établis à partir de données relatives à des communications électroniques. Ces données avaient été recueillies auprès de fournisseurs de services de télécommunications sur la base de la législation estonienne. Ce jugement a été confirmé en appel par un arrêt contre lequel le condamné a interjeté un recours en cassation. Cette dernière se pose la question « [...] de savoir si les procès-verbaux établis à partir des données visées à l'article 111[1], paragraphe 2, de la loi relative aux communications électroniques peuvent être considérés comme constituant des éléments de preuve recevables »[343].

Les deux premières questions préjudicielles portent sur l'étendue de l'article 15 de la directive e-privacy et, plus particulièrement, sur le fait de savoir si « l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale permettant l'accès d'autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation

un point de contact avec ces dernières, vise notamment à établir la politique de traitement des données à caractère personnel par Facebook Ireland » (*Ibid.*, point 94).

341 C.J.U.E., 15 juin 2021, *Facebook Ireland Ltd, Facebook Inc, Facebook Belgium BVBA c. Gegevensbeschermingsautoriteit*, point 95.

342 *Ibid.*, point 96.

343 C.J.U.E., 2 mars 2021, *H. K. c. Prokuratuur*, C-746/18, point 20.

des équipements terminaux qu'il utilise et de permettre de tirer des conclusions précises sur sa vie privée, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, sans que cet accès soit circonscrit à des procédures visant à la lutte contre la criminalité grave, ce indépendamment de la durée de la période pour laquelle l'accès auxdites données est sollicité, de la quantité ainsi que de la nature des données disponibles pour une telle période »[344].

La Cour rappelle que l'« article 15, paragraphe 1, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, s'oppose à des mesures législatives prévoyant, à de telles fins, à titre préventif, la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation (voy., en ce sens, arrêt du 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 168) »[345] mais également que l'accès aux données relatives au trafic et aux données de localisation conservées par les fournisseurs de services de communications électroniques « ne peut être octroyé que pour autant que ces données aient été conservées par ces fournisseurs d'une manière conforme audit article 15, paragraphe 1 (voy., en ce sens, arrêt du 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 167) »[346]. De plus, l'objectif d'un tel accès des autorités publiques « ne peut être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée à ces fournisseurs de services (voy., en ce sens, arrêt du 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 166) »[347]. De plus, le législateur national doit procéder à une analyse de proportionnalité dès lors que « seules des ingérences dans lesdits droits fondamentaux ne présentant pas un caractère grave peuvent être justifiées par l'objectif, poursuivi par la réglementation en cause au principal, de prévention, de recherche, de détection et de poursuite d'infractions pénales en général (voy., en ce sens, arrêt du 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 140 ainsi que 146) »[348].

La Cour conclut en considérant que, « dans ces conditions, seuls les objectifs de lutte contre la criminalité grave ou de prévention de menaces graves pour la sécurité publique sont de nature à justifier l'accès des autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et permettant de tirer des conclusions précises sur la vie privée des personnes concernées (voy., en ce sens, arrêt du 2 octobre 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, point 54), sans que d'autres facteurs

[344] *Ibid.*, point 27.
[345] *Ibid.*, point 30.
[346] *Ibid.*, point 29.
[347] *Ibid.*, point 31.
[348] *Ibid.*, point 33.

tenant à la proportionnalité d'une demande d'accès, tels que la durée de la période pour laquelle l'accès est sollicité à de telles données, puissent avoir pour effet que l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général soit susceptible de justifier un tel accès »[349].

Dans le cadre d'une troisième question préjudicielle, la Cour rappelle que l'accès aux données doit répondre à des « règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus. Cette réglementation doit être légalement contraignante en droit interne et indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire (voy., en ce sens, arrêts du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU:C:2016:970, points 117 et 118 ; du 6 octobre 2020, *Privacy International*, C-623/17, EU:C:2020:790, point 68, ainsi que du 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 132 et jurisprudence citée) »[350].

Il est également « essentiel que l'accès des autorités nationales compétentes aux données conservées soit subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante et que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales. En cas d'urgence dûment justifiée, le contrôle doit intervenir dans de brefs délais (voy., en ce sens, arrêt du 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 189 ainsi que jurisprudence citée) »[351]. Ce contrôle requiert, par ailleurs, « que la juridiction ou l'entité chargée d'effectuer ledit contrôle préalable dispose de toutes les attributions et présente toutes les garanties nécessaires en vue d'assurer une conciliation des différents intérêts et droits en cause. S'agissant plus particulièrement d'une enquête pénale, un tel contrôle exige que cette juridiction ou cette entité soit en mesure d'assurer un juste équilibre entre, d'une part, les intérêts liés aux besoins de l'enquête dans le cadre de la lutte contre la criminalité et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel des personnes dont les données sont concernées par l'accès »[352]. La Cour précise également que « lorsque ce contrôle est effectué non par une juridiction mais par une entité administrative indépendante, celle-ci doit jouir d'un statut lui permettant d'agir lors de l'exercice

[349] *Ibid.*, point 35.
[350] *Ibid.*, point 48.
[351] *Ibid.*, point 51.
[352] *Ibid.*, point 52.

de ses missions de manière objective et impartiale et doit être, à cet effet, à l'abri de toute influence extérieure [voy., en ce sens, arrêt du 9 mars 2010, *Commission/Allemagne*, C-518/07, EU:C:2010:125, point 25, ainsi que avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 229 et 230] »[353].

Jean Herveg

Directeur de l'Unité « Libertés & Société de l'Information », CRIDS-NADI, UNamur (www.crids.eu)
Avocat au barreau de Bruxelles
Auteur de la partie consacrée à la Cour européenne des droits de l'homme

Jean-Marc Van Gyseghem

Directeur de Recherche au CRIDS-NADI, UNamur (www.crids.eu)
Avocat au barreau de Bruxelles (www.rawlingsgiles.be)
Auteur de la partie consacrée aux juridictions de l'Union européenne

[353] *Ibid.*, point 53.