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

Guide sur la jurisprudence de la Convention européenne des droits de l'homme

Protection des données

Mis à jour le 28 février 2025

Préparé au sein du Greffe. Il ne lie pas la Cour.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Les éditeurs ou organisations souhaitant traduire et/ou reproduire tout ou partie de ce guide, sous forme de publication imprimée ou électronique (web), sont priés de compléter le formulaire de contact : *demande de reproduction ou republication d'une traduction* pour connaître les modalités d'autorisation.

Pour toute information sur les traductions en cours des Guides sur la jurisprudence, veuillez consulter la liste des *traductions en cours*.

Le texte original de ce guide est en français. Il est mis à jour sur une base régulière. La présente mise à jour a été arrêtée au 28 février 2025. Le texte peut subir des retouches de forme.

Le guide peut être téléchargé à l'adresse *https://ks.echr.coe.int*. Pour toute nouvelle information relative aux publications, veuillez consulter le compte X de la Cour : *https://x.com/ECHR_CEDH*.

© Conseil de l'Europe/Cour européenne des droits de l'homme, 2025

Table des matières

Avis au lecteur 6

Introduction..... 7

I. Définitions et principes de base de la protection des données 7

A. Terminologie de la protection des données..... 7
1. Notion de donnée à caractère personnel et son champ d'application 7
2. Catégories particulières de données 12
a. Catégories dites « sensibles »..... 12
i. Données qui révèlent l'origine raciale ou ethnique 12
ii. Données qui révèlent les opinions politiques, les convictions religieuses ou d'autres convictions, y compris philosophiques 13
iii. Données qui révèlent l'appartenance syndicale..... 13
iv. Données génétiques et biométriques 13
v. Données concernant la santé, la vie sexuelle ou l'orientation sexuelle..... 15
vi. Données relatives aux condamnations pénales et aux infractions 16
b. Autres catégories de données 17
i. Données sur l'emploi 17
ii. Données financières 18
iii. Données de trafic..... 18
iv. Échantillons vocaux..... 20
v. Données de localisation GPS 21
vi. Photos 22

B. Les deux aspects (négatif et positif) de la protection des données 24

C. Les trois « tests » en matière de protection des données..... 28
1. La légalité de l'ingérence 28
2. La légitimité de l'ingérence..... 31
3. La « nécessité dans une société démocratique » de l'ingérence 33
a. L'exigence de minimisation des données collectées ou enregistrées 33
b. L'exigence d'exactitude et de mise à jour des données enregistrées..... 34
c. L'exigence de limiter la durée de conservation des données pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles ont été enregistrées..... 35
d. L'exigence de limiter l'utilisation des données pour le but pour lequel elles ont été enregistrées..... 36
e. L'exigence de transparence du processus de traitement des données 37

II. Protection des données et droit au respect de la vie privée (article 8 de la Convention)..... 37

A. Opérations sur des données susceptibles de porter atteinte au droit au respect de la vie privée 38
1. Collecte des données à caractère personnel..... 38
a. Collecte de données par les autorités à travers la surveillance secrète..... 38
i. Écoutes ciblées et comptage téléphonique..... 38
ii. Interception des messages par biper..... 40
iii. Audiosurveillance et vidéosurveillance 40
iv. Géolocalisation d'un véhicule par GPS 42

v. Surveillance par des détectives privés 42
vi. Contrôle du courrier 42
vii. Opérations secrètes de surveillance, espionnage, surveillance de masse 42
b. Collecte de données par les employeurs sur le lieu de travail 44
c. Collecte des données en vue d'être exploitées comme éléments de preuve dans les affaires judiciaires 47
i. Saisies et perquisitions 47
ii. Acte médicaux obligatoires visant un prélèvement d'échantillons cellulaires 51
d. Collecte de données à caractère personnel dans le contexte de la santé 52
e. Transmission obligatoire de données à caractère personnel 53
2. Conservation des données à caractère personnel 54
a. Le fichage à des fins de lutte contre la criminalité 55
i. Caractère indiscriminé et indifférencié des données stockées 56
ii. Durée du stockage des données 57
iii. Garanties visant la destruction ou l'effacement des données stockées 60
iv. Garanties destinées à réglementer l'accès des tiers et à préserver l'intégrité et la confidentialité des données 61
b. Conservation de données à caractère personnel dans le contexte de la santé 62
c. Conservation en ligne, à des fins journalistiques, des données à caractère personnel 63
3. Divulgation des données à caractère personnel 63
a. L'incidence du consentement préalable 64
b. Divulgation des données dans le contexte des procédures judiciaires 66
c. Divulgation des données pour la protection de la santé publique 68
d. Divulgation des données pour la protection de la sécurité nationale 69
e. Divulgation des données pour la protection du bien-être économique du pays 70
f. Divulgation en masse des données à caractère personnel 71
B. Droits des personnes concernées 71
1. Droit d'accès à ses propres données 72
2. Droit de rectification 75
3. Droit à l'effacement 76
a. « Droit à l'oubli » 77
b. Autres contextes 80
4. Droit de jouir de garanties spéciales de procédure et d'un cadre procédural efficace pour faire valoir ses droits 82

III. Interaction avec d'autres dispositions de la Convention et de ses Protocoles 85

A. Protection des données et droits substantiels 86
1. Protection des données et liberté de pensée, de conscience et de religion (article 9 de la Convention) 87
2. Protection des données et liberté d'expression (article 10 de la Convention) 88
3. Protection des données et interdiction de la discrimination (article 14 de la Convention) 93
4. Protection des données et droit au respect des biens (article 1 du Protocole n° 1) 93
5. Protection des données et liberté de circulation (article 2 du Protocole n° 4) 94
B. Protection des données et droits procéduraux 95
1. Droit à un procès équitable (article 6 de la Convention) 95
a. Garanties générales (article 6 § 1 de la Convention) 96

i. Égalité des armes et respect du contradictoire lors d'une procédure impliquant des données sensibles ou confidentielles 96
ii. Motivation des décisions de justice et protection des données 96
iii. Administration comme éléments de preuve des données à caractère personnel recueillies illégalement ou contrairement à l'article 8 97
iv. Publicité des débats et du prononcé et confidentialité des données 98
v. Durée des procédures judiciaires statuant sur la question de la protection des données 98
b. Garanties spéciales (article 6 §§ 2 et 3 de la Convention) 99
i. Protection des données et respect de la présomption d'innocence (article 6 § 2 de la Convention) 99
ii. Protection des données et droits de la défense (article 6 § 3 b) de la Convention) 100
2. Droit à un recours effectif (article 13 de la Convention) 100
3. Droit à la liberté et sûreté (article 5 de la Convention) 103

IV. Les défis modernes de la protection des données 104

B. Avancées technologiques, algorithmes et intelligence artificielle 104
B. Internet et moteurs de recherche 106
C. Transferts et flux de données 107

Liste des affaires citées 109

Avis au lecteur

Le présent guide fait partie de la série des Guides sur la jurisprudence publiée par la Cour européenne des droits de l'homme (ci-après « la Cour », « la Cour européenne » ou « la Cour de Strasbourg »), dans le but d'informer les praticiens du droit sur les arrêts fondamentaux rendus par celle-ci. En l'occurrence, ce guide analyse et résume la jurisprudence relative aux dispositions de la Convention européenne des droits de l'homme (ci-après « la Convention » ou « la Convention européenne ») applicables en matière de protection des données. Il doit être lu en parallèle avec les guides de jurisprudence élaborés par article, auxquels il fait systématiquement référence.

La jurisprudence citée a été choisie parmi les arrêts et décisions de principe, importants, et/ou récents*.

Les arrêts de la Cour tranchent les affaires dont celle-ci est saisie, mais servent aussi plus largement à clarifier, sauvegarder et développer les normes de la Convention ; ils contribuent ainsi au respect par les États des engagements qu'ils ont pris en leur qualité de Parties contractantes (*Irlande c. Royaume-Uni*, 18 janvier 1978, § 154, série A n° 25, et, plus récemment, *Jeronovičs c. Lettonie* [GC], n° 44898/10, § 109, 5 juillet 2016).

Le système mis en place par la Convention a ainsi pour finalité de trancher, dans l'intérêt général, des questions qui relèvent de l'ordre public, en élevant les normes de protection des droits de l'homme et en élargissant la jurisprudence dans ce domaine à l'ensemble de la communauté des États parties à la Convention (*Konstantin Markin c. Russie* [GC], 30078/06, § 89, CEDH 2012). En effet, la Cour a souligné le rôle de la Convention en tant qu'« instrument constitutionnel de l'ordre public européen » dans le domaine des droits de l'homme (*Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi c. Irlande* [GC], n° 45036/98, § 156, CEDH 2005-VI, et, plus récemment, *N.D. et N.T. c. Espagne* [GC], n°s 8675/15 et 8697/15, § 110, 13 février 2020).

Le Protocole n° 15 à la Convention a récemment inscrit le principe de subsidiarité dans le préambule de la Convention. En vertu de ce principe, « la responsabilité de la protection des droits de l'homme est partagée entre les États parties et la Cour », et les autorités et juridictions nationales doivent interpréter et appliquer le droit interne d'une manière qui donne plein effet aux droits et libertés consacrés par la Convention et ses protocoles (*Grzęda c. Pologne* [GC], § 324).

* La jurisprudence citée peut être dans l'une et/ou l'autre des deux langues officielles (français et anglais) de la Cour et de la Commission européennes des droits de l'homme. Sauf mention particulière indiquée après le nom de l'affaire, la référence citée est celle d'un arrêt sur le fond rendu par une chambre de la Cour. La mention « (déc.) » renvoie à une décision de la Cour et la mention « [GC] » signifie que l'affaire a été examinée par la Grande Chambre. Les arrêts de chambre non définitifs à la date de la présente mise à jour sont signalés par un astérisque (*).

Introduction

1. Les avancées technologiques repoussent les frontières de la surveillance, de l'interception des communications et de la conservation des données, mettant sans cesse les données à caractère personnel face à des défis majeurs. Depuis l'arrêt *Leander c. Suède*, 1987, au sein duquel l'ancienne Cour s'est penchée, pour la première fois, sur la question de la mémorisation par une autorité publique des données à caractère personnel d'un individu, la jurisprudence des organes de la Convention en la matière a connu une évolution certaine.

2. Au fil des années, la Cour a examiné de nombreuses situations soulevant des questions liées à cette problématique. Un large éventail d'opérations effectuées sur des données à caractère personnel telles que la collecte, la mémorisation, l'exploitation et la diffusion de telles données fait désormais l'objet d'une jurisprudence des organes de la Convention qui est décrite dans ce guide. Cette jurisprudence s'étoffe au fur et à mesure de l'évolution rapide des technologies d'information et de communication.

I. Définitions et principes de base de la protection des données

3. Le droit à la protection des données à caractère personnel ne fait pas partie, en tant que droit autonome, des droits et libertés garantis par la Convention. La Cour a néanmoins reconnu que la protection des données à caractère personnel joue un rôle fondamental dans l'exercice du droit au respect de la vie privée et familiale, du domicile et de la correspondance garanti par l'article 8 de la Convention (*Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande* [GC], 2017, § 137 ; *Z c. Finlande,* 1997, § 95 ; *L.B. c. Hongrie* [GC], 2023, § 103). Cette disposition permet, dans le système de la Convention, d'assurer, de façon principale, la protection des données à caractère personnel, même si des considérations liées à cette protection peuvent également intervenir sur le terrain d'autres disposions de la Convention et de ses protocoles additionnels.

A. Terminologie de la protection des données

4. Avec l'essor des technologies, les opérations effectuées sur des données à caractère personnel susceptibles de constituer un « traitement automatisé » prennent des formes très différentes. En dépit d'une approche généreuse de la Cour quant à la définition de la notion de « vie privée », qui lui a permis de développer une jurisprudence répondant à l'évolution de la société, toute opération effectuée sur des données à caractère personnel n'entre pas nécessairement dans le champ d'application de l'article 8 ou ne porte pas nécessairement atteinte à l'un des intérêts qu'il protège.

1. Notion de donnée à caractère personnel et son champ d'application

5. La Cour explique dans ses arrêts la notion de « donnée à caractère personnel » par référence à la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, entrée en vigueur en 1985 et modernisée en 2018 (« Convention 108 »), dont le but est « de garantir, sur le territoire de chaque Partie, à toute personne physique (...) le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant (article 1) » (*Amann c. Suisse* [GC], 2000, § 65 ; *Haralambie c. Roumanie*, 2009, § 77). La Cour indique de façon claire que, selon l'article 2 de la Convention 108, une donnée à caractère personnel se définit comme « toute information concernant une personne physique identifiée ou identifiable » (*Amann c. Suisse* [GC], 2000, § 65 ; *Haralambie c. Roumanie,* 2009, § 77).

6. Une telle donnée comporte dès lors non seulement des éléments capables de conduire à l'établissement direct de l'identité civile d'un individu (le « sujet des données »), tel que son nom ou son prénom (*Guillot c. France*, 1996, §§ 21-22 ; *Mentzen c. Lettonie* (déc.), 2004 ; *Güzel Erdagöz c. Turquie*, 2008, § 43 ; *Garnaga c. Ukraine*, 2013, § 36 ; *Henry Kismoun c. France,* 2013, § 25 ; *Hájovský c. Slovaquie*, 2021 §§ 11-12 et 41), mais aussi tout élément susceptible de conduire indirectement à l'identification d'une personne tels que des adresses IP (Internet Protocol) dynamiques (*Benedik c. Slovénie*, 2018, §§ 107-108 ; voir aussi, concernant les adresses IP masquées par un VPN, *Le Marrec c. France* (déc.), 2024, §§ 51 et § 54).

7. Même si la question de la protection des données à caractère personnel semble concerner, de prime abord, les personnes physiques, sous l'angle de leur droit au respect de la « vie privée », garanti par l'article 8, les personnes morales peuvent également l'invoquer devant la Cour si elles sont directement affectées par une mesure qui porte atteinte à leur droit au respect de leur « correspondance » ou de leur « domicile ». Tel est le cas, par exemple, d'une décision enjoignant à une société de remettre une copie de l'intégralité des données du serveur informatique qu'elle partageait avec d'autres sociétés (*Bernh Larsen Holding AS et autres c. Norvège*, 2013, § 106) ou de l'interception, par le ministère de la Défense, sur la base d'un mandat, des communications vers l'extérieur d'organisations œuvrant dans le domaine des libertés civiles (*Liberty et autres c. Royaume-Uni*, 2008, §§ 56-57). En revanche, s'agissant des mesures qui mettaient en cause la protection des données personnelles des membres d'une organisation religieuse et le respect de leur « vie privée », l'organisation n'était pas directement affectée, et n'était pas une « victime », au sens de l'article 34 de la Convention (*Avilkina et autres c. Russie*, 2013, § 59).

8. Les données à caractère personnel prennent des formes très différentes. Il s'agit, par exemple :

- des informations sur l'abonné à un fournisseur de services Internet, associées à une adresse IP dynamique spécifique attribuée à un moment donné (*Benedik c. Slovénie*, 2018, §§ 108-109), y compris à une adresse IP masquée par un VPN si le requérant peut être identifié et localisé (*Le Marrec c. France* (déc.), 2024, § 54) ;
- des échantillons de voix enregistrés sur un support permanent et soumis à un processus d'analyse directement destiné à identifier cette personne à la lumière d'autres données personnelles (*P.G. et J.H. c. Royaume-Uni*, 2001, § 59) ;
- des échantillons cellulaires et profils ADN (S. et Marper c. Royaume-Uni [GC], 2008, §§ 70-77) ou des empreintes digitales (*ibidem*, § 84) qui, en dépit de leur caractère objectif et irréfutable, contenaient des informations uniques sur l'individu concerné et permettaient une identification précise dans un grand nombre de circonstances (*ibidem*, § 85) ;
- des informations relatives à une personne donnée, obtenues soit à partir de documents bancaires, que ces documents concernent, ou non, des données sensibles ou des activités professionnelles (*M.N. et autres c. Saint-Marin*, 2015, §§ 51 et suivants), soit depuis la base de données du Service d'information sur les contribuables, y compris, en particulier, des informations sur les revenus et les actifs nets d'une personne, ainsi que sur les affaires pendantes devant les autorités fiscales (*Casarini c. Italie* (déc.), 2024, §§ 56-57) ;
- des données relatives à la profession d'une personne identifiée ou identifiable collectées et mémorisées par la police (*Khelili c. Suisse*, 2011, § 56) ;
- des données de l'usage fait d'Internet et de la messagerie instantanée (Yahoo) d'un employé sur son lieu de travail obtenues par la mise en place d'une surveillance (*Bărbulescu c. Roumanie* [GC], 2017, §§ 18, 74-81) ;
- d'une copie des données électroniques saisies dans le cabinet d'avocats, même si elles n'avaient pas été déchiffrées, transcrites et officiellement attribuées aux personnes concernées (*Kırdök et autres c. Turquie*, 2019, § 36) ;

- des données collectées dans le cadre de la vidéosurveillance non secrète dans des amphithéâtres universitaires (*Antović et Mirković c. Monténégro*, 2017, §§ 44-45) ;
- des informations sur le revenu imposable et le patrimoine d'un grand nombre de personnes, nonobstant le fait que le public avait la possibilité d'accéder à ces données suivant certaines règles (*Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande* [GC], 2017, § 138) ;
- des données relatives aux circonstances de la naissance et de l'abandon d'une personne, qui comportaient des informations nécessaires à la découverte de la vérité concernant un aspect important de l'identité personnelle (*Gaskin c. Royaume-Uni*, 1989, § 39 ; *Mikulić c. Croatie*, 2002, §§ 54-64 ; *Odièvre c. France* [GC], 2003, §§ 28-29 ; *Gauvin-Fournis et Silliau c. France*, 2023, §§ 106 et 112 ; *Cherrier c. France*, 2024, § 50) ;
- des données figurant dans un accord de divorce, comprenant des détails sur la répartition des biens matrimoniaux, la garde et la résidence des enfants mineurs, le versement d'une pension alimentaire et une vue d'ensemble des biens/des revenus du requérant (*Liebscher c. Autriche*, 2021, §§ 31 et 68).
- d'enregistrements vidéo de conversations ayant été réalisés par un individu dans un cadre professionnel au moyen d'une caméra cachée et ayant finalement été utilisés dans une procédure pénale dirigée contre le requérant (*Sârbu c. Roumanie*, 2023 §§ 39-41).

9. Selon l'article 2 de la Convention 108, un « traitement de données » comprend : « toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel, telles que la collecte, l'enregistrement, la conservation, la modification, l'extraction, la communication, la mise à disposition, l'effacement ou la destruction des données, ou l'application d'opérations logiques et/ou arithmétiques à ces données ». Avec l'essor des technologies, les opérations susceptibles de constituer un « traitement de données » prennent des formes très différentes. Selon la jurisprudence de la Cour, constituent des exemples typiques de tels traitements :

- la collecte par la police, auprès d'un fournisseur de services Internet, de renseignements associés à l'adresse IP dynamique d'un individu (*Benedik c. Slovénie*, 2018, §§ 108-109)
- le fait de recueillir et mémoriser de manière systématique des informations de nature publique sur un individu, par exemple, des informations relatives à son activité politique (*Rotaru c. Roumanie* [GC], 2000, §§ 43-44 ; *Association "21 décembre 1989" et autres c. Roumanie*, 2011, §§ 167-168 ; *Amann c. Suisse* [GC], 2000, §§ 65-67 ; *Catt c. Royaume-Uni*, 2019, § 93) ;
- l'inscription du nom d'une personne dans une base de données judiciaires interne d'un ministère compétent (*L.F. c. France* (déc.), 2024, § 30), dans un fichier judiciaire national d'auteurs d'infractions sexuelles (*Gardel c. France*, 2009, § 58) ou dans une base de données nationale recensant toutes les procédures pénales dirigées contre des particuliers (*N.F. et autres c. Russie*, 2023, §§ 34 et 49), ainsi que la collecte et la conservation d'empreintes digitales de personnes soupçonnées d'avoir commis des infractions (*M.K. c. France*, 2013, § 29) ;
- l'enregistrement en secret, au poste de police, sur un support permanent, des voix d'individus aux fins d'un processus d'analyse directement destiné à identifier ces personnes à la lumière d'autres données (*P.G. et J.H. c. Royaume-Uni*, 2001, §§ 59-60) ;
- le fait de filmer un individu dans la salle de garde à vue d'un commissariat de police par des caméras installées pour des raisons de sécurité et parfaitement visibles, d'enregistrer la séquence litigieuse sur un support permanent et de l'insérer dans un montage en vue d'une utilisation ultérieure (*Perry c. Royaume-Uni*, 2003, § 41) ;
- le fait de recueillir systématiquement et de conserver des données issues de la surveillance par GPS, indiquant l'endroit où se trouvait l'intéressé et les déplacements de celui-ci en public (*Uzun c. Allemagne*, 2010, §§ 49-53) ;

- la publication dans un magazine d'un article illustré par des photos de célébrités prises à leur insu (*Von Hannover c. Allemagne (no 2)* [GC], 2012, §§ 95-99) ;
- l'enregistrement et la transmission aux médias d'une vidéo provenant d'une télévision en circuit fermé filmant une personne tentant de se suicider dans un lieu public (*Peck c. Royaume-Uni*, 2003, §§ 59-63) ;
- le fait pour les services de police de mémoriser des données relatives à la profession supposée d'une personne et de les conserver (*Khelili c. Suisse*, 2011, § 56) ;
- la divulgation par un hôpital psychiatrique, aux journalistes, d'informations confidentielles extrêmement sensibles à propos de la vie privée d'une patiente (*Mockutė c. Lituanie*, 2018, § 99) ;
- la collecte par l'État, dans le cadre de la lutte contre le dopage dans le sport, de la localisation et d'emplois du temps quotidiens détaillés, y compris le week-end, de sportifs de haut niveau (*Fédération nationale des associations et syndicats de sportifs (FNASS) et autres c. France*, 2018, §§ 155-159).
- la pratique consistant à scanner et enregistrer systématiquement la correspondance privée des détenus – aussi bien celle qu'ils voulaient expédier que celle qui leur était envoyée – sur le Système informatique du Réseau judiciaire national (*Nuh Uzun et autres c. Turquie*, 2022, §§ 80-82).
- le recours à une technologie de reconnaissance faciale dans le but, d'une part, d'identifier le requérant, qui s'était livré à une manifestation en solo sans déclaration préalable, à partir de photographies et vidéos publiées sur une chaîne Telegram et, d'autre part, de repérer et interpeller l'intéressé alors qu'il se déplaçait en métro (*Glukhin c. Russie*, 2023, § 73).

10. De telles mesures sont presque toujours considérées par la Cour comme des ingérences, à des degrés de gravité divers, dans le droit au respect de la vie privée, du domicile ou de la correspondance des sujets des données.

11. Toutefois, toute opération effectuée sur des données à caractère personnel n'entre pas nécessairement dans le champ d'application de l'article 8 ou ne porte pas automatiquement atteinte à l'un des intérêts qu'il protège. Ainsi, dans l'affaire *Mehmedovic c. Suisse* (déc.), 2018 (§ 18), la Cour a considéré que des informations éparses, recueillies par hasard et sans aucune pertinence pour l'investigation, qui étaient loin de constituer une collecte systématique ou permanente, n'entraînaient pas d'ingérence dans le droit au respect de la vie privée de l'individu concerné. En outre, dans l'affaire *Cakicisoy et autres c. Chypre* (déc.), 2014 (§§ 50-52), le prélèvement sur les requérants, par les autorités, d'échantillons de sang afin d'extraire leur profile ADN pour être utilisé dans le cadre d'un programme d'exhumation visant l'identification des restes de leurs proches disparus, ou la destruction de ces échantillons lorsqu'ils n'étaient plus soumis à des formulaires de consentement valides, n'ont pas été jugés constitutifs d'une ingérence dans le droit des requérants au respect de leur vie privée.

12. Il ressort de la jurisprudence de la Cour que les opérations effectuées sur des données à caractère personnel entrent dans le champ d'application de l'article 8 si des informations ont été recueillies sur une personne bien précise (*Amann c. Suisse*, [GC], 2000, §§ 66-67 ; *Rotaru c. Roumanie* [GC], 2000, §§ 43-44), si les données en question ont fait l'objet d'un enregistrement systématique ou permanent (*Uzun c. Allemagne*, 2010, § 51), si elles ont été soumises à un processus d'analyse directement destiné à identifier un individu à la lumière d'autres données personnelles (*P.G. et J.H. c. Royaume-Uni*, 2001, § 57) ou si elles ont été rendues publiques d'une manière ou dans une mesure excédant ce à quoi les intéressés pouvaient raisonnablement s'attendre (*Peck c. Royaume-Uni,* 2003, §§ 58-59 ; *Perry c. Royaume-Uni,* 2003, § 38). Le contexte particulier dans lequel les informations sur une personne ont été recueillies et conservées, la nature

des données consignées, la manière dont elles sont utilisées et traitées et les résultats qui peuvent en être tirés jouent aussi un rôle important (*S. et Marper c. Royaume-Uni* [GC], 2008, § 67).

13. Un élément significatif, quoique pas nécessairement décisif, est le fait de savoir si un individu est raisonnablement en droit d'attendre la protection de sa vie privée (*Perry c. Royaume-Uni,* 2003, § 37 ; *Bărbulescu c. Roumanie* [GC], 2017, § 80 ; *Glukhin c. Russie*, 2023, § 66). S'agissant des activités en ligne, l'anonymat des renseignements personnels en ligne est une considération importante dans cette appréciation et le fait pour un abonné à un fournisseur de service Internet de ne pas avoir dissimulé son adresse IP dynamique ne saurait être tenu pour déterminant dans l'appréciation du point de savoir si son espérance en matière de protection de la vie privée était raisonnable d'un point de vue objectif (*Benedik c. Slovénie*, 2018, § 116). Autrement, sur un lieu de travail, les instructions d'un employeur ne peuvent pas réduire à néant l'exercice de la vie privée sociale des employés, le respect de leur vie privée et de la confidentialité de leurs communications continuant donc à s'imposer, même si ces dernières peuvent être limitées dans la mesure du nécessaire (*Bărbulescu c. Roumanie* [GC], 2017, §§ 80-81 ; voir aussi, pour le cadre professionnel, *Sârbu c. Roumanie*, 2023, §§ 37-38 ; voir aussi, dans le contexte du contrôle par un parti politique de la correspondance électronique de ses membres, *Tena Arregui c. Espagne*, 2024, § 38). Le fait de surveiller les faits ou gestes d'un individu dans un lieu public au moyen de mécanismes de surveillance peut tomber sous le coup de l'article 8 dès lors que les données à caractère personnel ainsi collectées sont enregistrées de manière systématique ou permanente (*Glukhin c. Russie*, 2023, § 66) ou que la divulgation de ces données, par ses modalités ou son ampleur, excède ce à quoi les intéressés pouvaient raisonnablement s'attendre (*Peck c. Royaume-Uni*, 2003, § 62 ; *Perry c. Royaume-Uni,* 2003, §§ 41-43). S'agissant des articles de presse donnant des informations sur l'arrestation d'un acteur de télévision illustrés par des photos, la Cour a jugé que l'« espérance légitime » d'un acteur de voir sa vie privée effectivement protégée était limitée par le fait qu'il s'était en quelque sorte lui-même projeté au-devant de la scène en révélant lui-même des détails de sa vie privée dans un certain nombre d'interviews (*Axel Springer AG c. Allemagne* [GC], 2012, § 101).

14. S'agissant de la nature des données consignées, certaines données à caractère personnel ou certaines méthodes de traitement de ces données sont davantage problématiques car elles révèlent des informations plus sensibles sur la conduite, les opinions ou les sentiments des individus (*Uzun c. Allemagne,* 2010, § 52, qui procède à une comparaison des données collectées par GPS avec les données collectées par des moyens visuels ou acoustiques de surveillance). La mémorisation ou divulgation sans autorisation de l'intéressé de données hautement intimes ou sensibles, relatives, par exemple, à la santé d'un individu, entrent nécessairement dans le champ d'application de l'article 8 (*Z c. Finlande,* 1997, § 71 ; *Radu c. République de Moldova*, 2014, § 27 ; *Mockutė c. Lituanie*, 2018, §§ 93-95). La conservation d'échantillons cellulaires et des profils ADN d'un individu doit être considérée comme constituant en soi une atteinte à son droit au respect de la vie privée au vu de la nature et de la quantité d'informations personnelles qu'ils contiennent, même si seule une petite partie de ces informations soit en réalité extraite ou utilisée par les autorités et qu'aucun préjudice immédiat n'ait été causé (*S. et Marper c. Royaume-Uni* [GC], 2008, §§ 70-77).

15. Le fait que les données à caractère personnel étaient déjà dans le domaine public ou que le public avait la possibilité d'y accéder ne les soustrait pas nécessairement à la protection de l'article 8 (*Satakunnan Markkinapörssi oy et Satamedia oy c. Finlande* [GC], 2017, § 134 ; *L.B. c. Hongrie* [GC], 2023 ; § 104). Des données de nature publique peuvent relever de la « vie privée » d'un individu lorsqu'elles ont été recueillies et mémorisées d'une manière systématique (*P.G. et J.H. c. Royaume-Uni*, 2001, § 57 ; *Peck c. Royaume-Uni,* 2003, §§ 58-59 ; *Perry c. Royaume-Uni,* 2003, § 38), même sans recours à des méthodes de surveillance secrètes (*Rotaru c. Roumanie* [GC], 2000, §§ 43-44 ; *Antović et Mirković c. Monténégro*, 2017, §§ 44-45). L'article 8 consacre 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 et déjà dans le domaine public, sont collectées, traitées et diffusées à la collectivité, selon des formes ou modalités telles que leurs droits

au titre de l'article 8 puissent être mis en jeu (*Satakunnan Markkinapörssi oy et Satamedia oy c. Finlande* [GC], 2017, § 137 ; *L.B. c. Hongrie* [GC], 2023 ; § 103).

16. Dans la plupart des affaires où un traitement des données à caractère personnel était destiné à permettre aux autorités de conduire une enquête contre leur titulaire ou à recueillir des moyens de preuve dans le cadre d'une procédure judiciaire devant les juridictions nationales, la Cour a estimé qu'un tel traitement entrait dans le champ d'application de l'article 8 et donnait lieu à une ingérence dans la vie privée des personnes concernées (*Perry c. Royaume-Uni,* 2003, §§ 39-43 ; *Uzun c. Allemagne*, 2010, §§ 51-52 ; *Vukota-Bojić c. Suisse*, 2016, §§ 57-59 ; *López Ribalda et autres c. Espagne* [GC], 2019, § 94 ; *Sârbu c. Roumanie*, 2023, §§ 38 et 41 ; voir, *a contrario*, *Lupker et autres c. Pays-Bas*, 1992, sur l'utilisation par la police, à des fins d'identification des requérants, de photographies qui avaient été volontairement remises aux autorités ou qui avaient été prises par la police lors d'arrestations antérieures ; *Friedl c. Autriche*, 1994, §§ 50-51, sur une prise de photographies par les autorités durant une manifestation dans le but d'une possible enquête ultérieure sur des manifestants pour infractions au code de la route).

17. Enfin, pour que l'article 8 puisse entrer en ligne de compte, les résultats qui peuvent être tirés d'un traitement des données à caractère personnel doivent atteindre un certain niveau de gravité de manière à causer un préjudice à la jouissance du droit au respect de la vie privée (*M.L. et W.W. c. Allemagne*, 2018, § 88). Dans l'affaire *Vučina c. Croatie* (déc.) 2019 (§ 50), la Cour a rejeté comme incompatible *ratione materiae* un grief tiré de la publication d'une photographie dans un magazine féminin sous un titre erroné, désignant la requérante par le nom d'une autre personne. Pour la Cour, le faible degré de gravité de cette erreur et le désagrément très limité qui en est résulté n'étaient pas suffisamment sérieux pour que l'article 8 puisse entrer en jeu.

2. Catégories particulières de données

18. Certaines informations hautement intimes ou sensibles justifient clairement, aux yeux de la Cour, une protection renforcée. D'autres catégories de données doivent être également sujettes à caution, compte tenu de l'essor des technologies qui démultiplient les possibilités d'accès à ces données et leur interconnexion.

a. Catégories dites « sensibles »

19. Selon l'article 6 de la Convention 108, les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle d'un individu, ou à ses éventuelles condamnations pénales ne peuvent être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées. Les informations relevant de ces catégories, que la Cour qualifie de « sensibles », justifient, selon elle, une protection accrue.

i. Données qui révèlent l'origine raciale ou ethnique

20. L'identité ethnique d'un individu doit être considérée comme un élément important de sa vie privée (*S. et Marper c. Royaume-Uni*, [GC], 2008, § 66; *Ciubotaru c. Moldova*, 2010, § 49). Il faut attacher de l'importance aux données qui pourraient, compte tenu particulièrement du rythme élevé auquel se succèdent les innovations dans le domaine de la génétique et des technologies de l'information, révéler l'origine ou ethnique d'une personne (*S. et Marper c. Royaume-Uni* [GC], 2008, § 71). Des échantillons et des profils ADN contiennent beaucoup d'informations sensibles et fournissent un moyen de découvrir les relations génétiques pouvant exister entre des individus et de tirer des déductions quant à l'origine ethnique (*ibidem*, §§ 72-77 ; *Aycaguer c. France,* 2017, § 33). Dans une affaire relative à l'inscription de l'origine ethnique d'un individu sur les registres officiels, la Cour, soulignant la nature hautement sensible de l'enregistrement de ces données, a reconnu l'existence d'une obligation positive de l'État de garantir au sujet des données le droit de faire

rectifier l'inscription en question sur la base d'éléments de preuve objectifs (*Ciubotaru c. Moldova*, 2010, §§ 52-59).

ii. Données qui révèlent les opinions politiques, les convictions religieuses ou d'autres convictions, y compris philosophiques

21. Les données qui révèlent les opinions politiques sont considérées comme une catégorie « sensible » de données à caractère personnel et, aux yeux de la Cour, il est inacceptable que les autorités nationales négligent cet aspect et traitent ces données en suivant simplement les règles générales au niveau interne, sans prendre en compte le fait qu'elles doivent bénéficier d'un niveau de protection accrue (*Catt c. Royaume-Uni*, 2019, § 112). Dans l'affaire *Catt c. Royaume-Uni*, qui concernait la conservation dans une base de données de la police de données relatives à un manifestant pacifique, les juridictions nationales avaient simplement fait référence à la loi sur la protection des données en général lors de l'examen de la légalité de l'ingérence. La Cour a conclu à une violation de l'article 8 en soulignant que la nature sensible des données en question aurait dû constituer un élément central de l'affaire devant les juridictions internes, comme elle l'a été devant la Cour (*ibidem*, § 112). Elle a également conclu à la violation de cet article dans l'affaire *M.D. et autres c. Espagne*, 2022, (§§ 63-64), qui concernait un rapport que la police avait rédigé à propos de juges et magistrats qui exerçaient en Catalogne et qui avaient signé un manifeste dans lequel ils s'étaient déclarés, d'un point de vue juridique, favorables à la possibilité pour le peuple catalan d'exercer son « droit de décider », rapport qui révélait, en particulier, les opinions politiques de certains des requérants. La Cour a également précisé que les données à caractère personnel qui révèlent une opinion politique appellent un niveau de protection accru (*Glukhin c. Russie*, 2023 (§§ 76 et 86), où les données à caractère personnel relatives au requérant qui avaient été traitées renfermaient des informations sur la participation de l'intéressé à une manifestation pacifique).

22. Le droit à la protection des données à caractère personnel qui révèlent les convictions religieuses ou d'autres convictions, y compris philosophiques, d'un individu a été examiné par la Cour dans les affaires *Sinan Işık c. Turquie*, 2010 (§ 37) et *Mockutė c. Lituanie*, 2018 (§ 117). S'agissant de la mention de la religion sur les cartes d'identité des requérants, la Cour a mis en exergue l'importance du droit à la protection des données relatives aux convictions religieuses, qui figurent parmi les éléments les plus essentiels de l'identité des croyants et de leur conception de la vie protégées par l'article 9 de la Convention (*Sinan Işık c. Turquie,* 2010, § 37).

iii. Données qui révèlent l'appartenance syndicale

23. Des données à caractère personnel qui révèlent l'appartenance syndicale d'une personne sont également des données sensibles, qui bénéficient d'une protection accrue. Dans l'affaire *Catt c. Royaume-Uni*, 2019 (§ 112), des informations avaient été collectées par les autorités de police sur la participation du requérant aux différentes manifestations organisées par un certain nombre de syndicats, notamment son nom, sa présence, sa date de naissance et son adresse. Dans certains cas, son apparence avait également été décrite, accompagnée des photos prises lors des manifestations en question (*ibidem*, § 10). La Cour souligne que le fait pour un individu de s'engager dans des manifestations pacifiques bénéficie d'une protection spécifique en vertu de l'article 11 de la Convention, qui contient également une protection spéciale pour les syndicats (*ibidem*, § 123). En l'occurrence, si la collecte par la police de données à caractère personnel concernant le requérant pouvait passer pour une mesure justifiée, la conservation de ses données ne répondait pas, quant à elle, à un besoin impérieux, en l'absence de toute règle fixant la durée maximale de conservation de pareilles données (*ibidem*, §§ 117-119).

iv. Données génétiques et biométriques

24. La Cour a traité plusieurs affaires concernant le prélèvement ou la conservation des :

- échantillons cellulaires (*Van der Velden c. Pays-Bas* (déc.), 2005 ; *Schmidt c. Allemagne* (déc.), 2006 ; *S. et Marper c. Royaume-Uni* [GC], 2008 ; *Canonne c. France* (déc.), 2015 ; *Caruana c. Malte* (déc.), 2018 ; *Trajkovski et Chipovski c. Macédoine du Nord*, 2020; *Boljević c. Serbie*, 2020) ;
- profils ADN (*Van der Velden c. Pays-Bas* (déc.), 2005 ; *Schmidt c. Allemagne* (déc.), 2006 ; *S. et Marper c. Royaume-Uni* [GC], 2008 ; *W. c. Pays-Bas* (déc.), 2009 ; *Peruzzo et Martens c. Allemagne* (déc.), 2013 ; *Canonne c. Francee* (déc.), 2015 ; *Aycaguer c. France*, 2017 ; *Mifsud c. Malte*, 2019 ; *Gaughran c. Royaume-Uni*, 2020 ; *Trajkovski et Chipovski c. Macédoine du Nord*, 2020 ; *Dragan Petrović c. Serbie*, 2020) ;
- empreintes digitales (*McVeigh, O'Neill et Evans c. Royaume-Uni*, 1981 ; *Kinnunen c. Finlande*, 1993 ; *S. et Marper c. Royaume-Uni* [GC], 2008 ; *Dimitrov-Kazakov c. Bulgarie*, 2011 ; *M.K. c. France*, 2013 ; *Suprunenko c. Russie* (déc.) [comité], 2018 ; *Gaughran c. Royaume-Uni*, 2020 ; *P.N. c. Allemagne*, 2020 ; *Willems c. Pays-Bas* (déc.), 2021) ;
- empreintes palmaires (*P.N. c. Allemagne*, 2020) ;
- échantillons vocaux (*P.G. et J.H. c. Royaume-Uni*, 2001 ; *Allan c. Royaume-Uni*, 2002 ; *Doerga c. Pays-Bas*, 2004 ; *Vetter c. France*, 2005 ; *Wisse c. France*, 2005).

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

26. S'agissant des échantillons cellulaires, leur conservation constitue en soi une atteinte au droit au respect de la vie privée des individus concernés, compte tenu de la nature et la quantité des informations personnelles qu'ils contiennent, nonobstant le fait que seule une petite partie de ces informations soit en réalité extraite ou utilisée par les autorités pour les besoins de la création de profils ADN et qu'aucun préjudice immédiat ne soit provoqué dans un cas particulier (*ibidem*, § 73 ; *Amann c. Suisse* [GC], 2000, § 69).

27. Quant aux profils ADN, la possibilité qu'ils offrent de tirer des déductions quant à l'origine ethnique rend leur conservation d'autant plus sensible et susceptible de porter atteinte au droit à la vie privée, appelant une protection accrue (*S. et Marper c. Royaume-Uni* [GC], 2008, § 76). Même si les informations contenues dans les profils ADN peuvent passer pour objectives et irréfutables, le simple fait que les profils ADN fournissent un moyen de découvrir les relations génétiques pouvant exister entre des individus suffit en soi pour conclure que leur conservation constitue une atteinte au droit à la vie privée de ces individus, nonobstant les garanties qui les entourent et la probabilité que survienne un préjudice dans un cas donné (*ibidem*, § 75 ; *Amann c. Suisse* [GC], 2000, § 69). Le fait que l'information n'était intelligible qu'à l'aide de l'informatique du fait qu'elle était codée, et qu'elle ne pouvait être interprétée que par un nombre restreint de personnes n'y changeait rien (*S. et Marper c. Royaume-Uni* [GC], 2008, §§ 74-75).

28. En matière d'empreintes digitales, leur conservation sans le consentement de l'individu concerné ne saurait passer pour une mesure neutre ou banale du fait qu'elles contiennent objectivement des informations uniques sur l'individu concerné et permettent une identification précise dans un grand nombre de circonstances (*ibidem*, § 84). Même si la conservation, dans un fichier des autorités nationales, des empreintes digitales d'un individu identifié ou identifiable a un impact moindre sur sa vie privée que celle des échantillons cellulaires et profils ADN (*ibidem*, § 69), elle peut donner lieu à des préoccupations importantes concernant le respect de la vie privée en dépit du caractère objectif et irréfutable de ces données (*ibidem*, § 85, opérant un revirement de jurisprudence par rapport à la décision de la Commission dans l'affaire *Kinnunen c. Finlande,* 1996). Dans l'affaire *Willems c. Pays-Bas* (déc.), 2021, des griefs tirés de l'obligation, en vertu de la loi sur les passeports, de faire relever les empreintes digitales lors de la demande de passeport ainsi que de

la conservation de ces empreintes sur une puce électronique suite à l'incorporation dans le droit national (sans aucune marge de manœuvre pour les autorités nationales) du règlement de l'UE sur les éléments de sécurité et la biométrie dans les documents de voyage ont été rejetés comme manifestement mal fondés eu égard à la « présomption de protection équivalente » en vertu du droit de l'UE (*ibidem*, §§ 26-36).

29. La conservation des échantillons cellulaires et profils ADN a un impact plus grand sur la vie privée que celle d'empreintes digitales (*S. et Marper c. Royaume-Uni* [GC], 2008, § 86). S'il peut se révéler nécessaire de distinguer entre les empreintes digitales, d'une part, et les échantillons et profils, d'autre part, pour ce qui est de leur prélèvement, de leur utilisation et de leur stockage lorsqu'il s'agit de trancher la question de la justification de l'ingérence, il n'en demeure pas moins que la conservation d'empreintes digitales constitue une atteinte en soi au droit au respect de la vie privée.

30. Dans certaines circonstances, notamment dans le cadre de procédures mettant en cause la paternité d'un individu, les autorités peuvent contraindre une personne à fournir un échantillon génétique, à condition que les droits de la défense soient respectés et qu'un juste équilibre soit ménagé entre les intérêts en jeu (*Mifsud c. Malte*, 2019, §§ 77-78). L'article 8 n'interdit pas en tant que tel le recours à une intervention médicale contre la volonté d'un suspect, ou contre la volonté d'un témoin, en vue de l'obtention de preuves, de telles méthodes, y compris dans le domaine civil, n'étant pas en elles-mêmes contraires à l'état de droit et à la justice naturelle (*ibidem*, § 71). Un système qui ne prévoit pas de moyens de contraindre un père présumé à subir un test ADN n'est toutefois pas en soi incompatible avec les obligations découlant de l'article 8, notamment si le système en question offre d'autres moyens grâce auxquels une autorité indépendante peut statuer rapidement sur l'action en recherche de paternité (*Mikulić c. Croatie*, 2002, §§ 55, 64).

v. Données concernant la santé, la vie sexuelle ou l'orientation sexuelle

31. Les informations relatives à la santé d'une personne constituent un élément important de sa vie privée (*Yvonne Chave née Jullien c. France,* 1991, § 75 ; *L.L. c. France*, 2006 ; *Radu c. Moldavie*, 2014 ; *L.H. c. Lettonie*, 2014, § 56 ; *Konovalova c. Russie*, 2014, §§ 27, 41 ; *Y.Y. c. Russie*, 2016, § 38 ; *Surikov c. Ukraine*, 2017 ; *Frâncu c. Roumanie*, 2020, § 52). Le respect du caractère confidentiel de ces informations est capital non seulement pour protéger la vie privée des malades, mais également pour préserver leur confiance dans le corps médical et les services de santé en général. Ces considérations valent particulièrement lorsqu'il s'agit de protéger la confidentialité des informations relatives à la séropositivité d'une personne (*Z c. Finlande*, 1997, § 96 ; *Kiyutin c. Russie*, 2011, § 64 ; *Armonienė c. Lituanie*, 2008, § 40 ; *Biriuk c. Lituanie*, 2008, § 39 ; *I. c. Finlande*, 2008, § 38 ; *C.C. c. Espagne*, 2009, § 33 ; *Y. c. Turquie* (déc.), 2015, § 65 ; *P.T. c. République de Moldova*, 2020, §§ 5-6, 26 ; *Y.G. c. Russie*, 2022, § 45). La divulgation de tels renseignements pourrait avoir des conséquences dévastatrices sur la vie privée et familiale de la personne concernée et sur sa situation sociale et professionnelle, l'exposant à l'opprobre et à un risque d'exclusion (*Z c. Finlande*, 1997, § 96 ; *C.C. c. Espagne*, 2009, § 33 ; *P. et S. c. Pologne*, 2012, § 128 ; *Avilkina et autres c. Russie,* 2013, § 45 ; *Y. c. Turquie* (déc.), 2015, § 65 ; *Y.G. c. Russie*, 2022, § 45).

32. L'intérêt qu'il y a à protéger la confidentialité de telles informations pèsera donc lourdement dans la balance lorsqu'il s'agira de déterminer si l'ingérence était proportionnée au but légitime poursuivi, sachant qu'une telle ingérence ne peut se concilier avec l'article 8 que si elle vise à défendre un aspect primordial de l'intérêt public (*Z c. Finlande*, 1997, § 96). Compte tenu du caractère extrêmement intime et sensible des informations se rapportant à la séropositivité, toute mesure prise par un État pour contraindre à les communiquer ou à les divulguer, sans le consentement de la personne concernée, appelle un examen des plus rigoureux de la part de la Cour (*ibidem*, § 96).

33. Ainsi la Cour a conclu à la violation de l'article 8 par exemple dans les affaires *Z c. Finlande*, 1997 (§§ 113-114), pour la publication de l'identité et de la séropositivité d'une femme dans un arrêt, rendu au cours de la procédure pénales intentées contre son mari, transmis à la presse ; *L.L. c. France*, 2006 (§§ 32-48), pour la reproduction dans un jugement de divorce d'un extrait d'une pièce médicale personnelle ; *I. c. Finlande*, 2008 (§§ 35-49), pour la protection insuffisante contre les accès non autorisés du dossier médical d'une infirmière séropositive ; *C.C. c. Espagne*, 2009 (§§ 26-41), pour la publication de l'identité du requérant dans le jugement rendu en rapport avec sa séropositivité ; *P. et S. c. Pologne*, 2012 (§§ 128-137), pour la divulgation d'informations par un hôpital public sur une mineure enceinte qui souhaitait se faire avorter après avoir subi un viol ; *Konovalova c. Russie*, 2014 (§§ 39-50), pour l'accouchement en présence d'étudiants en médecine sans le consentement de la parturiente concernée ; *P.T. c. République de Moldova*, 2020 (§§ 24-33), pour la présence non nécessaire de données médicales sensibles sur une attestation destinée à être produite dans diverses situations ; *Frâncu c. Roumanie*, 2020 (§§ 52), pour le huis clos refusé, dans une affaire de corruption visant un maire, pour l'examen d'une demande de libération pour raison de santé ; *Y.G. c. Russie*, 2022, (§§ 46-53), où le requérant alléguait qu'une base de données renfermant, en particulier, ses données de santé, avait été proposée à la vente sur un marché ; et *A.P. c. Arménie*, 2024, §§ 150-159, où la requérante se plaignait de ce que son nom complet, son adresse et le texte intégral des décisions de justice la déboutant de sa demande de dommages et intérêts pour abus sexuels avaient été publiés sur la base de données judiciaires officielle en ligne accessible au public, alors qu'elle avait spécifiquement demandé à ce que ces éléments d'information ne soient pas publiés.

34. Les informations sur la santé mentale d'un individu constituent des données de nature hautement sensible (*Mockutė c. Lituanie,* 2018, § 94, sur la divulgation des données sur l'état mental d'un patient par un hôpital psychiatrique ; *Malanicheva c. Russie* (déc.), 2016, §§ 13, §§ 15-18, concernant la mémorisation dans le dossier d'un hôpital de données relatives à l'internement d'office des requérants), tout comme les données permettant de conduire à l'identification sexuelle, à l'orientation sexuelle (*Dudgeon c. Royaume-Uni,* 1981, § 41, *J.L. c. Italie*, 2021, § 136, et *Drelon c. France*, 2022, § 79) et à la vie sexuelle d'une personne, telles des données relatives à un avortement transmises d'une autorité publique à une autre sans le consentement de l'intéressée (*M.S. c. Suède*, 1997, §§ 41-42). La législation interne doit ménager des garanties appropriées pour empêcher toute communication ou divulgation de ces données qui ne serait pas conforme aux garanties prévues à l'article 8 (*Z c. Finlande*, 1997, § 95).

vi. Données relatives aux condamnations pénales et aux infractions

35. Des données concernant des infractions, des procédures pénales, des condamnations ou des mesures de sûreté connexes constituent une catégorie de données susceptible d'une protection accrue au regard de l'article 6 de la Convention 108 (*M.M. c. Royaume-Uni*, 2012, § 188 ; *Margari c. Grèce*, 2023, § 59). Il est donc capital que, lorsque des données sensibles sont publiées dans le contexte de procédures pénales pendantes ou d'enquêtes sur des infractions pénales, les données reflètent de manière précise la situation et les faits pour lesquels l'accusé est poursuivi, en tenant compte également de la nécessité de respecter la présomption d'innocence (*ibidem*). Un traitement des données à caractère personnel d'un individu ayant fait l'objet d'une procédure classée sans suite (*Brunet c. France,* 2014, §§ 38-40 ; *N.F. et autres c. Russie*, 2023, § 38), sanctionné par un avertissement (*M.M. c. Royaume-Uni*, 2012, §§ 188-190), condamné pénalement (*Gardel c. France*, 2009, § 58 ; *Peruzzo et Martens c. Allemagne* (déc.), 2013, § 44 ; *Trajkovski et Chipovski c. Macédoine du Nord*, 2020, § 46, *N.F. et autres c. Russie*, 2023, § 38) ou soumis à une mesure de sûreté connexe telle un placement en garde à vue (*Suprunenko c. Russie*, (déc.) [comité], 2018, § 61) emporte une ingérence dans le droit au respect de la vie privée du sujet des données.

36. Pour la Cour, bien que les données figurant dans le casier judiciaire soient, dans un certain sens, des informations publiques, leur mémorisation systématique dans les fichiers centraux signifie

qu'elles peuvent être divulguées bien après l'événement, lorsque tout le monde, hormis la personne concernée, aura vraisemblablement oublié l'incident. Au fil du temps, la condamnation ou l'avertissement deviennent partie intégrante de la vie privée d'un individu, qui doit être respectée (*M.M. c. Royaume-Uni*, 2012, § 188). Cela vaut davantage lorsque ces données concernent le passé lointain d'une personne (*B.B. c. France*, 2009, § 57 ; *Catt c. Royaume-Uni*, 2019, § 93 ; *M.L. et W.W. c. Allemagne*, 2018, §§ 98-100).

37. Une mesure impliquant la conservation, dans les registres de la police, des données d'identification, des empreintes digitales et des photos d'identité d'un individu peut avoir des conséquences graves pour celui-ci, pouvant rendre plus difficile sa vie quotidienne (*Dimitrov-Kazakov c. Bulgarie*, 2011, §§ 8, 10, 13, 30). Dans une affaire relative à l'inscription d'un individu comme « délinquant » dans les registres de la police, après avoir été interrogé au sujet d'un viol et le maintien de cette mention sans qu'aucun acte d'accusation n'ait été établi par la suite, la Cour a conclu à la violation de l'article 8 après avoir constaté que le sujet des données avait fait l'objet, en raison précisément de l'inscription en question, de plusieurs contrôles de police en relation avec des plaintes pour viol ou avec des disparitions de jeunes filles (*ibidem*, §§ 8, 10, 13, 30).

38. En outre, la Cour a jugé que la conservation continue de données relatives à une sanction administrative de substitution (une forme de règlement sans condamnation d'une affaire pénale) ayant été infligée à un requérant s'analysait en une ingérence dans l'exercice par l'intéressé de son droit au respect de sa vie privée garanti par l'article 8 de la Convention (*Borislav Tonchev c. Bulgarie*, 2024, § 125). Selon la jurisprudence de la Cour, la simple conservation par une autorité publique de telles données constitue une ingérence, que les données soient utilisées ultérieurement ou non. La Cour a conclu à la violation de l'article 8 de la Convention au motif que la réglementation bulgare pertinente était suffisamment vague pour semer la confusion parmi les autorités nationales chargées de son interprétation et de son application et que, dès lors, la réglementation n'était pas suffisamment prévisible. En outre, les divergences constatées s'étendaient à l'application du droit de l'UE en matière de protection des données (principe de la limitation de la conservation ; *ibidem*, § 137).

b. Autres catégories de données

39. En dehors des catégories d'informations dites « sensibles », d'autres catégories de données à caractère personnel doivent être également sujette à caution, compte tenu notamment des techniques de plus en plus sophistiquées de surveillance et de la capacité des technologies d'information et de communication de rendre plus difficile au quotidien la vie des sujets des données concernés.

i. Données sur l'emploi

40. La mémorisation de données se rapportant à un individu identifié ou identifiable relatives à sa profession et leur conservation constituent une ingérence dans le droit au respect de la vie privée du sujet des données, protégé par l'article 8 (*Khelili c. Suisse*, 2011, § 56 ; *Sõro c. Estonie*, 2015, §§ 49 et 56 ; *Florindo de Almeida Vasconcelos Gramaxo c. Portugal*, 2022, §§ 95-96). Étant donné que les informations recueillies par les autorités et conservées dans leurs dossiers sont de nos jours soumises à un traitement automatique qui facilite considérablement l'accès à celles-ci et leur diffusion, de telles mesures peuvent avoir des conséquences graves, pouvant nuire à la réputation des individus ou rendre plus difficile leur vie quotidienne. La Cour est parvenue à un constat de violation de l'article 8 dans les affaires *Khelili c. Suisse,* 2011 (§ 64), où la requérante avait été fichée comme « prostituée » par la police, mention ultérieurement corrigée et remplacée par celle de « couturière » dans les fichiers informatiques, et *Sõro c. Estonie*, 2015 (§ 63), où le requérant s'était vu obligé de quitter son travail suite à la divulgation de données sur son emploi en tant que chauffeur dans les anciens services de sécurité. Dans l'arrêt *Florindo de Almeida Vasconcelos Gramaxo c. Portugal*, 2022 (§§ 95-96), où l'employeur du requérant avait installé un système GPS

dans le véhicule de fonction de l'intéressé dans le but de contrôler les distances que celui-ci parcourait dans l'exercice de son activité professionnelle et, le cas échéant, lors de ses déplacements privés, la Cour a considéré que les informations ainsi recueillies constituaient des données à caractère personnel. Elle a également noté que les employés n'étaient pas autorisés à désactiver le système GPS, de sorte que celui-ci restait actif 24 heures sur 24 et 7 jours sur 7, et que la surveillance était donc permanente et systématique, empiétant ainsi incontestablement sur la vie privée du requérant[1].

ii. Données financières

41. Des informations obtenues à partir des documents bancaires d'un individu constituent des données à caractère personnel, qu'il s'agisse de renseignements sensibles de nature privée ou des informations sur les activités professionnelles du sujet des données (*M.N. et autres c. Saint-Marin,* 2015, § 51 ; *G.S.B. c. Suisse*, 2015, § 51). Le fait, pour autorités, de copier des informations bancaires puis de les conserver s'analyse en une ingérence dans l'exercice, par le sujet des données, de son droit au respect de sa vie privée et de sa correspondance (*M.N. et autres c. Saint-Marin*, 2015, § 55).

42. La Cour a examiné la question de la collecte, du traitement et de la divulgation des données financières dans le contexte : d'une enquête pénale (*M.N. et autres c. Saint-Marin*, 2015, §§ 7-9, §§ 53-55) ; de la publication à grande échelle, par la presse, de données financières aux fins de permettre la tenue d'un débat sur des questions d'intérêt général (*Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande* [GC], 2017, §§ 172-173) ; de l'obligation imposée à un avocat de révéler des données soumises au secret professionnel en déclarant ses soupçons relatifs aux activités illicites de blanchiment d'argent de ses clients (*Michaud c. France,* 2012, §§ 91-92) ; de la transmission de données financières aux autorités d'un autre État qui n'est pas partie à la Convention (*G.S.B. c. Suisse*, 2015, § 50) ; du rejet d'une action concernant la divulgation d'informations sur le numéro de contribuable et la déclaration de revenus de la requérante dans un reportage télévisé consacré à une affaire pénale visant son époux (*Samoylova c. Russie*, 2021, §§ 83 et 90-93) ; de la consultation illicite et l'utilisation impropre de données conservées dans la base de données du Service d'information sur les contribuables (*Casarini c. Italie* (déc.), 2024, §§ 56-57).

43. L'existence d'un intérêt général à ce que de grandes quantités de données fiscales soient accessibles et à ce que la collecte de ces données soit autorisée ne signifie pas nécessairement ou automatiquement qu'il existe également un intérêt général à diffuser en masse pareilles données brutes, telles quelles, sans aucun apport analytique (*Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande* [GC], 2017, §§ 172-178, 198).

44. Même si, en matière fiscale, la marge d'appréciation de l'État est plus ample lorsqu'il s'agit de la protection des données purement financières qui ne comportent pas de données intimes ou liées étroitement à l'identité du sujet des données (*G.S.B. c. Suisse*, 2015, § 93), les considérations liées à la vie privée entrent en jeu dans les situations où des données de nature fiscale ont été recueillies sur une personne bien précise, ou lorsqu'elles ont été rendues publiques d'une manière ou dans une mesure excédant ce à quoi les intéressés pouvaient raisonnablement s'attendre (*M.N. et autres c. Saint-Marin*, 2015, §§ 52-53 ; *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande* [GC], 2017, § 136).

iii. Données de trafic

45. Des données de trafic sont des informations recueillies auprès des opérateurs téléphoniques ne touchant pas au contenu des communications, et qui comprennent la date, l'horaire, la durée de chaque communication, ainsi que le ou les destinataires de la communication (*Malone*

[1] Voir aussi la section intitulée « Données de localisation GPS » ci-dessous.

c. Royaume-Uni, 1984, §§ 83-84 ; *Copland c. Royaume-Uni*, 2007, § 43). Le placement sous « comptage » (*metering*) du téléphone d'un individu dans le cadre d'une enquête pénale à travers l'emploi d'un mécanisme (un compteur combiné avec une imprimante) qui enregistre les numéros formés sur un appareil de téléphone donné, ainsi que l'heure et la durée de chaque appel, sans surveiller ni intercepter les communications, constitue une ingérence dans la vie privée de l'individu concerné (*Malone c. Royaume-Uni*, 1984, §§ 83-84). L'exploitation des éléments rassemblés de la sorte, notamment des numéros composés, peut poser problème au regard de l'article 8, ces éléments faisant partie intégrante des communications téléphoniques (*Malone c. Royaume-Uni*, 1984, § 84 ; *Copland c. Royaume-Uni*, 2007, § 43). Aux yeux de la Cour, les révéler à la police sans l'accord de l'abonné peut porter atteinte à un droit garanti par l'article 8 (*Malone c. Royaume-Uni*, 1984, § 84).

46. Le « comptage » des communications, qui en soi ne porte pas atteinte à l'article 8 s'il est effectué par exemple par une compagnie de téléphone à des fins de facturation, se distingue par nature de l'interception des communications (*Malone c. Royaume-Uni*, 1984, §§ 83-84 ; *P.G. et J.H. c. Royaume-Uni*, 2001, § 42). Une réquisition judiciaire adressée à un opérateur de téléphonie de recueillir les appels reçus et émis par différentes lignes de téléphones portables d'un individu et de procéder à un « bornage » de ses lignes téléphoniques permettant de suivre *a posteriori* ses déplacements n'était pas nécessairement incompatible avec l'article 8 dans la mesure où elle était autorisée par une loi qui prévoyait suffisamment de garanties contre l'arbitraire (*Ben Faiza c. France*, 2018, §§ 56, 59, 69). La Cour est parvenue à un constat de non-violation de l'article 8 dans une affaire où de telles réquisitions étaient soumises à l'autorisation préalable d'un magistrat du parquet sous peine de nullité, étaient susceptibles d'un contrôle juridictionnel et les éléments obtenus pouvaient être exclus en cas d'illégalité (*ibidem*, §§ 79, 73).

47. Des données personnelles d'utilisateurs de cartes SIM prépayées, tels que les noms, les adresses, les numéros de téléphone des clients recueillies par les opérateurs de téléphonie mobile ne doivent pas être considérées comme « insignifiantes » (*Breyer c. Allemagne*, 2020, §§ 92-95). La simple conservation, par les opérateurs de communication, de telles données des clients constitue une ingérence dans le droit au respect de la vie privée du sujet des données, indépendamment de leur éventuelle utilisation ultérieure (*ibidem*, § 92). Une telle ingérence est toutefois de nature relativement limitée (*ibidem*, § 95) et les États membres du Conseil de l'Europe jouissent d'une certaine marge d'appréciation en la matière compte tenu de l'absence de consensus européen (*ibidem*, § 90). L'existence d'une supervision par une autorité indépendante, compétente pour examiner, lorsqu'elle perçoit des raisons de le faire, s'il est acceptable de transmettre les données concernées aux autorités qui en font la demande, et la disponibilité d'un recours auprès d'une autorité administrative ouvert à toute personne pensant avoir fait l'objet d'une procédure d'extraction ou d'une demande d'information, ont pour conséquence que l'absence de notification concernant une procédure d'extraction n'est pas incompatible avec l'article 8 (*ibidem*, §§ 103-107).

48. Dans le cas d'une connexion à Internet, les données de trafic sont des données permettant d'identifier l'utilisateur, par exemple son adresse IP, son adresse courriel, le ou les destinataires de la communication, des données relatives aux équipements terminaux de communication utilisés, aux services complémentaires demandés ou utilisés et leurs fournisseurs (*Benedik c. Slovénie*, 2018, § 96). Aux yeux de la Cour, les informations sur un abonné associées à une adresse IP dynamique spécifique attribuée à un moment donné sont des données personnelles. Elles ne sont pas accessibles au public et ne peuvent donc pas être comparées aux informations que l'on trouve dans un annuaire téléphonique classique ou dans une base de données publique comportant les numéros d'immatriculation des véhicules (*ibidem*, § 108).

49. L'acquisition des données de communication associées dans le cadre d'une interception en masse n'est pas nécessairement moins intrusive que l'acquisition du contenu des communications (*Centrum för rättvisa c. Suède* [GC], 2021, 277, et *Big Brother Watch et autres c. Royaume-Uni* [GC], 2021, § 363). L'interception et la conservation des données de communication associées, ainsi que

les recherches effectuées sur celles-ci, doivent donc être analysées au regard des mêmes garanties que celles applicables au contenu des communications. Cela étant, compte tenu de la nature différente des données de communication associées et des différentes façons dont elles sont utilisées par les services de renseignement, 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 (*Centrum för rättvisa c. Suède* [GC], 2021, § 278 ; et *Big Brother Watch et autres c. Royaume-Uni* [GC], 2021, § 364).

50. La prépondérance octroyée à l'exigence de confidentialité des données de trafic peut, dans certaines circonstances, s'avérer contraire à l'article 8 si elle est de nature à entraver l'efficacité d'une enquête pénale permettant d'identifier et de sanctionner l'auteur d'une infraction commis par voie d'Internet (*K.U. c. Finlande,* 2008, § 49). La garantie des utilisateurs des télécommunications et des services Internet que leur intimité sera respectée doit parfois s'effacer devant d'autres impératifs légitimes, tels que la défense de l'ordre et la prévention des infractions pénales ou la protection des droits et libertés d'autrui (*ibidem*, § 49).

iv. Échantillons vocaux

51. L'opération de « sonorisation » vise l'interception des propos d'un individu par le biais d'un dispositif de surveillance audio dissimulé dans un local privé (*Vetter c. France*, 2005, §§ 10, 20) ou public (*P.G. et J.H. c. Royaume-Uni*, 2001, §§ 38, 63 ; *Allan c. Royaume-Uni*, 2002, § 35 ; *Doerga c. Pays-Bas*, 2004, § 43 ; *Wisse c. France*, 2005, § 29).

52. L'enregistrement en secret de la voix d'un individu sur un support permanent aux fins d'un processus d'analyse directement destiné à identifier cet individu à la lumière d'autres données personnelles constitue un traitement de données personnelles révélant une ingérence dans le droit du sujet des données au respect de sa vie privée (*P.G. et J.H. c. Royaume-Uni*, 2001, §§ 59-60). En l'absence d'un cadre législatif qui régisse l'emploi d'appareils d'écoute dissimulés par la police dans ses propres locaux ou dans un lieu privé, la Cour est parvenue à un constat de violation de l'article 8 (*ibidem*, §§ 38, 63).

53. L'écoute des conversations par le biais de la pose de micros représente, à l'instar de l'interception des entretiens téléphoniques, une atteinte grave au respect de la vie privée du sujet des données (*Vetter c. France*, 2005, § 26). Elle doit donc se fonder sur une « loi » d'une précision particulière : dans ce domaine aussi, l'existence de règles claires et détaillées apparaît indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner (*ibidem*, § 26). Selon la Cour, la « loi » doit offrir aux justiciables « des sauvegardes adéquates » contre les abus à redouter de même nature qu'en matière d'écoutes téléphoniques (*ibidem*, § 26). Ainsi, notamment, les catégories de personnes susceptibles de faire l'objet d'une telle mesure et la nature des infractions pouvant y donner lieu doivent être définies ; le juge doit être astreint à fixer une limite à la durée de l'exécution de la mesure ; et doivent également être précisées les conditions d'établissement des procès-verbaux de synthèse consignant les conversations « écoutées », les précautions à prendre pour communiquer intacts et complets les enregistrements réalisés, aux fins de contrôle éventuel par le juge et par la défense, ainsi que les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction desdites bandes, notamment après un non-lieu ou une relaxe (*ibidem*, § 26 faisant référence aux critères en matière de l'interception de communications indiquées dans l'arrêt *Kruslin c. France*, 1990, § 35).

54. Lorsque l'enregistrement de la voix d'un individu a été effectuée sans respecter le degré minimal de protection voulu par la prééminence du droit dans une société démocratique, il emporte une violation de l'article 8 (*Wisse c. France,* 2005, § 34 sur l'enregistrement et l'utilisation subséquente des conversations tenues au parloir d'une prison par les requérants avec leurs proches ; *Allan c. Royaume-Uni*, 2002, § 36, sur la mise en place d'un dispositif de surveillance audio placé dans la cellule d'un détenu en prison).

v. Données de localisation GPS

55. Les données recueillies par le GPS peuvent indiquer l'endroit où se trouvait un individu et les déplacements de celui-ci en public et sont des données personnelles (*Uzun c. Allemagne*, 2010, §§ 51-52, *Florindo de Almeida Vasconcelos Gramaxo c. Portugal*, 2022, § 95). Le traitement et l'utilisation de telles données s'analysent en une ingérence dans l'exercice du droit au respect de la vie privée du sujet des données (*Uzun c. Allemagne*, 2010, §§ 51-52 ; *Florindo de Almeida Vasconcelos Gramaxo c. Portugal*, 2022, § 96). Il y a lieu de distinguer la surveillance par GPS d'autres méthodes de surveillance par des moyens visuels ou acoustiques qui, en règle générale, sont davantage susceptibles de porter atteinte au droit d'une personne au respect de sa vie privée car elles révèlent plus d'informations sur la conduite, les opinions ou les sentiments de l'individu qui en fait l'objet (*Uzun c. Allemagne*, 2010, § 52).

56. S'agissant d'une ingérence moins importante dans la vie privée du sujet des données par rapport à l'interception des conversations téléphoniques, les critères relativement stricts établis et suivis dans le contexte spécifique de la surveillance des télécommunications ne sont pas applicables en tant que tels à la surveillance par GPS des déplacements d'un individu (*ibidem*, § 66). Pour examiner si, dans une affaire donnée, un individu frappé d'une mesure de géolocalisation par GPS a bénéficié d'une protection adéquate contre une ingérence arbitraire dans l'exercice de ses droits protégés par l'article 8, la Cour doit suivre des principes plus généraux quand elle examine la question de la prévisibilité de la loi (*ibidem*, § 66 et les références citées au § 63). La délivrance d'un mandat par un organe indépendant n'est pas toujours nécessaire et un contrôle judiciaire ultérieur de la surveillance d'une personne par GPS est de nature à offrir une protection suffisante contre l'arbitraire (*ibidem*, § 72).

57. La mise en place d'un dispositif de géolocalisation sur le véhicule d'un individu dans le cadre d'une enquête pénale portant sur un trafic de stupéfiants a été jugée par la Cour contraire à l'article 8 dans une affaire où le droit interne, écrit et non écrit, n'indiquait pas avec assez de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités en la matière (*Ben Faiza c. France*, 2018, §§ 58-61).

58. En revanche, dans une autre affaire où la Cour a eu à examiner la question des données personnelles d'un individu recueillies par le biais de la géolocalisation et l'utilisation des données ainsi obtenues dans le cadre de la procédure pénale dirigée contre lui, elle a conclu à la non-violation de l'article 8 (*Uzun c. Allemagne*, 2010, §§ 60-74). L'existence d'un contrôle judiciaire ultérieur de la surveillance par GPS ainsi que la possibilité d'exclure les éléments de preuve obtenus au moyen d'une surveillance illégale ont constitué des garanties importantes, capables de décourager les autorités d'enquête de recueillir des preuves par des moyens illégaux (*ibidem*, § 72). Le fait que le droit interne subordonnait l'autorisation de la mesure de surveillance litigieuse à des conditions très strictes, que la surveillance par GPS avait seulement été ordonnée après que d'autres mesures d'investigation, moins attentatoires à la vie privée, s'étaient révélées inefficaces, et que cette mesure avait été mise en œuvre pendant une période relativement courte, ont aussi été pris en compte dans le cadre de l'examen de la proportionnalité de l'ingérence (*ibidem*, §§ 77-81).

59. Dans l'arrêt *Florindo de Almeida Vasconcelos Gramaxo c. Portugal*, 2022 (§§ 95-96 et §§ 105-125) l'employeur du requérant avait installé un système GPS dans le véhicule de fonction de l'intéressé dans le but de contrôler les distances que celui-ci parcourait dans l'exercice de son activité professionnelle et, le cas échéant, lors de ses déplacements privés. La Cour a observé que le système en cause permettait de suivre en temps réel les déplacements d'un véhicule : il était ainsi possible de localiser géographiquement la ou les personnes qui étaient supposées s'en servir à un instant donné ou en continu. La Cour a considéré que ces informations constituaient des données à caractère personnel. Elle a également noté que les employés n'étaient pas autorisés à désactiver le système GPS, de sorte qu'il restait actif 24 heures sur 24 et 7 jours sur 7, et que la surveillance était donc permanente et systématique, empiétant ainsi incontestablement sur la vie privée de

l'intéressé. Dans le même temps, elle a considéré que les juridictions internes avaient correctement mis en balance les intérêts concurrents en jeu, c'est-à-dire, d'un côté, le droit du requérant au respect de sa vie privée et, de l'autre, le droit de l'employeur au bon fonctionnement de son entreprise, en tenant compte du but légitime poursuivi par l'entreprise, à savoir le droit de contrôler ses dépenses. Elle a donc conclu à la non-violation de l'article 8 de la Convention.

vi. Photos

60. Le droit d'un individu à la protection de son image constitue l'une des composantes essentielles de son épanouissement personnel et présuppose principalement la maîtrise par l'individu de son image (*Reklos et Davourlis c. Grèce*, 2009, §§ 40-43 ; *Margari c. Grèce*, 2023, § 28 ; *Glukhin c. Russie*, 2023, § 66). Lorsqu'un individu ne s'est pas exposé sciemment ou accidentellement à l'objectif d'un photographe dans le cadre d'une activité susceptible d'être enregistrée ou rapportée publiquement, la protection effective de son image présuppose, en principe, le consentement de l'individu dès sa captation, et non pas seulement au moment de son éventuelle diffusion au public (*Reklos et Davourlis c. Grèce*, 2009, §§ 37, 40). Ce principe n'est toutefois pas absolu. La qualité de personne publique ou de personne jouissant d'une certaine notoriété peuvent justifier, dans certaines circonstances, à des fins d'intérêt général, la captation de l'image d'un individu sans son consentement et sa diffusion à son insu[2].

61. Dans le cas de personnes arrêtées ou poursuivies, l'utilité objective de photos prises par les autorités suite à l'arrestation d'un individu soupçonné d'avoir commis une infraction peut rendre nécessaire dans une société démocratique la conservation de telles données à des fins de lutte contre la criminalité (*Suprunenko c. Russie* (déc.) [comité], 2018, §§ 63-65). Le fait qu'une photo soit prise d'un individu soupçonné d'avoir commis une infraction et qu'elle soit conservée dans la base de données n'entraîne pas nécessairement un stigmate de suspicion ou de culpabilité à son égard (*ibidem*, § 64). Dans l'affaire *Murray c. Royaume-Uni* [GC], 1994 (§§ 92-93), la prise et la conservation d'une photographie d'une personne soupçonnée de terrorisme sans son accord n'était pas une mesure disproportionnée au but poursuivi de prévention du terrorisme, légitime dans une société démocratique. En consignant et en conservant de telles données personnelles de base sur la personne arrêtée, ou même sur d'autres personnes présentes aux temps et lieu de l'arrestation, les autorités compétentes ne franchissaient pas les limites légitimes de la procédure de poursuite des infractions terroristes (*ibidem*, § 93). La Cour a également déclaré manifestement mal fondée une requête relative à la conservation dans le système d'information du ministère de l'Intérieur d'une photo du requérant, soupçonné d'avoir commis une infraction, prise par les autorités lors de son appréhension par la police (*Suprunenko c. Russie* (déc.) [comité], 2018, § 65). À ses yeux, bien que les informations ainsi recueillies et conservées sur l'ordinateur de la police aient été de nature personnelle, elles ne sauraient être considérées comme intimes ou sensibles (*ibidem*, § 64).

62. La Cour a conclu en revanche à une violation de l'article 8 dans des cas où des services de police avaient donné à la presse des photographies de personnes arrêtées ou poursuivies sans leur accord (*Sciacca c. Italie*, 2005, §§ 29-31 ; *Khoujine et autres c. Russie*, 2008, §§ 115-118 ; *Margari c. Grèce*, 2023, §§54-60) ou avaient invité des équipes de télévision à filmer illégalement le requérant au poste de police et à diffuser ces images à la télévision (*Toma c. Roumanie*, 2009, §§ 90-93 ; *Khmel c. Russie*, 2013, § 41), dans un cas où le ministère de l'Intérieur avait publié sur son site Internet des photographies des requérantes qui avaient été prises lors de leur garde à vue et sur lesquelles l'identité des intéressées n'avait pas été dissimulée (*D.H. et autres c. Macédoine du Nord*, 2023, §§ 63-65), dans un cas où l'affichage d'une photographie du requérant sur le panneau des personnes

[2] Voir aussi le *Guide sur l'article 10 de la Convention - liberté d'expression* sur la publication de photos à des fins journalistiques.

recherchées n'était pas prévu par la loi (*Guiorgui Nikolaïchvili c. Géorgie*, 2009, §§ 129-131), et dans un cas où les règles et procédures en place ne respectaient pas l'exigence de « qualité de la loi » (*Negru c. République de Moldova*, 2023, §§ 29-35).

63. Pour la Cour, la conservation, sans limitation de durée, de la photographie d'un individu soupçonné d'avoir commis des infractions, mais qui n'a pas été reconnu coupable, comporte un risque de stigmatisation plus élevé que la conservation des données appartenant aux individus reconnus coupables d'une infraction (*S. et Marper c. Royaume-Uni* [GC], 2008, § 122 ; *Gaughran c. Royaume-Uni*, 2020, §§ 82-84). L'élément déterminant lorsqu'il s'agit de rechercher si un État a outrepassé sa marge d'appréciation lorsqu'il décide de conserver de telles données personnelles n'est pas nécessairement la durée de conservation des données, mais le fait de savoir si des garanties effectives ont été mises en place (*ibidem*, § 88).

64. La technologie de reconnaissance faciale et de cartographie faciale susceptible d'être appliquées de nos jours à la photographie d'un individu est de plus en plus complexe et les juridictions internes doivent en tenir compte dans l'examen de la nécessité de l'ingérence dans le droit au respect de la vie privée de l'individu dont l'image a été captée par les autorités (*ibidem*, §§ 67-70 ; voir aussi, sur l'utilisation par la police d'une technologie de reconnaissance faciale dans le but d'identifier le requérant à partir de photographies publiées sur une chaîne Telegram publique, *Glukhin c. Russie*, 2023, §§ 64-91).

65. Dans l'affaire *Gaughran c. Royaume-Uni*, 2020 (§§ 97-98), où les autorités avaient décidé de conserver sans limitation de durée la photographie d'un individu reconnu coupable de conduite en état d'ivresse, en plus de son profil ADN et de ses empreintes digitales, la Cour a conclu à la violation de l'article 8, considérant que la conservation des données personnelles du requérant, mesure prise sans tenir compte de la gravité de l'infraction commise et sans lui offrir une réelle possibilité de réexamen, ne traduisait pas un juste équilibre entre les intérêts publics et privés concurrents. Même si l'État conserve une marge d'appréciation légèrement plus large en ce qui concerne la conservation des photographies des personnes condamnées par rapport à la conservation de leurs profils ADN (*ibidem*, §§ 84, 96), cette marge élargie ne suffit pas pour rendre la conservation de ces données proportionnée dans toutes circonstances, notamment en l'absence de garanties pertinentes, y compris l'absence de véritable examen par les juridictions nationales (*ibidem*, § 96).

66. Dans l'affaire *P.N. c. Allemagne*, 2020 (§§ 76-91), la Cour a conclu à la non-violation de l'article 8 s'agissant d'une collecte ordonnée par la police, à la suite de l'ouverture d'une nouvelle procédure pénale à l'encontre d'un individu préalablement condamné, d'éléments destinés à l'identifier, tels que des photographies de son visage et de son corps, notamment d'éventuels tatouages, ainsi que des empreintes digitales et palmaires. Au vu du degré relativement limité de l'intrusion et de la durée du recueil des données d'identification en question, de l'effet limité sur la vie quotidienne du requérant de la conservation des données, limitée à cinq ans, dans une base de données interne de la police subordonnée à des garanties et à un contrôle individualisé, la mesure litigieuse constituait une ingérence proportionnée dans le droit du requérant au respect de sa vie privée.

67. Dans des contextes différents, la Cour a conclu à la violation de l'article 8 dans l'affaire *Reklos et Davourlis c. Grèce*, 2009 (§§ 41-43), au motif que la prise de photos d'un nouveau-né dans une clinique et leur conservation par le photographe sous une forme identifiante, pouvant faire l'objet d'une exploitation ultérieure, avait eu lieu contrairement à la volonté des parents, ainsi que dans les affaires *Hájovský c. Slovaquie*, 2021 (§§ 46-49), s'agissant de la publication dans la presse d'images non floutées du requérant, prises à son insu et au moyen d'un stratagème, et *Volodina c. Russie (n° 2)*, 2021, § 68, qui concernait la défaillance des autorités de protéger une femme contre la cyberviolence répétée de son compagnon qui avait créé de faux profils à son nom et publié ses photos intimes.

68. Dans l'affaire *Vučina c. Croatie* (déc.), 2019 (§§ 34-51), le simple fait qu'un autre nom que celui de la requérante, un nom qui n'était porteur d'aucune connotation négative, ait été indiqué par

erreur dans la légende d'une photographie publiée dans un magazine féminin ne saurait être considéré comme une atteinte particulièrement substantielle au droit au respect de la vie privée du sujet des données.

69. Dans l'affaire *Von Hannover c. Allemagne (n° 2)* [GC], 2012 (§§ 114-126), le refus des juridictions internes d'interdire la publication d'une photographie d'un couple célèbre prise à leur insu n'a pas constitué une violation de l'article 8 étant donné que les juridictions nationales ont procédé à une mise en balance circonstanciée du droit des sociétés d'édition à la liberté d'expression avec le droit des requérants au respect de leur vie privée. Ce faisant, elles ont attaché une importance primordiale à la question de savoir si les photos, considérées à la lumière des articles les accompagnant, avaient apporté une contribution à un débat d'intérêt général. Elles se sont en outre penchées sur les circonstances dans lesquelles les photos avaient été prises.

70. Dans l'affaire *Kahn c. Allemagne*, 2016 (§§ 63-76), la Cour a conclu à la non-violation de l'article 8 au sujet de l'absence de condamnation d'un éditeur au paiement d'une somme pour avoir enfreint une interdiction de publier des photographies de deux enfants d'un ancien gardien de but de l'équipe nationale de football allemande. La Cour a spécifié qu'on ne saurait tirer de l'article 8 le principe que, pour protéger la vie privée d'une personne de manière effective, la condamnation d'un éditeur au paiement d'une somme pour avoir enfreint une interdiction de publier ne saurait être suffisante que si cette somme revient à la victime, si tant est que l'État, dans l'exercice de sa marge d'appréciation, met à la disposition des personnes lésées d'autres moyens qui peuvent se révéler effectifs et dont on ne saurait dire qu'ils limitent la possibilité d'obtenir le redressement des violations alléguées de manière disproportionnée (*ibidem*, § 75).

B. Les deux aspects (négatif et positif) de la protection des données

71. L'article 8, qui assure, de façon principale, la protection de données à caractère personnel, impose essentiellement aux États une obligation de s'abstenir de toute ingérence arbitraire dans l'exercice du droit au respect « de la vie privée et familiale, du domicile et de la correspondance » d'un individu, qu'elle soit l'œuvre des pouvoirs publics eux-mêmes ou des organismes privés auxquels l'État aurait préalablement délégué ses responsabilités. À cette exigence plutôt négative peuvent s'ajouter des obligations positives inhérentes à un respect effectif des droits garantis par la Convention (*Bărbulescu c. Roumanie* [GC], 2017, § 108).

72. Lorsqu'une mesure portant atteinte à la protection de données à caractère personnel d'un individu émane d'un individu ou d'une entité relevant strictement du secteur privé, la Cour examine l'affaire sous l'angle des obligations positives de l'État (*Craxi c. Italie (n° 2)*, 2003, §§ 68-76 ; *Köpke c. Allemagne* (déc.), 2010 ; *Alkaya c. Turquie*, 2012, § 32 ; *Söderman c. Suède* [GC], 2013, § 89 ; Bărbulescu c. Roumanie [GC], 2017, § 111 ; *López Ribalda et autres c. Espagne* [GC], 2019, § 111 ; *Buturugă c. Roumanie*, 2020, §§ 60-63 ; *Volodina c. Russie (n° 2)*, 2021, §§ 58-68 ; *Florindo de Almeida Vasconcelos Gramaxo c. Portugal*, 2022, § 111 ; *Tena Arregui c. Espagne*, 2024, § 35). Lorsqu'une telle mesure émane, en revanche, d'une entité relevant du secteur public (*Copland c. Royaume-Uni*, 2007, § 39 ; *Libert c. France,* 2018, § 41 ; *Drelon c. France*, 2022, § 85 ; *Cherrier c. France*, 2024, § 57), d'un organisme privé auquel un organisme public avait préalablement délégué ses obligations (*Vukota-Bojić c. Suisse*, 2016, § 47) ou d'un organisme privé agissant conformément à une obligation légale (*Podchasov c. Russie*, 2024, § 52) la Cour examine l'affaire sous l'angle de l'obligation négative de l'État. La Cour doit alors vérifier si l'ingérence était conforme aux exigences de l'article 8 § 2, à savoir si elle était prévue par la loi, si elle poursuivait un but légitime et si elle était nécessaire dans une société démocratique. Cette question sera analysée de manière plus détaillée dans la partie ci-dessous du présent guide sur Les trois « tests » en matière de protection des données.

73. Dans l'affaire *Vukota-Bojić c. Suisse*, 2016 (§ 47), la Cour a souligné qu'un État ne pouvait pas se soustraire à sa responsabilité découlant de la Convention en déléguant ses obligations à des organismes privés ou à des particuliers. Puisque la compagnie d'assurance privée, qui avaient mené la collecte et la mémorisation des données personnelles, mettait en œuvre le régime d'assurance public et était réputée être une autorité publique en droit interne, il y avait lieu de la considérer comme telle et d'imputer ses actes à l'État défendeur (*ibidem,* § 47).

74. Dans l'affaire *Libert c. France,* 2018 (§§ 37-41), la Cour a écarté l'objection du Gouvernement selon laquelle la Société nationale des chemins de fer (SNCF), l'employeur du requérant mis en cause pour l'ouverture des fichiers personnels stockés sur un ordinateur professionnel, ne pouvait être regardée comme une « autorité publique » aux fins de l'article 8. Bien que son personnel soit avec elle dans une relation de droit privé, une telle société est une personne morale de droit public, placée sous la tutelle de l'État et dont la direction est nommée par lui, bénéficiant d'une garantie implicite de l'État.

75. S'agissant de la surveillance des appels téléphoniques, du courrier électronique et des connexions Internet d'une employée d'un collège, la Cour a considéré que la question soulevée se rapportait à l'obligation négative incombant à l'État de ne pas violer la vie privée et la correspondance de l'intéressée puisque le collège était un organisme public d'enseignement supérieur dont les actes engageaient la responsabilité de l'État au regard de la Convention (*Copland c. Royaume-Uni*, 2007, § 39).

76. Dans l'affaire *Liebscher c. Autriche*, 2021, le requérant se plaignait de l'obligation qui lui était faite de présenter l'intégralité de son accord de divorce (et non simplement un extrait) pour obtenir le transfert à son ex-femme de sa partie du patrimoine immobilier du couple. L'accord de divorce indiquait le nom et le lieu de résidence des enfants mineurs du couple et de l'ex-femme du requérant, le montant de la pension alimentaire et les modalités de la garde des enfants, la répartition des biens (meubles) du couple et une liste des revenus et avoirs du requérant. Le transfert de propriété des biens immobiliers, et dès lors tous les documents afférents, y compris l'accord de divorce, devaient être inscrits dans un registre foncier public et donc consultable sans restriction par n'importe qui. La Cour a abordé l'affaire du point de vue de l'obligation positive pour l'État d'adopter des mesures visant à assurer le respect de la vie privée, notamment en mettant en place un cadre réglementaire et en appliquant, le cas échéant, des mesures spécifiques (*ibidem*, §§ 60-61).

77. Si la frontière entre les obligations positives et les obligations négatives de l'État au regard de la Convention ne se prête pas à une définition précise, les principes applicables sont néanmoins comparables. Dans les deux hypothèses, un juste équilibre doit être ménagé entre l'intérêt général et les intérêts de l'individu, l'État jouissant en toute hypothèse d'une marge d'appréciation (*Bărbulescu c. Roumanie* [GC], 2017, § 112 ; *Tena Arregui c. Espagne*, 2024, § 32).

78. Dans les affaires qui soulèvent la question de la protection des données à caractère personnel, la Cour a jugé que la marge d'appréciation des autorités était plus large : lorsqu'il n'y a pas de consensus au sein des États membres du Conseil de l'Europe sur l'importance relative à l'intérêt en jeu ou sur les meilleurs moyens de le protéger (*Odièvre c. France* [GC], 2003, § 47 ; *Breyer c. Allemagne*, 2020, § 108 ; *Gauvin-Fournis et Silliau c. France*, 2023, § 111) ; lorsque les données en jeu, purement financières, ne sont pas étroitement liées à l'identité d'un requérant (*G.S.B. c. Suisse*, 2015, § 93) ; et, enfin, en matière de sécurité nationale (*Leander c. Suède*, 1987, § 59). En revanche, la marge d'appréciation réservée aux autorités nationales a été jugée plus restreinte lorsqu'il s'agissait, par exemple, de données à caractère personnel soumises à un traitement automatique facilitant considérablement leur accès et leur diffusion, et pouvant nuire à la réputation d'une personne et rendre plus difficile sa vie quotidienne (*Khelili c. Suisse*, 2011, §§ 64, 70). Il en a été de même dans le cas de la protection de catégories sensibles de données, notamment des données

ADN qui reflètent le patrimoine génétique d'un individu et revêtent une importance considérable tant pour lui-même que pour sa famille (*S. et Marper c. Royaume-Uni* [GC], 2008, §§ 102-103).

79. Les obligations positives inhérentes pour assurer la protection effective des droits et libertés garantis par la Convention peuvent impliquer, par exemple, l'obligation d'offrir à un individu : un accès dans un délai raisonnable aux informations mémorisés de façon systématique sur lui par les anciens services secrets de l'État, concernant son passé lointain (*Haralambie c. Roumanie*, 2009, § 79 ; *Jarnea c. Roumanie*, 2011, § 50 ; *Joanna Szulc c. Pologne*, 2012, § 87) ; une « procédure effective et accessible » qui lui permette d'avoir accès à « l'ensemble des informations pertinentes et appropriées » recueillies et mémorisées par les pouvoirs public pour connaître et comprendre son enfance et ses années de formation (*Gaskin c. Royaume-Uni*, 1989, § 49), pour retracer son identité personnelle (*Odièvre c. France* [GC], 2003, § 42 ; *Gauvin-Fournis et Silliau c. France*, 2023, § 110), ou pour identifier les risques pour la santé auxquels il avait été exposés (*Guerra et autres c. Italie,* 1998, § 60 ; *McGinley et Egan c. Royaume-Uni*, 1998, § 101 ; *Roche c. Royaume-Uni* [GC], 2005, § 162).

80. La Cour a estimé, en revanche, que des telles obligations positives ne pesaient pas sur les autorités nationales dans le contexte des renseignements sensibles pour la sécurité nationale recueillis sur un individu par les autorités (*Leander c. Suède*, 1987, § 51).

81. Aussi, dans l'affaire *Kotilainen et autres c. Finlande*, 2020 (§ 83), relative à une fusillade qui s'était déroulée dans un établissement scolaire, la Cour a estimé que l'obligation positive des autorités de protéger la vie des proches des requérants ne s'étendait pas, sous le volet matériel de l'article 2, à une obligation, pour la police, d'obtenir, avant que la fusillade ne se produise, les dossiers médicaux et militaires de son auteur pour vérifier les données relatives à sa santé mentale. Pour la Cour, l'accès par la police aux données médicales d'un individu ne peut pas être une question de routine et doit rester soumis à des exigences spécifiques de nécessité et de justification.

82. Dans certaines circonstances où la question des données à caractère personnel entre en jeu, s'agissant notamment d'actes interindividuels particulièrement graves, une jouissance effective des droits garantis par la Convention exige de l'État qu'il adopte un cadre législatif propre à protéger le droit en cause. Ainsi, dans l'affaire *Söderman c. Suède* [GC], 2013 (§§ 86-117), la Cour a conclu à la violation de l'article 8 compte tenu de l'absence de dispositions légales claires, incriminant l'acte isolé consistant à filmer ou photographier une enfant nue à son insu, lacunes qui n'étaient pas comblées par d'autres dispositions pénales à l'époque des faits, et au regard de l'inefficacité des recours de caractère civil (*ibidem*, §§ 108-114). De même, dans l'affaire *K.U. c. Finlande*, 2008 (§§ 49-50), l'absence d'une base légale permettant aux autorités de contraindre le fournisseur d'accès Internet à divulguer l'identité d'une personne recherchée pour avoir placé un message indécent concernant un mineur sur un site de rencontres et de concilier ainsi les différents intérêts à protéger dans ce contexte a emporté un constat de violation de l'article 8. L'affaire *Khadija Ismayilova c. Azerbaïdjan*, 2019 (§§ 105-132), portait quant à elle sur l'enregistrement vidéo secret d'une journaliste à son domicile et sur la diffusion de ces vidéos au public. En l'espèce, les actes litigieux étaient réprimés par le droit pénal et une enquête pénale avait effectivement été ouverte. La Cour a toutefois jugé que les autorités n'avaient pas honoré l'obligation positive qui leur incombait d'assurer la protection adéquate de la vie privée de la requérante en menant une enquête pénale effective sur les ingérences très graves dans la vie privée de celle-ci (*ibidem*, §§ 119-131). L'affaire *Volodina c. Russie (no 2)*, 2021, § 68, concernait la défaillance, reprochée par la requérante aux autorités, de la protéger contre la cyberviolence répétée de son compagnon qui avait créé de faux profils à son nom, publié ses photos intimes, suivi ses déplacements et lui avait envoyé des menaces de mort via les médias sociaux. La Cour constate, en particulier, que, bien que disposant des outils juridiques pour poursuivre le partenaire de la requérante, les autorités n'ont pas mené d'enquête effective et n'ont envisagé à aucun moment ce qui aurait pu et dû être fait pour la protéger. Les autorités ont donc manqué à l'obligation qui leur incombait de la protéger contre des abus graves.

83. Pour des actes interindividuels de moindre gravité, telle que la surveillance des employés sur le lieu de travail, les États ont le choix d'adopter, ou non, une législation spécifique concernant la vidéosurveillance (*López Ribalda et autres c. Espagne* [GC], 2019, § 113 ; *Köpke c. Allemagne* (déc.), 2010) ou la surveillance de la correspondance et des communications non professionnelles des employés (*Bărbulescu c. Roumanie* [GC], 2017, § 119). Il appartient toutefois aux juridictions internes de s'assurer que la mise en place par un employeur de mesures de surveillance portant atteinte au droit au respect de la vie privée ou de la correspondance des employés est proportionnée et s'accompagne de garanties adéquates et suffisantes contre les abus (*Köpke c. Allemagne* (déc.), 2010 ; *Bărbulescu c. Roumanie* [GC], 2017, § 120 ; *López Ribalda et autres c. Espagne* [GC], 2019, § 116 ; voir aussi, dans le contexte du contrôle par un parti politique de la correspondance électronique de ses membres, *Tena Arregui c. Espagne*, 2024, § 38).

84. Dans d'autres affaires relatives à la question de la divulgation des données à caractère personnel, la Cour a retenu l'obligation positive incombant à l'État d'enquêter sur les violations alléguées de l'article 8, qu'elles aient été l'œuvre des particuliers ou des autorités. Ainsi, dans l'affaire *Craxi c. Italie (n° 2)*, 2003 (§§ 68-76), qui concernait la lecture en audience puis la divulgation dans la presse de retranscriptions de conversations téléphoniques d'un politicien, interceptées dans le contexte de poursuites pénales pour corruption, la Cour a estimé que les autorités avaient une obligation positive d'empêcher la divulgation dans le domaine public de telles conversations privées. La divulgation n'ayant pas été la conséquence directe d'un acte du procureur mais plutôt le résultat d'un dysfonctionnement du greffe du tribunal, la Cour a conclu à la violation de l'article 8, les autorités ayant failli à prendre les mesures qui s'imposaient pour assurer la protection effective des droits du requérant en mettant en place les garanties appropriées et en menant une enquête effective.

85. Dans l'affaire *Alkaya c. Turquie*, 2012 (§§ 30-40), la Cour a mis en cause le degré de protection, jugé insuffisant, accordé par les juridictions internes à la protection des renseignements personnels d'une actrice célèbre, dont l'adresse complète avait été diffusée par un organe de presse. N'ayant aperçu aucun élément susceptible d'éclairer d'éventuelles raisons d'intérêt général pour lesquelles le journal avait décidé de divulguer l'adresse domiciliaire de la requérante, la Cour a observé que les juridictions nationales n'avaient pas pris en compte les répercussions sur la vie de la requérante de la diffusion de son adresse personnelle dans la presse. À ses yeux, ce défaut d'évaluation des intérêts en cause par les juridictions internes ne pouvait pas passer pour conforme aux obligations positives de l'État au titre de l'article 8.

86. Dans le contexte de la violence domestique, la Cour a estimé, dans l'affaire *Buturugă c. Roumanie*, 2020 (§§ 73-78), où l'ex-mari de la requérante avait abusivement consulté ses comptes électroniques, dont son compte Facebook, et fait des copies de ses conversations privées, de ses documents et de ses photos, que pesait sur les autorités l'obligation d'enquêter sur la violation du secret de la correspondance de la requérante. Reconnaissant la cyberviolence comme un aspect de la violence à l'encontre des femmes et des filles qui peut se présenter sous diverses formes, dont l'intrusion dans l'ordinateur de la victime et la prise, le partage et la manipulation des données et des images, y compris des données intimes, la Cour a accepté que des actes tels que surveiller, accéder à ou sauvegarder sans droit la correspondance du conjoint pouvaient être pris en compte lorsque les autorités nationales enquêtaient sur des faits de violence domestique. De telles allégations de violation de la correspondance appellent de la part des autorités un examen sur le fond afin de pouvoir appréhender de manière globale le phénomène de violence conjugale dans toutes ses formes (*ibidem*, §§ 76-77). Un tel examen avait fait défaut en l'espèce et la Cour a conclu à la violation de l'article 8 (voir aussi, dans un contexte similaire, *Volodina c. Russie (n° 2)*, 2021, §§ 48-68).

C. Les trois « tests » en matière de protection des données

87. Le paragraphe 2 de l'article 8 précise dans quelles conditions il peut y avoir ingérence dans la jouissance du droit protégé ; une telle ingérence doit être « prévue par la loi », poursuivre un « but légitime » et être « nécessaire dans une société démocratique ».

1. La légalité de l'ingérence

88. La Cour a examiné dans plusieurs affaires la question de savoir si l'exigence, énoncée à l'article 5 de la Convention 108, selon laquelle les données à caractère personnel faisant l'objet d'un traitement automatisé doivent avoir été obtenues et traitées loyalement et licitement, a été respectée ou non. Dans quelques affaires, la Cour a conclu à une violation de l'article 8 en se fondant seulement sur l'absence d'une base légale au niveau national qui autoriserait les mesures susceptibles d'y porter atteinte (*Taylor-Sabori c. Royaume-Uni*, 2002, §§ 17-19 ; *Radu c. Moldova*, 2014, § 31 ; *Mockutė c. Lituanie*, 2018, §§ 103-104 ; *M.D. et autres c. Espagne*, 2022, §§ 61-64 ; *Kaczmarek c. Pologne*, 2024, §§ 74-80).

89. En particulier, dans l'affaire *Mockutė c. Lituanie*, 2018 (§§ 103-104), la Cour a relevé que ni le gouvernement ni les juridictions nationales n'avaient indiqué une quelconque disposition juridique sur laquelle aurait reposé, le cas échéant, la communication, par l'hôpital psychiatrique, d'informations sur la santé de la requérante adulte à sa mère et aux journalistes. Dans l'affaire *Taylor-Sabori c. Royaume-Uni*, 2002 (§§ 17-19), où le requérant avait fait l'objet d'une surveillance policière par le biais d'un « clone » de son messager de poche, le droit interne n'était pas doté de dispositions régissant l'interception de communications transmises par un système de télécommunications privé. Dans l'affaire *Radu c. République de Moldova*, 2014 (§ 31), la diffusion, par un hôpital public, des informations médicales au sujet de la grossesse de la requérante, de son état de santé et du traitement qu'elle avait reçu auprès de son employeur n'était pas « prévue par la loi ». Dans l'affaire *M.D. et autres c. Espagne*, 2022 (§§ 61-64), la police avait rédigé un rapport sur des juges et magistrats qui exerçaient en Catalogne et qui avaient signé un manifeste dans lequel ils s'étaient déclarés favorables, d'un point de vue juridique, à la possibilité pour le peuple catalan d'exercer son « droit de décider ». Or, le rapport en question renfermait des données à caractère personnel, des photographies, des informations d'ordre professionnel et les opinions politiques de certains des intéressés. La Cour a relevé que la rédaction par la police d'un tel rapport n'était pas prévue par la loi, et que, étant donné que les autorités publiques avaient utilisé des données à caractère personnel à des fins qui n'étaient pas celles pour lesquelles elles avaient été recueillies, la seule existence de ce rapport, qui portait sur des personnes n'ayant commis aucun acte pénalement répréhensible, s'analysait en une violation de l'article 8 de la Convention. Dans l'arrêt *Kaczmarek c. Pologne*, 2024 (§§ 74-80), où l'enregistrement de la conversation téléphonique du requérant avait été divulgué lors d'une conférence de presse, la Cour a estimé que la disposition pertinente de la loi sur la procédure pénale, qui concernait principalement l'examen du dossier et la réalisation de copies au cours de l'enquête, ne pouvait pas être considérée comme une base légale propre à justifier pareille divulgation.

90. Dans d'autres affaires, la Cour a abouti à un constat de violation de l'article 8 au motif que la loi nationale, censée protéger les données à caractère personnel, était inaccessible ou confidentielle (*Vasil Vasilev c. Bulgarie*, 2021, §§ 169-170, *Nuh Uzun et autres c. Turquie*, 2022, §§ 80-99) ou n'était pas suffisamment claire et prévisible (*Vukota-Bojić c. Suisse*, 2016 ; *Ben Faiza c. France*, 2018, §§ 58-61 ; *Benedik c. Slovénie*, 2018 ; *Rotaru c. Roumanie* [GC], 2000 ; *Zoltán Varga c. Slovaquie*, 2021, § 162 ; *Haščák c. Slovaquie*, 2022, §§ 94-95 ; *Kaczmarek c. Pologne*, 2024, §§ 93-96). Ainsi, dans l'affaire *Nuh Uzun et autres c. Turquie*, 2022, §§ 80-99, la correspondance des détenus était scannée et enregistrée sur le Système informatique du Réseau judiciaire national conformément à des instructions qui avaient été communiquées directement et spécifiquement au parquet et aux autorités pénitentiaires par le ministère de la Justice mais qui n'avaient pas été rendues accessibles

au public en général ou aux requérants en particulier. Dans l'affaire *Vukota-Bojić c. Suisse*, 2016 (§§ 71-77), les dispositions sur lesquelles se fondait la surveillance secrète à laquelle la requérante avait été soumise par sa compagnie d'assurance après un accident de la route n'indiquaient pas de manière suffisamment claire l'étendue et les modalités d'exercice du pouvoir discrétionnaire conféré aux compagnies d'assurances agissant en tant qu'autorités publiques pour faire surveiller secrètement un assuré. Dans l'affaire *Rotaru c. Roumanie* [GC], 2000 (§§ 57-62), concernant les informations à caractère personnel conservées dans des dossiers détenus par le service de renseignement roumain, le droit national ne définissait pas le type d'informations qui pouvaient être traitées, les catégories de personnes à l'égard desquelles des mesures de surveillance pouvaient être prises, les circonstances dans lesquelles de telles mesures pouvaient être prises ou la procédure à suivre. Dans l'affaire *Benedik c. Slovénie*, 2018 (§ 132), certaines dispositions juridiques utilisées par la police pour obtenir les données sur l'abonné associées à l'adresse IP dynamique manquaient de clarté et n'offraient aucune protection contre une ingérence arbitraire, ne prévoyant pas des garanties contre d'éventuels abus ou de surveillance indépendante des pouvoirs de police en jeu. De même, dans l'arrêt *Kaczmarek c. Pologne*, 2024 (§§ 93-96), la conservation par les autorités d'éléments concernant la requérante qui avaient été recueillis dans le cadre d'une surveillance au cours d'une opération de sécurité dont elle-même ne faisait pas l'objet était fondée sur des dispositions légales qui manquaient de clarté et n'offraient aucune garantie procédurale, de sorte que la requérante n'avait pas été en mesure d'obtenir la destruction des éléments en question.

91. Au contraire, dans d'autres affaires, la Cour a abouti à un constat de non-violation de l'article 8 après avoir constaté que la loi nationale était claire et prévisible et comportait suffisamment de garanties contre les éventuels abus (*Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande* [GC], 2017, § 154 ; *Ben Faiza c. France*, 2018, § 75). Dans l'affaire *Ben Faiza c. France*, 2018 (§§ 70-76), la réquisition judiciaire utilisée pour obtenir, auprès d'un opérateur de téléphonie mobile, des données personnelles du requérant ne touchant pas au contenu de ses communications était « prévue par la loi ». Une disposition législative interne l'autorisait et l'encadrait, et contenait des garanties contre l'arbitraire, puisque de telles mesures étaient soumises à l'autorisation préalable d'un magistrat du parquet sous peine de nullité, étaient susceptibles d'un contrôle juridictionnel et les éléments obtenus pouvaient être exclus en cas d'illégalité (*ibidem*, § 73).

92. La Cour est parvenue à une conclusion similaire dans l'affaire *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande* [GC], 2017 (§ 154), relative à une décision de la commission de la protection des données personnelles, entérinée par la justice, interdisant la publication à grande échelle d'informations fiscales. Le libellé de la législation pertinente en matière de protection des données ainsi que la manière dont ces dispositions ont été appliquées à la suite des directives d'interprétation données aux juridictions finlandaises par la Cour de justice de l'Union européenne (CJUE), étaient suffisamment prévisibles. Le fait que l'affaire en question était la première de ce type au regard de la loi sur les données à caractère personnel et que la Cour administrative suprême a demandé à la CJUE des directives d'interprétation d'une dérogation prévue par la réglementation de l'Union européenne, ne rendaient pas l'interprétation et l'application de cette dérogation, par les juridictions internes, arbitraires ou imprévisibles (*ibidem*, § 150). Puisque les sociétés requérantes étaient des entreprises de médias, elles auraient dû, en cette qualité, avoir conscience que la collecte et la diffusion à grande échelle des données pouvaient ne pas être considérées comme un traitement de données effectué aux « seules » fins de journalisme au regard de la loi finlandaise ou de la réglementation de l'Union européenne (*ibidem*, § 151).

93. Dans l'affaire *Le Marrec c. France* (déc.), 2024, §§ 72-75, la Cour a conclu qu'un acte réglementaire qui contenait des dispositions précises, concernant le traitement des adresses IP, notamment, et qui avait été publié sur le site web de la Caisse d'allocations familiales, était suffisamment accessible au public et répondait donc à l'exigence de « légalité » posée par l'article 8 de la Convention.

94. Enfin, dans d'autres affaires, la Cour a jugé que la condition qu'une ingérence soit « prévue par la loi » était si étroitement liée à celle d'être « nécessaire dans une société démocratique » que ces conditions devaient être discutées ensemble (*S. et Marper c. Royaume-Uni* [GC], 2008, § 99 ; *Kvasnica c. Slovaquie*, 2009, § 84 ; *Kennedy c. Royaume-Uni*, 2010, § 155 ; *Glukhin c. Russie*, 2023, § 78).

95. Dans le contexte particulier des mesures de surveillance secrète, telle l'interception de communications, la Cour a jugé que la « prévisibilité » ne pouvait pas se comprendre de la même façon que dans beaucoup d'autres domaines. À ses yeux, 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 (*Adomaitis c. Lituanie*, 2022, § 83 ; voir aussi *Sârbu c. Roumanie*, 2023, § 51, où les mêmes principes ont été appliqués dans le contexte d'enregistrements réalisés par un particulier au moyen d'une caméra cachée). Cependant, puisque le risque d'arbitraire apparaît avec netteté là où un pouvoir de l'exécutif s'exerce en secret, il est indispensable que des règles claires et détaillées encadrent les mesures de surveillance secrète, 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 (*Malone c. Royaume-Uni,* 1984, § 67 ; *Leander c. Suède*, 1987, § 51 ; *Valenzuela Contreras c. Espagne*, 1998, § 46 ; *Weber et Saravia c. Allemagne* (déc.), 2006, § 93 ; *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev c. Bulgarie*, 2007, § 75 ; *Roman Zakharov c. Russie* [GC], 2015, § 229 ; *Denysyuk et autres c. Ukraine*, 2025, § 88). 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 (*Roman Zakharov c. Russie* [GC], 2015, § 230).

96. Au fil de sa jurisprudence relative à l'interception des communications dans le cadre des enquêtes pénales, la Cour a déterminé que, pour prévenir les abus de pouvoir, la loi doit au minimum énoncer les six éléments suivants : 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 ; et les circonstances dans lesquelles les données interceptées peuvent ou doivent être effacées ou détruites (*Huvig c. France*, 1990, § 34 ; *Valenzuela Contreras c. Espagne*, 1998, § 46 ; *Weber et Saravia c. Allemagne* (déc.), 2006, § 95 ; *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev c. Bulgarie*, 2007, § 76 ; *Denysyuk et autres c. Ukraine*, 2025, § 88). Dans l'arrêt *Roman Zakharov c. Russie* [GC], 2015 (§ 238), elle a confirmé que ces mêmes garanties minimales s'appliquaient aussi dans les cas où l'interception était faite pour des raisons de sécurité nationale ; toutefois, pour déterminer si la loi litigieuse était contraire à l'article 8, la Cour a tenu compte également des éléments suivants : les modalités du contrôle de l'application de mesures de surveillance secrète, l'existence éventuelle d'un mécanisme de notification et les recours prévus en droit interne[3].

97. Dans le contexte des données à caractère personnel recueillies par les autorités et conservées dans des bases de données pour prévenir ou réprimer la criminalité, la Cour a indiqué qu'il était essentiel de fixer des règles claires et détaillées régissant la portée et l'application de telles mesures et imposant un minimum d'exigences concernant, notamment, la durée, le stockage, l'utilisation, l'accès des tiers, les procédures destinées à préserver l'intégrité et la confidentialité des données et

[3] Voir aussi le *Guide sur l'article 8 de la Convention - droit au respect de la vie privée et familiale* sur l'exigence de prévisibilité de la loi en matière d'interception des communications, d'écoutes téléphoniques et des opérations secrètes de surveillance.

les procédures de destruction de celles-ci, de manière à ce que les justiciables disposent de garanties suffisantes contre les risques d'abus et d'arbitraire (*S. et Marper c. Royaume-Uni* [GC], 2008, §§ 99, 103 ; *Nuh Uzun et autres c. Turquie*, 2022, § 86). La Cour est parvenue à un constat de violation de l'article 8 dans les affaires où le droit interne ne définissait pas avec une clarté suffisante la portée et le mode d'exercice du pouvoir discrétionnaire conféré aux autorités internes (*Shimovolos c. Russie* (déc.), 2011, § 69 ; *Dimitrov-Kazakov c. Bulgarie*, 2011, § 33 ; *Negru c. République de Moldova*, 2023, § 34). Dans l'affaire *Shimovolos c. Russie* (déc.), 2011 (§ 70), la création et la mise à jour d'une base de données relative aux surveillances secrètes, enregistrant des données personnelles et des déplacements d'un militant des droits de l'homme, ainsi que ses modalités de fonctionnement étaient régies par un arrêté ministériel qui n'avait jamais été publié ou rendu accessible d'une autre manière au public. Dans l'affaire *Dimitrov-Kazakov c. Bulgarie*, 2011 (§ 33), le fichage d'un individu comme « délinquant » dans les registres de la police était fondé sur une instruction non publique à l'époque des faits, qui revêtait un caractère confidentiel et était réservée, jusqu'à son déclassement ultérieur, à l'usage interne du ministère des Affaires intérieures. Dans l'affaire *Negru c. République de Moldova*, 2023 (§ 24), la requérante figurait sur la liste des personnes recherchées, ce qui signifiait que les données à caractère personnel la concernant étaient traitées dans le système d'information automatisé et intégré répertoriant au niveau national les infractions, les affaires pénales et les auteurs d'infractions, et sa photographie avait été placée sur le panneau d'affichage public d'un poste de police à la suite d'une décision qui avait été rendue dans le cadre d'une procédure opaque par un procureur qui avait joui d'une latitude dont la Cour a jugé qu'elle équivalait à un pouvoir sans limite.

98. Dans l'affaire *Catt c. Royaume-Uni*, 2019 (§§ 97, 106), la Cour a souligné le danger d'une approche ambiguë de la part des autorités en matière de collecte et conservation de données personnelles que favorise des notions définies de façon trop vague dans le droit interne.

99. Dans le contexte de la mise en application d'une technologie de reconnaissance faciale, la Cour a dit qu'aux fins du respect de l'exigence de « qualité de la loi », il était essentiel de disposer de règles détaillées régissant la portée et l'application des mesures, ainsi que de garanties solides contre le risque d'abus et d'arbitraire, et que la nécessité de disposer de garanties était d'autant plus grande lorsque la technologie de reconnaissance faciale était utilisée en temps réel (*Glukhin c. Russie*, 2023, § 82). Dans l'affaire en question, où elle se penchait pour la première fois sur la question de l'utilisation de cette technologie, elle a exprimé de sérieux doutes quant au respect de l'exigence de « qualité de la loi » par les dispositions légales litigieuses qui autorisaient le traitement de données biométriques à caractère personnel, y compris à l'aide de la technologie de la reconnaissance faciale, « en lien avec l'administration de la justice », ces dispositions étant formulées très largement et semblant permettre le traitement des données en question dans le cadre de tout type de procédure judiciaire. Elle a observé que le droit interne ne renfermait aucune limite quant à la nature des situations dans lesquelles la technologie de reconnaissance faciale pouvait être utilisée, aux buts pour lesquels elle pouvait être utilisée, aux catégories de personnes pouvant être visées ou au traitement des données sensibles à caractère personnel. Elle a en outre relevé que le recours à la technologie de reconnaissance faciale ne semblait être entouré d'aucune garantie procédurale – procédures d'autorisation, procédures à suivre aux fins de l'examen, de l'utilisation et de la conservation des données obtenues, mécanismes de surveillance ou voies de recours disponibles (*ibidem*, § 83).

2. La légitimité de l'ingérence

100. La Cour a examiné dans plusieurs affaires la question de savoir si l'exigence, énoncée à l'article 5 de la Convention 108, selon laquelle les données à caractère personnel faisant l'objet d'un traitement automatisé doivent avoir été recueillies ou enregistrées pour des finalités déterminées et légitimes, a été, ou non, respectée. Dans ces affaires, l'examen des buts légitimes susceptibles de justifier une ingérence dans l'exercice des droits qu'il protège, énumérés par l'article 8 § 2, est plutôt

succinct. Ces buts sont : la protection de la sécurité nationale, de la sûreté publique et du bien-être économique du pays, la défense de l'ordre et la prévention des infractions pénales, la protection de la santé ou de la morale, ou la protection des droits et libertés d'autrui. La Cour confirme généralement l'existence d'un ou de plusieurs de ces buts légitimes allégués par le gouvernement.

101. La Cour a par exemple considéré que la mémorisation, dans un registre secret de la police, de données relatives à la vie privée des personnes, puis leur utilisation dans le cadre de l'évaluation de l'aptitude de candidats à des postes importants du point de vue de la sécurité nationale poursuivait un but légitime au regard de l'article 8, à savoir la protection de la sécurité nationale (*Leander c. Suède*, 1987, § 49). La surveillance d'un requérant par GPS, ordonnée par le procureur aux fins d'enquêter sur plusieurs accusations de tentatives de meurtre revendiquées par un mouvement terroriste et de prévenir d'autres attentats à la bombe avait, pour la Cour, été menée dans l'intérêt de la sécurité nationale, de la sûreté publique, de la prévention des infractions pénales et de la protection des droits des victimes (*Uzun c. Allemagne,* 2010, § 77).

102. La Cour a également jugé que la défense du bien-être économique du pays constituait un but légitime en matière de transmission de données bancaires aux autorités d'un autre État en application d'un accord bilatéral (*G.S.B. c. Suisse*, 2015, § 83). Le secteur bancaire représentant une branche économique importante pour l'État défendeur, la mesure incriminée, qui participait d'une tentative globale du gouvernement suisse de régler le conflit entre un établissement bancaire, qualifié d'« acteur important de l'économie suisse et employeur d'un nombre considérable de personnes », et les autorités fiscales américaines, pouvait valablement être considérée comme de nature à contribuer à la protection du bien-être économique du pays (*ibidem*, § 83).

103. Renvoyant aux textes internationaux qui font du fairplay et de l'égalité des chances l'un des fondements de la lutte antidopage, la Cour a estimé que la protection de la santé et de la morale justifiait l'obligation de localisation des sportifs compte tenu de l'impératif de combattre le dopage dans le domaine sportif (*Fédération nationale des associations et syndicats de sportifs (FNASS) et autres c. France*, 2018, §§ 164-166). Pour la Cour, ce que le Gouvernement qualifiait de « morale », s'agissant de la recherche d'un sport égalitaire et authentique, se rattachait également au but légitime que constitue la « protection des droits et liberté d'autrui » puisque l'usage de substances dopantes pour obtenir des résultats dépassant ceux des autres sportifs incite dangereusement les pratiquants amateurs, en particulier les jeunes, à utiliser de tels procédés pour capter des succès valorisants et prive les spectateurs d'une compétition loyale à laquelle ils sont légitimement attachés (*ibidem*, § 166).

104. Dans l'affaire *Ben Faiza c. France*, 2018 (§ 77), la Cour a considéré que la réquisition, adressée par les autorités d'enquête à un opérateur de téléphonie mobile et utilisée pour requérir des données personnelles ne touchant pas au contenu des communications, visait à permettre la manifestation de la vérité dans le cadre d'une procédure pénale relative à des faits d'importation de stupéfiants en bande organisée, d'association de malfaiteurs et de blanchiment. Cette mesure poursuivait donc les buts légitimes de la défense de l'ordre, la prévention des infractions pénales ainsi que la protection de la santé publique.

105. Dans l'affaire *Adomaitis c. Lituanie*, 2022 (§ 84), la Cour a conclu que l'interception de communications téléphoniques du requérant – un directeur de prison soupçonné de corruption –, la conservation de ces informations et leur divulgation lors de la procédure disciplinaire ayant abouti à son licenciement avaient eu pour but d'empêcher des actes de corruption et de garantir la transparence et l'ouverture au sein du service public, et que ces mesures avaient donc poursuivi les buts légitimes que constituent la défense de l'ordre et la prévention des infractions pénales ainsi que la protection des droits et libertés d'autrui. La Cour a formulé des conclusions similaires concernant l'enregistrement de conversations au moyen d'une caméra cachée par un particulier dans un cadre professionnel, enregistrement que les autorités avaient ensuite utilisé pour prouver que le requérant était coupable de corruption (*Sârbu c. Roumanie*, 2023, § 54).

106. Dans l'affaire *López Ribalda et autres c. Espagne* [GC], 2019 (§ 118, 123), l'intérêt légitime pour un employeur d'adopter des mesures afin de découvrir les responsables des pertes constatées et de les sanctionner, dans le but d'assurer la protection de ses biens et le bon fonctionnement de l'entreprise, pouvaient justifier les mesures de surveillances de ses employés sur leur lieu de travail.

107. La Cour a dit que la publication, sur le portail internet des services fiscaux, de renseignements propres à permettre l'identification du requérant, y compris son nom complet et l'adresse de son domicile, à raison du manquement de celui-ci à ses obligations fiscales, visait la protection du « bien-être économique du pays » et « la protection des droits et libertés d'autrui » (*L.B. c. Hongrie* [GC], 2023, §§ 111-13). Dans la même veine, elle a considéré que le traitement de l'adresse IP et d'autres données de connexion du requérant, qui avait permis à la Caisse d'allocations familiales de localiser l'intéressé dans un but de prévention de la fraude sociale, était dans l'intérêt du bien-être économique du pays et visait la prévention des infractions pénales (*Le Marrec c. France* (déc.), 2024, § 76).

3. La « nécessité dans une société démocratique » de l'ingérence

108. Pour être « nécessaire dans une société démocratique », toute mesure portant atteinte à la protection des données à caractère personnel qui relèvent de l'article 8 doit répondre à un « besoin social impérieux » et ne doit pas être disproportionnée par rapport aux buts légitimes poursuivis (*Z c. Finlande*, 1997, § 94 ; *Khelili c. Suisse*, 2011, § 62 ; *Vicent Del Campo c. Espagne*, 2018, § 46). Les motifs invoqués par le gouvernement doivent être pertinents et suffisants (*Z c. Finlande*, 1997, § 94). S'il appartient aux autorités nationales de juger les premières si ces conditions se trouvent remplies, c'est à la Cour qu'il revient de trancher en définitive la question de la nécessité de l'ingérence au regard des exigences de la Convention (*S. et Marper c. Royaume-Uni* [GC], 2008, § 101).

109. Dans les affaires relatives aux actes interindividuels d'une certaine gravité susceptibles de porter atteinte à l'article 8, le contrôle, par la Cour, de l'exigence de « nécessité dans une société démocratique » porte sur la manière dont l'État a assuré, au travers du cadre législatif, une protection adéquate et suffisante de l'individu (*K.U. c. Finlande*, 2008, §§ 43-50 ; *Söderman c. Suède* [GC], 2013, §§ 80-83). S'agissant des actes interindividuels de gravité moindre, tels, par exemple, la surveillance des employés sur leur lieu de travail, le contrôle, par la Cour, de l'exigence de « nécessité dans une société démocratique » porte sur la manière dont les juridictions internes ont pris en compte les critères que la Cour a dégagés dans sa propre jurisprudence et qui permettent de vérifier si les intérêts en jeu ont été correctement mis en balance (*López Ribalda et autres c. Espagne* [GC], 2019, §§ 116-117, § 122). Dans le cadre du contrôle sur les critères dégagés, si l'un des éléments fait défaut, les garanties découlant des autres critères revêtiront d'autant plus d'importance, et peuvent compenser l'élément défaillant (*ibidem*, § 131).

110. De façon plus générale, pour contrôler si une mesure portant atteinte à la protection des données à caractère personnel qui relèvent de l'article 8 remplit, ou non, la condition de « nécessité dans une société démocratique », la Cour a été amenée à examiner si elle respectait l'une ou l'autre des exigences énumérées par l'article 5 de la Convention 108, à savoir, notamment, l'exigence de minimisation des données stockés, de leur exactitude, de l'adéquation et de leur pertinence par rapport aux finalités pour lesquelles elles sont enregistrées, de la limitation de la durée de leur conservation, de leur utilisation pour le but pour lequel elles ont été recueillies et de la transparence du processus de traitement.

a. L'exigence de minimisation des données collectées ou enregistrées

111. La Cour a examiné dans plusieurs affaires la question de savoir si les données à caractère personnel faisant l'objet d'un traitement automatisé ont été adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées (*L.L. c. France*, 2006,

§§ 45-46 ; *Vicent Del Campo c. Espagne*, 2018, § 51 ; *Khadija Ismayilova c. Azerbaïdjan*, 2019, § 147, *Kruglov et autres c. Russie*, 2020, § 132 *in fine* ; *L.F. c. France* (déc.), 2024, § 34)).

112. La Cour a conclu à la violation de l'article 8 : après avoir noté qu'aucune procédure de filtrage des dispositifs de stockage des requérants, qui aurait pu minimiser les données saisies par les enquêteurs, n'avait été suivie au cours des perquisitions (*Kruglov et autres c. Russie*, 2020, § 132 *in fine*) ; s'agissant de la désignation d'une personne, dans une décision de justice interne, comme étant le harceleur d'une collègue de travail, alors que le juge pouvait ne pas indiquer son nom ou ne mentionner que ses initiales afin d'éviter sa stigmatisation (*Vicent Del Campo c. Espagne*, 2018, § 51) ; s'agissant d'une divulgation jugée excessive et inutile, lors d'un rapport d'avancement d'une enquête, des données personnelles d'une journaliste ayant été filmée à son insu dans l'intimité de son domicile (*Khadija Ismayilova c. Azerbaïdjan*, 2019, § 147).

113. Pour la Cour, des fichiers que les autorités nationales sont amenées à constituer pour contribuer à la répression et à la prévention de certaines infractions ne sauraient être mis en œuvre dans une logique excessive de maximalisation des informations qui y sont placées (*B.B. c. France*, 2009, § 62 ; *Gardel c. France*, 2009, § 63 ; *M.B. c. France,* 2009, § 54). Sans le respect d'une nécessaire proportionnalité au regard des objectifs légitimes qui leur sont attribués, les avantages qu'ils apportent seraient compromis par les atteintes graves qu'ils causeraient aux droits et libertés que les États doivent assurer aux personnes placées sous leur juridiction (*M. K. c. France*, 2013, § 35 ; *Aycaguer c. France*, 2017, § 34). Dans le cadre d'un système de conservation indiscriminée et illimitée des données personnelles, accepter l'argument selon lequel plus les données sont conservées, plus la criminalité serait évitée, reviendrait en pratique à justifier le stockage d'informations sur l'ensemble de la population et de leurs proches décédés, ce qui serait certainement excessif et dénué de pertinence (*Gaughran c. Royaume-Uni*, 2020, § 89).

114. Dans l'affaire *Catt c. Royaume-Uni*, 2019 (§ 122), la Cour a dit que l'absence de garanties effectives permettant la suppression, sur une base de données de la police, des données à caractère personnel révélant les opinions politiques d'un manifestant pacifique dès que la poursuite de leur conservation devenait disproportionnée s'analysait en une violation de l'article 8.

115. À l'inverse, la Cour a jugé que le traitement de données à caractère personnel ne présentant pas un caractère « sensible » au sens de l'article 6 de la *Convention 108* est conforme aux exigences de l'article 8 dès lors qu'il se limite à la conservation dans une base de données interne du ministère de la Justice d'informations factuelles et objectives relatives aux procédures judiciaires auxquelles un individu est partie (*L.F. c. France* (déc.), 2024, §§ 34 et 40). De même, dans l'affaire *Le Marrec c. France* (déc.), 2024, §§ 78-79, la Cour a relevé que l'adresse IP et les autres « données de connexion » du requérant, dont le traitement par la Caisse d'allocations familiales avait permis de déterminer qu'il résidait dans un « autre pays », ne présentaient pas un caractère « sensible », au sens exposé ci-dessus, pas plus qu'elles ne portaient sur les aspects les plus intimes ou les aspects particulièrement importants de l'existence ou de l'identité de l'intéressé : en effet, il s'agissait d'informations approximatives concernant le requérant, et la marge d'appréciation accordée aux autorités à cet égard était par conséquent étendue.

b. L'exigence d'exactitude et de mise à jour des données enregistrées

116. La Cour a eu à connaître de plusieurs affaires relatives à la mémorisation, par les autorités, de données qui se sont avérées inexactes ou dont l'exactitude était contestée par l'intéressé (*Cemalettin Canlı c. Turquie*, 2008, §§ 34-37, sur la présence de fichiers inexacts de la police dans une procédure pénale ; *Rotaru c. Roumanie* [GC], 2000, § 36, sur l'impossibilité de réfuter les données concernant une supposée participation d'un individu à un mouvement légionnaire dans son passé lointain recueillies par le service de sécurité).

117. Des informations de nature personnelle, fausses ou incomplètes, recueillies et conservées par les autorités peuvent rendre plus difficile la vie quotidienne de la personne concernée (*Khelili*

c. Suisse, 2011, § 64), s'avérer diffamatoires (*Rotaru c. Roumanie* [GC], 2000, § 44) ou peuvent écarter un certain nombre de garanties procédurales importantes prévues par la loi pour protéger les droits des personne concernée lorsque ces données peuvent être transmises entre différentes autorités (*Cemalettin Canlı c. Turquie*, 2008, §§ 42-43). La Cour a en outre souligné qu'il était inadéquat de collecter une donnée personnelle en l'absence de base factuelle avérée, sur le seul fondement de spéculations ou de présomptions (*Drelon c. France*, 2022, § 97).

118. Pour la Cour, c'est aux autorités qu'il incombe de démontrer l'exactitude des données qui avaient fait l'objet d'une telle mémorisation. Dans l'affaire *Khelili c. Suisse*, 2011 (§§ 66-70), où des incertitudes entouraient l'allégation vague et générale de prostitution à laquelle se serait livrée la requérante aux yeux des autorités, le maintien de la mention « prostituée » dans le dossier de police pendant plusieurs années n'a pas été jugé « nécessaire dans une société démocratique » au regard du comportement contradictoire des autorités, du principe selon lequel il leur appartenait d'apporter la preuve de l'exactitude d'une donnée, de la marge d'appréciation réduite dont elles jouissaient et de la gravité de l'ingérence dans le droit au respect de la vie privée garanti par l'article 8. De même, dans l'arrêt *Drelon c. France,* 2022 (§§ 95-97), qui concernait le refus opposé par l'Établissement français du sang à la candidature au don de sang du requérant en raison de son homosexualité supposée, la Cour a observé que la collecte de données à caractère personnel devait reposer sur une base factuelle précise et exacte, mais que l'Établissement français du sang avait tiré une conclusion sur les pratiques sexuelles du requérant en se fondant uniquement sur le fait que l'intéressé avait refusé de répondre lors de l'entretien médical préalable au don à des questions concernant sa sexualité.

119. Dans l'affaire *Anchev c. Bulgarie* (déc.), 2017 (§§ 112-115), où le requérant avait fait l'objet de trois enquêtes et avait été signalé, sur la foi des archives, comme collaborateur des anciens services de sécurité en vertu d'une loi sur la révélation des noms des personnes titulaires de fonctions publiques passant pour avoir collaboré au régime communiste, la Cour a rejeté le grief du requérant pour défaut manifeste de fondement, après avoir relevé qu'il avait pu consulter les archives, puis contester publiquement leur fiabilité sur la base d'éléments concrets.

120. Dans l'arrêt *Margari c. Grèce*, 2023, § 59, où les informations publiées dans la presse concernant les infractions pénales dont la requérante était accusée ne reflétaient pas de manière exacte les accusation portées contre elle, la Cour a souligné qu'il était capital que les données publiées dans le contexte de procédures pénales pendantes ou d'enquêtes sur des infractions pénales reflètent de manière précise la situation et les accusations pesant sur l'accusé, dans le respect également de la présomption d'innocence.

c. L'exigence de limiter la durée de conservation des données pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles ont été enregistrées[4]

121. La question de la nécessité de limiter la durée de conservation des données à caractère personnel a été examinée par la Cour dans plusieurs affaires (*S. et Marper c. Royaume-Uni* [GC], 2008 ; *B.B. c. France*, 2009 ; *Gardel c. France*, 2009 ; *M.B. c. France,* 2009 ; *M.K. c. France*, 2013 ; *J.P.D. c. France* (déc.), 2014 ; *Peruzzo et Martens c. Allemagne* (déc.), 2013 ; *W. c. Pays-Bas* (déc.), 2009 ; *Brunet c. France*, 2014 ; *Drelon c. France*, 2022, § 98). Une durée de conservation des données de trente ans maximum au fichier judiciaire national automatisé des auteurs d'infractions sexuelles à compter de l'expiration de la peine d'emprisonnement de cinq à quinze ans pour viol sur mineurs n'a pas été jugée disproportionnée au regard des buts légitimes poursuivis, par la mémorisation des

[4] Voir aussi la partie ci-dessous du présent Guide sur la « Durée du stockage des données ».

informations, de la défense de l'ordre et de la prévention des infractions pénales (*B.B. c. France*, 2009, §§ 67-68 ; *Gardel c. France*, 2009, §§ 68-69 ; *M.B. c. France*, 2009, §§ 59-60).

122. En revanche, la conservation permanente, dans une base de données nationale, des empreintes digitales, échantillons biologiques et profils ADN des personnes soupçonnées d'avoir commis une infraction mais non condamnées, quelle que soit la nature ou la gravité de l'infraction dont la personne avait été à l'origine soupçonnée et indépendamment de son âge, a été jugée contraire à l'article 8 (*S. et Marper c. Royaume-Uni* [GC], 2008, §§ 125-126). Dans le cas de mineurs soupçonnés d'avoir commis une infraction mais non condamnés, la conservation permanente de leurs données peut être particulièrement préjudiciable, en raison de leur situation spéciale et de l'importance que revêt leur développement et leur intégration dans la société (*ibidem*, § 124).

123. Cela dit, la destruction immédiate de données collectées, dès le moment où elles sont considérées comme étant dépourvues d'intérêt aux fins de la collecte en cause, en particulier dans le contexte d'une mesure secrète, n'est pas, en elle-même, contraire à la Convention (*Denysyuk et autres c. Ukraine*, 2025, § 108).

124. L'absence d'une période maximum pour la conservation des données personnelles n'est pas nécessairement incompatible avec l'article 8 (*Gaughran c. Royaume-Uni*, 2020, § 88 ; *Peruzzo et Martens c. Allemagne* (déc.), 2013, § 46), mais les garanties procédurales sont d'autant plus nécessaires là où la mémorisation des données dépend entièrement de la diligence avec laquelle les autorités veillent au caractère proportionné de la durée de leur conservation (*ibidem*, § 46 ; *Aycaguer c. France*, 2017, §§ 44-46). Dans l'arrêt *Grande Oriente d'Italia c. Italie*, 2024, §§ 144-46, un grand nombre de documents, qui renfermaient en particulier les données à caractère personnel concernant les membres de l'association requérante, avaient été saisis au cours d'une perquisition dans les locaux de cette association, perquisition qui avait été ordonnée dans le contexte d'une enquête parlementaire concernant la criminalité organisée. La Cour a observé qu'une copie des documents saisis était toujours conservée dans les archives de la commission d'enquête parlementaire, alors même que celle-ci avait achevé sa mission et avait été dissoute et qu'en vertu de la législation interne, les documents saisis auraient dû être restitués ou leurs copies détruites à la fin de l'enquête. Elle a rappelé à cet égard que l'absence de règles imposant la destruction de copies de documents obtenus dans le cadre d'une perquisition pouvait être incompatible avec l'article 8 de la Convention.

d. L'exigence de limiter l'utilisation des données pour le but pour lequel elles ont été enregistrées

125. La Cour a estimé qu'il est important de limiter l'utilisation des données pour le but pour lequel elles ont été enregistrées. Ainsi dans l'affaire *Karabeyoğlu c. Turquie*, 2016 (§§ 112-121), l'utilisation dans le cadre d'une enquête disciplinaire de données provenant d'écoutes téléphoniques issues d'une enquête pénale et, ayant donc pour finalité une autre que celle pour laquelle les données avaient été collectées, a été jugée contraire à l'article 8.

126. Dans l'affaire *Surikov c. Ukraine*, 2017 (§§ 83-95), la conservation de données relatives à la santé d'une personne pendant une très longue période ainsi que leurs diffusion et utilisation à des fins dépourvues de lien avec les raisons ayant initialement motivé leur collecte ont été considérées comme une atteinte disproportionnée au droit au respect de la vie privée du sujet des données.

127. La question du risque d'utilisation abusive des informations à caractère personnel s'est également posée dans l'affaires *K.H. et autres c. Slovaquie*, 2009 (§§ 45-57), où les requérantes, huit femmes d'origine rom, soupçonnées d'avoir été stérilisées pendant leur séjour dans des hôpitaux, se plaignaient de n'avoir pu obtenir des photocopies de leur dossier médical. La Cour a conclu à la violation de l'article 8 en soulignant que, pour parer au risque d'utilisation abusive des informations médicales allégué par le Gouvernement, il aurait suffi de mettre en place un dispositif législatif

visant à limiter strictement les cas dans lesquels celles-ci peuvent être utilisées ainsi que le nombre de personnes pouvant y avoir accès (*ibidem*, § 56).

128. Pour établir la frontière de l'intimité de la vie privée garantie par l'article 8, la Cour a distingué la surveillance des actes d'un individu dans un lieu public à des fins de sécurité, des enregistrements de ces actes utilisés à d'autres fins, allant au-delà de ce que l'intéressé aurait pu prévoir (*Peck c. Royaume-Uni*, 2003, §§ 59-62, sur un enregistrement du requérant sur une voie publique à des fins de sécurité, communiqué aux médias ; *Perry c. Royaume-Uni*, 2003, §§ 41-42, sur un subterfuge employé par la police à des fins d'identification vidéo du requérant excédant les limites de l'utilisation normale ou prévisible des caméra de surveillance dans les commissariats de police ; *Glukhin c. Russie*, 2023, §§ 65-73, sur l'utilisation d'une technologie de reconnaissance faciale dans le contexte de la surveillance de l'espace public au moyen de caméras de surveillance en circuit fermé).

e. L'exigence de transparence du processus de traitement des données[5]

129. Dans une série d'affaires relatives aux données à caractère personnel recueillies et mémorisées par les pouvoirs publics, la Cour a considéré que pesait sur les autorités une obligation positive d'offrir aux intéressés une « procédure effective et accessible » qui leur permette d'avoir accès à « l'ensemble des informations pertinentes et appropriées » pour connaître et comprendre leurs enfance et années de formation (*Gaskin c. Royaume-Uni*, 1989, § 49), pour retracer leur identité personnelle (*Odièvre c. France* [GC], 2003, §§ 41-49), pour identifier les risques pour la santé auxquels ils avaient été exposés (*Roche c. Royaume-Uni* [GC], 2005, § 162 ; *Guerra et autres c. Italie*, 1998, § 60 ; *McGinley et Egan c. Royaume-Uni*, 1998, § 101), ou pour retracer leur parcours personnel lors d'un ancien régime totalitaire (*Haralambie c. Roumanie*, 2009, § 93).

130. Une telle exigence de transparence est moindre dans le contexte des renseignements sensibles pour la sécurité nationale (*Leander c. Suède*, 1987, § 51 ; *Segerstedt-Wiberg et autres c. Suède*, 2006, § 102 ; *Dalea c. France* (déc.), 2010).

II. Protection des données et droit au respect de la vie privée (article 8 de la Convention)

Article 8 de la Convention

> « 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
>
> 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

[5] Voir aussi la partie ci-dessous du présent Guide sur le « Droit d'accès à ses propres données ».

131. La Cour s'est à ce jour penchée sur un grand nombre d'opérations effectuées sur des données à caractère personnel par des autorités ou par des entités privées pour examiner si la « vie privée », le « domicile » et/ou la « correspondance » du sujet des données ont été atteints de manière incompatible avec l'article 8. Dans différents contextes elle a précisé la portée d'un certain nombre de droits dont les personnes physiques ou morales concernées pouvaient se prévaloir pour protéger leurs données.

A. Opérations sur des données susceptibles de porter atteinte au droit au respect de la vie privée

132. Avec l'essor des technologies, la collecte, la conservation ou la divulgation des données prennent des formes très différentes. Dans plusieurs affaires, la Cour a examiné si une ou un ensemble de ces opérations a entraîné une atteinte injustifiée dans le droit au respect de la vie privée du sujet des données.

1. Collecte des données à caractère personnel

133. L'opération de collecte des données à caractère personnel a été examinée par la Cour dans différents contextes : s'agissant de la lutte contre le crime organisé et le terrorisme, à travers différents systèmes de surveillance secrète mis en place par les autorités ; dans le contexte judiciaire, s'agissant des données à caractère personnel recueillies par les autorités en vue d'être exploitées comme éléments de preuve ; dans le contexte de la santé ; dans le contexte des données recueillies sur les lieux de travail, qu'il s'agisse des employeurs publics ou privés ; et, enfin, dans le contexte d'obligations légales incombant aux entités publiques ou privées de transmettre aux autorités les données à caractère personnel en leur possession afin de protéger un intérêt public général.

a. Collecte de données par les autorités à travers la surveillance secrète[6]

134. La Cour a eu à traiter un nombre considérable d'affaires qui portaient sur la question de la collecte des données à caractère personnel à travers diverses méthodes de surveillance secrète. Quel que soit le système de surveillance employé par les autorités, l'existence de garanties adéquates et suffisantes contre les abus est essentielle. Pour la Cour, le pouvoir de surveiller en secret les citoyens n'est tolérable que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques (*Klass et autres c. Allemagne*, 1978, § 42 ; *Szabó et Vissy c. Hongrie*, 2016, §§ 72-73). Pareille ingérence doit se fonder sur des motifs pertinents et suffisants et doit être proportionnée aux buts légitimes poursuivis (*Segerstedt-Wiberg et autres c. Suède*, § 88). La législation interne doit être assortie de garanties suffisamment précises, effectives et complètes en ce qui concerne la prise, l'exécution et la réparation éventuelle des mesures de surveillance (*Szabó et Vissy c. Hongrie*, 2016, § 89).

i. Écoutes ciblées et comptage téléphonique

135. Dans le cadre judiciaire, la Cour a conclu à la violation de l'article 8 au sujet de : l'interception de communications et la livraison à la police de relevés de comptage (les numéros de téléphone appelés) (*Malone c. Royaume-Uni*, 1984, §§ 63-89) ; l'écoute et à la transcription de toutes les communications téléphoniques commerciales et privées des intéressés (*Huvig c. France*, 1990, §§ 24-35) ; l'interception et enregistrement de plusieurs conversations du requérant via la mise sur écoute d'une ligne tierce (*Kruslin c. France*, 1990, §§ 25-36) ; des écoutes téléphoniques dont une personne avait fait l'objet sur la ligne d'un tiers (*Lambert c. France*, 1998, §§ 21-41) ; l'interception et

[6] Voir aussi le *Guide sur l'article 8 de la Convention - droit au respect de la vie privée et familiale*.

l'enregistrement par le ministère public d'un appel téléphonique reçu par un individu, dans son bureau, d'un autre individu de l'ambassade, alors soviétique, à Berne (*Amann c. Suisse* [GC], 2000, §§ 45-62) ; des écoutes téléphoniques effectuées dans le cadre d'une enquête préliminaire (*Prado Bugallo c. Espagne,* 2003, §§ 28-33) ; des conversations téléphoniques interceptées dans le contexte de poursuites pénales et ultérieurement diffusées dans la presse (*Craxi c. Italie (nº 2)*, 2003, §§ 57-84) ; le versement au dossier pénal du requérant de la transcription d'écoutes téléphoniques réalisées dans une procédure à laquelle il était étranger (*Matheron c. France*, 2005, §§ 27-44) ; l'interception des communications téléphoniques par les autorités faute d'une autorisation du procureur délivrée au nom de la personne soupçonnée et en l'absence d'une loi offrant des garanties suffisantes contre l'arbitraire (*Dumitru Popescu c. Roumanie (nº 2)*, 2007, §§ 61-86) ; l'écoute des communications téléphoniques d'un avocat pour les enquêtes criminelles (*Kvasnica c. Slovaquie*, 2009, §§ 80-89) ; les garanties insuffisantes contre l'arbitraire dans les dispositions internes relatives à la mise sur écoute téléphonique (*Dragojević c. Croatie*, 2015, §§ 85-102 ; *Liblik et autres c. Estonie*, 2019, §§ 132-143 ; *Denysyuk et autres c. Ukraine*, 2025, §§ 93-135) ; l'absence de garanties judiciaires adéquates (*Moskalev c. Russie*, 2017, §§ 35-45) ; l'absence d'un contrôle efficace de l'enregistrement de communications téléphoniques dans le cadre d'une procédure pénale (*Pruteanu c. Roumanie*, 2015, §§ 41-58) ; l'interception des conversations du téléphone portable (*Šantare et Labazņikovs c. Lettonie*, 2016, §§ 56-63) ; l'absence non justifiée de notification *a posteriori* d'une écoute téléphonique temporaire du téléphone mobile (*Cevat Özel c. Turquie,* 2016, §§ 29-37) ; l'interception préventive des communications téléphoniques (*Mustafa Sezgin Tanrıkulu c. Turquie,* 2017, §§ 45-66) ; le pouvoir pratiquement illimité des services de renseignement pour mener une opération de surveillance d'un individu et des réunions qui étaient organisées dans un appartement dont il était propriétaire sans garanties juridiques suffisantes (*Zoltán Varga c. Slovaquie*, 2021, §§ 170-171), laquelle a aussi touché de manière aléatoire une autre personne qui ne bénéficiait d'aucune protection en vertu du droit interne (*Haščák c. Slovaquie*, 2022, § 95) ; et l'interception, l'enregistrement et la transcription d'une conversation téléphonique entre un avocat et l'un de ses clients, un ancien ministre de la Défense, qui était surveillé secrètement dans le cadre d'une affaire pénale (*Vasil Vasilev c. Bulgarie*, 2021, §§ 167-181).

136. La Cour a conclu à la non-violation de l'article 8 concernant des écoutes téléphoniques qui avaient été autorisées par décision judiciaire et sachant que la nécessité de la mesure avait été appréciée par les tribunaux (*İrfan Güzel c. Turquie*, 2017, §§ 78-89).

137. La Cour a aussi conclu à l'absence de violation de l'article 8 s'agissant : de la collecte par la police des numéros de téléphone appelés par un individu grâce au placement sous comptage de son téléphone privé (*P.G. et J.H. c. Royaume-Uni*, 2001, §§ 42-51) ; de la mise sur écoute des lignes téléphoniques d'un magistrat dans le cadre d'une enquête pénale menée sur une organisation illégale à laquelle il était suspecté d'appartenance ou d'aide et de soutien (*Karabeyoğlu c. Turquie*, 2016, §§ 74-111) ; et de l'interception de communications téléphoniques d'un directeur de prison dans le cadre d'une enquête sur des actes de corruption que l'intéressé était soupçonné d'avoir commis à des fins d'enrichissement personnel dans le cadre de ses fonctions, même si l'enquête a finalement été interrompue faute de preuves suffisantes (*Adomaitis c. Lituanie*, 2022, §§ 81-90).

138. Plusieurs requêtes ont été déclarées irrecevables, pour défaut manifeste de fondement, s'agissant : d'écoutes téléphoniques dans le cadre d'activités de renseignement préventives menées par la police (*Deveci c. Türkiye* (déc.), 2022) ; des écoutes téléphoniques dans le cadre d'une enquête préliminaire (*Greuter c. Pays-Bas* (déc.), 2002) ; de la mise sur écoutes de lignes téléphoniques dans le cadre d'une enquête pénale, ayant été l'un des principaux moyens d'investigation contribuant à démontrer l'implication d'individus dans un important trafic de stupéfiants (*Coban c. Espagne* (déc.), 2006) ; et de l'interception des communications téléphoniques d'un membre du Parlement européen accusé d'abus de biens sociaux et de l'inapplicabilité en l'occurrence du traitement particulier réservé aux députés nationaux (*Marchiani c. France* (déc.), 2008).

139. Dans le contexte de la prison, l'enregistrement et la conservation de conversations téléphoniques d'un prisonnier par les autorités pénitentiaires non prévues par la loi, et ensuite utilisés comme élément de preuve pour condamner le détenu pour une autre infraction ont emporté une violation de l'article 8 dans l'affaire *Doerga c. Pays-Bas*, 2004 (§§ 43-54).

140. Dans divers autres domaines, la Cour a conclu à la violation de l'article 8 relativement à : un régime de surveillance générale et indifférenciée de la correspondance et des conversations téléphoniques de mineurs placés dans un internat éducatif excluant toute confidentialité sans aucune distinction quant au type d'échanges interceptés (*D.L. c. Bulgarie*, 2006, §§ 100-116) ; l'interception par le ministère de la Défense, sur la base d'un mandat, des communications vers l'extérieur d'organisations œuvrant dans le domaine des libertés civiles (*Liberty et autres c. Royaume-Uni*, 2008, §§ 56-70) ; la simple existence d'une législation permettant d'intercepter les télécommunications d'une organisation non gouvernementale moldave spécialisée dans la représentation des requérants devant la Cour (*Iordachi et autres c. Moldova*, 2009, §§ 29-54) ; les fuites dans les médias et de la diffusion d'une conversation d'ordre privé enregistrée, avec l'aval des autorités, sur la ligne téléphonique d'un homme politique, qui était en cours d'examen devant les autorités de poursuites (*Drakšas c. Lituanie*, 2012, § 62) ; les défaillances du cadre juridique régissant la surveillance secrète des communications de téléphonie mobile mise en place par les opérateurs de réseau mobile permettant au Service fédéral de sécurité d'intercepter toute communication téléphonique sans autorisation judiciaire préalable (*Roman Zakharov c. Russie* [GC], 2015, §§ 163-305) ; et l'utilisation dans le cadre d'une enquête disciplinaire de données provenant d'écoutes téléphoniques issues d'une enquête pénale (*Karabeyoğlu c. Turquie*, 2016, §§ 112-121) ; l'utilisation de la transcription d'une conversation avec un client sur écoute téléphonique dans une procédure disciplinaire contre une avocate (*Versini-Campinchi et Crasnianski c. France*, 2016, §§ 49-84). À l'inverse, la Cour a jugé proportionné le recours, dans une procédure disciplinaire dirigée contre un directeur de prison, à des informations qui avaient été recueillies au moyen d'une mise sur écoute ordonnée dans le cadre d'une enquête pénale sur des actes de corruption que l'intéressé était soupçonné d'avoir commis (*Adomaitis c. Lituanie*, 2022, § 87).

ii. Interception des messages par biper

141. Dans le cadre de procédures judicaires, l'interception par la police des messages par biper du requérant et la référence subséquente à ces messages pour fonder une décision de condamnation ont été jugés, dans l'affaire *Taylor-Sabori c. Royaume-Uni,* 2002, §§ 18-19, contraires à l'article 8 en l'absence de cadre légal pour réglementer cette forme interception.

iii. Audiosurveillance et vidéosurveillance

142. La Cour a conclu à la violation de l'article 8 lorsque l'enregistrement d'une conversation à l'aide d'un appareil de radiotransmission dans le cadre d'une opération secrète de la police n'était pas entouré de garanties procédurales (*Bykov c. Russie* [GC], 2009, §§ 81, 83 ; *Oleynik c. Russie*, 2016, §§ 75-79).

143. La Cour a distingué la surveillance des actes d'un individu dans un lieu public à des fins de sécurité, des enregistrements de ces actes qui seraient utilisés à d'autres fins, allant au-delà de ce que l'intéressé aurait pu prévoir (*Peck c. Royaume-Uni*, 2003, §§ 59-62 ; *Perry c. Royaume-Uni*, 2003, §§ 41-42) pour établir, dans le domaine des mesures secrètes de surveillance ou de l'interception de communication par les autorités publiques, la frontière de l'intimité de la vie privée garantie par l'article 8. Elle a en outre souligné le caractère très intrusif de la technologie de reconnaissance faciale, en particulier de la technologie de reconnaissance faciale en temps réel utilisée dans le cadre de la surveillance de lieux publics au moyen de caméras de surveillance en circuit fermé, qui avait permis à la police de repérer et interpeller le requérant, alors qu'il se déplaçait en métro, pour s'être livré à une manifestation en solo sans déclaration préalable. La Cour a souligné qu'un niveau élevé de justification était nécessaire pour que ces mesures puissent être considérées comme

« nécessaires dans une société démocratique », le niveau de justification le plus élevé étant requis pour l'utilisation de technologies de reconnaissance faciale en temps réel (*Glukhin c. Russie*, 2023, § 86).

144. Dans le cadre judiciaire, la Cour a conclu à la violation de l'article 8 concernant : l'enregistrement des voix des requérants lors de leur inculpation et à l'intérieur de leur cellule au commissariat (*P.G. et J.H. c. Royaume-Uni*, 2001, §§ 56-63) ; l'enregistrement sur film à l'aide d'une caméra cachée de télévision en circuit fermé, à des fins d'identification, d'un suspect dans un commissariat de police (*Perry c. Royaume-Uni*, 2003, §§ 36-49) ; l'enregistrement par la police, grâce à l'installation d'un appareil d'écoute dans la maison d'un tiers chez qui le requérant s'était rendu, d'une conversation spontanée et non provoquée au cours de laquelle le requérant a admis être complice d'un réseau d'importation de drogue (*Khan c. Royaume-Uni*, 2000, §§ 25-28) ; la pose de micros par la police dans un lieu privé dans le cadre d'une information judiciaire (*Vetter c. France*, 2005, §§ 20-27) ; l'enregistrement d'une conversation grâce à un appareil d'écoute installé à même le corps par les autorités de police et son utilisation subséquente en tant que preuve essentielle lors du procès pénal, sans être la seule preuve accusatrice (*Heglas c. République tchèque*, 2007, §§ 71-76) ; l'enregistrement de communications par un particulier dans le contexte et au profit d'une enquête officielle, pénale ou autre, avec la complicité et l'assistance technique des autorités publiques d'enquête (*Van Vondel c. Pays-Bas*, 2007, §§ 47-55). À l'inverse, elle a conclu à l'absence de violation dans une affaire concernant l'utilisation dans une procédure pénale d'enregistrements vidéo de conversations entre le requérant et un particulier dans un contexte professionnel, enregistrements que le particulier en question avait réalisés de sa propre initiative au moyen d'une caméra cachée et que les autorités avaient découverts lors de l'examen de l'ordinateur d'un tiers sur lequel ils avaient été sauvegardés (*Sârbu c. Roumanie*, 2023, §§ 48-59).

145. Dans le contexte de la prison, la Cour a conclu à la violation de l'article 8 concernant : l'utilisation par les autorités d'appareils d'enregistrement vidéo et audio placés à l'insu du requérant dans sa cellule et dans la zone de visite de la prison ainsi que sur la personne d'un codétenu ayant permis l'enregistrement de déclarations du requérant non spontanées et provoquées (*Allan c. Royaume-Uni*, 2002, §§ 35-36) ; l'enregistrement des propos tenu par des détenus avec leurs proches dans les parloirs des prisons (*Wisse c. France*, 2005, §§ 28-34) ; la surveillance secrète des consultations d'un détenu avec son avocat (*R.E. c. Royaume-Uni*, 2015, §§ 115-143) ; et la vidéosurveillance permanente de détenus dans leurs cellules au moyen d'une caméra cachée de télévision en circuit fermé (*Gorlov et autres c. Russie*, 2019, §§ 83-100).

146. La Cour a conclu à la non-violation de l'article 8 relativement à la surveillance secrète des consultations du détenu avec la personne désignée pour l'aider, en tant que personne vulnérable, après son arrestation (*R.E. c. Royaume-Uni*, 2015, §§ 154-168). Les dispositions qui prévoyaient la possibilité de surveiller les consultations entre un détenu vulnérable et un adulte qualifié comportaient des garanties suffisantes contre les abus.

147. Dans différents contextes où la collecte des données avait été réalisée par caméras cachées, la Cour a conclu à la violation de l'article 8 au sujet de : la transmission aux médias d'une vidéo provenant d'une caméra cachée de télévision en circuit fermé, filmant une personne tentant de se suicider dans un lieu public (*Peck c. Royaume-Uni*, 2003, §§ 57-87) ; la diffusion à la télévision de l'image sans floutage ou voilage d'un particulier obtenue en caméra cachée (*Bremner c. Turquie*, 2015, §§ 71-85) ; l'enregistrement vidéo secret d'une journaliste à son domicile et la diffusion de ces vidéos au public (*Khadija Ismayilova c. Azerbaïdjan*, 2019, §§ 108-132).

iv. Géolocalisation d'un véhicule par GPS[7]

148. La surveillance par GPS d'une personne soupçonnée de terrorisme n'a pas constitué une violation de l'article 8 dans l'affaire *Uzun c. Allemagne*, 2010 (§§ 49-81). À l'inverse, dans l'affaire *Ben Faiza c. France*, 2018 (§§ 53-61), la mise en place d'un dispositif de géolocalisation dans un véhicule et l'exploitation des données issues de cette mesure ayant permis aux enquêteurs de connaître, en temps réel, les déplacements du requérant puis de procéder à son arrestation ont été jugés contraires à l'article 8.

v. Surveillance par des détectives privés

149. La surveillance illicite par des détectives privés des activités d'une allocataire de prestations sociales en litige a emporté un constat de violation de l'article 8 dans l'affaire *Vukota-Bojić c. Suisse*, 2016 (§§ 52-78). Le droit interne n'indiquait pas de manière suffisamment claire l'étendue et les modalités d'exercice du pouvoir discrétionnaire conféré aux compagnies d'assurances, agissant en tant qu'autorités publiques dans le cadre de litiges en matière d'assurances, pour faire surveiller secrètement des assurés.

vi. Contrôle du courrier

150. Dans le contexte de la prison, la Cour a conclu à la violation de l'article 8 concernant : la saisie et dépouillement de la correspondance d'un détenu (*Lavents c. Lettonie*, 2002, §§ 136-137) ; l'ouverture du courrier du détenu, y compris en cas de dysfonctionnement du service du courrier au sein de l'établissement pénitentiaire (*Demirtepe c. France*, 1999, §§ 26-28 ; *Valašinas c. Lituanie*, 2001, §§ 128-130) ; l'interception et la censure de la correspondance d'un détenu (*Silver et autres c. Royaume-Uni*, 1983, §§ 84-105 ; *Labita c. Italie* [GC], 2000, §§ 176-184 ; *Niedbała c. Pologne*, 2000, §§ 78-84 ; *Messina c. Italie (n° 2)*, 2000, §§ 78-83) ; l'interception de courriers de détenus à leur avocat (*Ekinci et Akalın c. Turquie*, 2007, §§ 37-48) ; l'interception de courriers de détenus avec l'avocat et avec la Commission européenne des Droits de l'Homme (*Campbell c. Royaume-Uni*, 1992, §§ 32-54 ; *A.B. c. Pays-Bas*, 2002, §§ 81-94) ; l'ouverture de la correspondance adressée à un détenu par la Commission (*Peers c. Grèce*, 2001, §§ 81-84) ; la surveillance de la correspondance d'un détenu avec le médecin spécialiste qui le suivait (*Szuluk c. Royaume-Uni*, 2009, §§ 47-55) ; la pratique consistant à scanner et enregistrer sur le Système informatique du Réseau judiciaire national la correspondance des détenus – aussi bien celle qu'ils voulaient expédier que celle qui leur était envoyée (*Nuh Uzun c. Turquie*, 2022, §§ 80-99). En revanche, dans l'affaire *Erdem c. Allemagne*, 2001 (§§ 53-70), le contrôle de la correspondance entre un détenu soupçonné de terrorisme et son avocat n'a pas donné lieu à un constat de violation de l'article 8.

151. Dans un autre contexte, le courrier d'une personne ayant fait faillite ouvert et copié par le mandataire-liquidateur a donné lieu à la violation de l'article 8 (*Foxley c. Royaume-Uni*, 2000, §§ 27-47).

vii. Opérations secrètes de surveillance, espionnage, surveillance de masse

152. Dans l'affaire *Roman Zakharov c. Russie* [GC], 2015 (§§ 171-172), la Cour a admis qu'un requérant pouvait se prétendre victime d'une violation entraînée par la simple existence de mesures de surveillance secrète ou d'une législation permettant de telles mesures si certaines conditions étaient remplies. Elle a également estimé que l'approche abordée dans l'affaire *Kennedy c. Royaume-Uni*, 2010 (§ 124) était la mieux adaptée à la nécessité de veiller à ce que le caractère secret des mesures de surveillance ne conduise pas à ce qu'elles soient en pratique inattaquables et qu'elles échappent au contrôle des autorités judiciaires nationales et de la Cour. Dans l'affaire

[7] Voir aussi la partie ci-dessus du présent guide sur les « Données de localisation GPS ».

Ekimdzhiev et autres c. Bulgarie, 2022 (§§ 262-277 et 371-384), elle a admis, en se fondant sur les principes qu'elle avait développés dans l'arrêt *Roman Zakharov c. Russie* [GC], 2015 (§ 171), que les requérants, deux avocats et deux organisations non gouvernementales qui leur étaient liées, pouvaient se dire victimes d'un ingérence dans l'exercice par eux de leurs droits consacrés par l'article 8 à raison de la simple existence d'une législation ou de pratiques internes autorisant la surveillance secrète ainsi que de lois régissant l'accès par les autorités à des données de communication ayant été conservées (voir aussi *Podchasov c. Russie*, 2024, §§ 54-55, pour une approche similaire concernant l'obligation légale pour les fournisseurs de services de communication sur Internet de stocker le contenu des communications sur Internet et les données de communication associées, de donner accès à ces données, sur demande, aux forces de l'ordre et aux services de sécurité, et, le cas échéant, de décrypter les messages électroniques cryptés).

153. La Cour a conclu à la violation de l'article 8 concernant : la possibilité pour l'association requérante de faire l'objet de mesures de surveillance à tout moment, sans avertissement en vertu de la loi sur les moyens de surveillance spéciaux (*Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev c. Bulgarie*, 2007, §§ 69-94) ; l'interception et l'enregistrement d'une conversation à l'aide d'un appareil de radiotransmission dans le cadre d'une opération secrète de la police sans garanties procédurales (*Bykov c. Russie* [GC], 2009, §§ 72-83) ; l'enregistrement de conversations entrepris dans le cadre de l'opération test sur l'initiative du Service fédéral de sécurité non « prévue par la loi » (*Oleynik c. Russie*, 2016, §§ 74-79) ; l'interception par le ministère de la Défense, sur la base d'un mandat, des communications vers l'extérieur d'organisations œuvrant dans le domaine des libertés civiles (*Liberty et autres c. Royaume-Uni*, 2008 ; §§ 55-70) ; le fichage et la surveillance par la police d'un requérant en raison de son appartenance à une organisation de défense des droits de l'homme (*Shimovolos c. Russie*, 2011, §§ 64-71) ; la législation en matière de surveillance secrète créant une task force spéciale en matière de lutte contre le terrorisme, en l'absence de garanties suffisantes contre les abus (*Szabó et Vissy c. Hongrie*, 2016, §§ 52-89) ; la conservation des renseignements collectés grâce à une surveillance secrète (*Rotaru c. Roumanie* [GC], 2000, §§ 45-63 ; *Association « 21 Décembre 1989 » et autres c. Roumanie*, 2011, §§ 169-177) ; les différentes défaillances du cadre juridique national régissant la surveillance secrète des communications de téléphonie mobile (*Roman Zakharov c. Russie* [GC], 2015, §§ 163-305) ; et des régimes d'interception en masse des communication qui ne renfermaient pas suffisamment de garanties « de bout en bout » pour offrir une protection adéquate et effective contre l'arbitraire et le risque d'abus, en dépit de certains garde-fous solides qu'ils comportaient (*Centrum för rättvisa c. Suède* [GC], 2021, §§ 365-374, et *Big Brother Watch et autres c. Royaume-Uni* [GC], 2021, §§ 424-427). Dans l'affaire *Ekimdzhiev et autres c. Bulgarie*, 2022 (§§ 356-359 et 419-421), elle a également conclu à la violation de l'article 8 : elle a observé, en particulier, qu'en dépit des améliorations notables qui y avaient été apportées depuis son examen dans le cadre de l'affaire *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev c. Bulgarie*, 2007, la législation relative à la surveillance secrète, telle qu'appliquée en pratique, n'offrait toujours pas, à plusieurs égards, les garanties minimales contre l'arbitraire et les abus qu'elle aurait dû offrir. Elle est parvenue à la même conclusion concernant les lois relatives à la conservation de données de communication et à l'accès par les autorités à ces données. Dans la même veine, la Cour a considéré dans l'affaire *Pietrzak et Bychawska-Siniarska et autres c. Pologne*, 2024 (§§ 195-278), que deux lois polonaises permettant des mesures de surveillance secrète et la conservation et le traitement de données de communication n'offraient pas de garanties suffisantes contre l'arbitraire.

154. Dans l'arrêt *Denysyuk et autres c. Ukraine*, 2025 (§§ 93-135 et §§ 148-50), trois requérants avaient fait l'objet de mesures de surveillance secrète dans le contexte d'opérations de police qui avaient été menées dans le cadre de procédures pénales les concernant. Or, ces mesures de surveillance secrète auraient pu donner lieu à l'interception de leurs communications avec le quatrième requérant, un avocat, ce qui aurait porté atteinte à la confidentialité des relations entre avocat et client. Eu égard i) au fait que les requérants s'étaient vu refuser, sans aucune mise en balance des intérêts concurrents en jeu, l'accès aux décisions judiciaires par lesquelles la mise en

œuvre de mesures de surveillance avait été autorisée, au seul motif que ces décisions étaient « classées », ii) à l'absence de règles ou directives internes précises définissant la procédure à suivre pour identifier et traiter les communications confidentielles entre un avocat et son client ayant été accidentellement interceptées, ou portant création d'une autorité indépendante chargée de contrôler l'interception de communications privées ; et iii) à l'absence de garanties procédurales suffisantes permettant de contrôler *a posteriori* la légalité et la nécessité de l'ingérence en cause et d'offrir une voie de redressement appropriée en cas de violation alléguée des droits garantis par l'article 8, la Cour est parvenue à la conclusion que l'ingérence litigieuse n'était pas « prévue par la loi » et qu'il y avait donc eu violation de l'Article 8 de la Convention.

155. La Cour a conclu à la non-violation de l'article 8 au sujet : du recours à un agent infiltré, couplé à la mise sur table d'écoutes du requérant, inculpé de trafic de stupéfiants (*Lüdi c. Suisse*, 1992, §§ 38-41) ; d'un régime autorisant la surveillance secrète de la correspondance, des envois postaux et des communications téléphoniques de la population (*Klass et autres c. Allemagne*, 1978, §§ 39-60) ; d'un dispositif législatif autorisant l'interception des communications internes pour lutter contre le terrorisme et les infractions graves (*Kennedy c. Royaume-Uni*, 2010, §§ 151-170).

156. La Cour a déclaré manifestement mal fondée l'affaire *Weber et Saravia c. Allemagne* (déc.), 2006 (§§ 143-153), sur la surveillance à but stratégique de télécommunications, affaire faisant suite à l'affaire *Klass et autres c. Allemagne*, 1978.

b. Collecte de données par les employeurs sur le lieu de travail

157. La Cour a examiné sous l'angle de l'article 8 la question de la collecte des données à caractère personnel sur le lieu de travail par des employeurs du secteur public (*Halford c. Royaume-Uni*, 1997, §§ 49, 45 ; *Antović et Mirković c. Monténégro*, 2017, § 58 ; *Libert c. France*, 2018, § 41) ou privé (*Köpke c. Allemagne* (déc.), 2010 ; *Bărbulescu c. Roumanie* [GC], 2017, § 109 ; *López Ribalda et autres c. Espagne* [GC], 2019, § 109). Dans certaines affaires, l'opération de collecte avait eu lieu à l'insu du sujet des données, lors d'une surveillance tenue secrète, en tout (*Halford c. Royaume-Uni*, 1997, § 49 ; *Copland c. Royaume-Uni,* 2007, § 45 ; *Bărbulescu c. Roumanie* [GC], 2017, § 78) ou en partie (*López Ribalda et autres c. Espagne* [GC], 2019, § 93), tandis que dans d'autres affaires la collecte avait été menée au vu et au su des employés concernés (*Antović et Mirković c. Monténégro*, 2017, § 44).

158. Les données personnelles visées par la collecte provenaient de : la surveillance des appels téléphoniques non professionnels émanant des locaux professionnels (*Halford c. Royaume-Uni*, 1997, § 44) ; la surveillance du téléphone, du courrier électronique et de l'Internet au travail (*Copland c. Royaume-Uni*, 2007, §§ 44-49) ; la surveillance de l'usage fait d'Internet et de la messagerie instantanée (Yahoo) (*Bărbulescu c. Roumanie* [GC], 2017, § 74) ; de l'ouverture des fichiers stockées par un employé sur un ordinateur mis à sa disposition par son employeur pour l'accomplissement de ses fonctions (*Libert c. France*, 2018, § 25) ; des images captées par des moyens d'enregistrement vidéo montrant le comportement d'un employé identifié ou identifiable sur son lieu de travail (*Köpke c. Allemagne* (déc.), 2010 ; *Antović et Mirković c. Monténégro*, 2017, § 44 ; *López Ribalda et autres c. Espagne* [GC], 2019, § 92) ; ou la surveillance, au moyen d'un système GPS, des distances qu'un employé parcourait avec son véhicule de fonction dans l'exercice de son activité professionnelle et, le cas échéant, lors de ses déplacements privés (*Florindo de Almeida Vasconcelos Gramaxo c. Portugal*, 2022, §§ 94-96).

159. Dans les deux premiers arrêts rendus dans ce domaine (*Halford c. Royaume-Uni*, 1997, § 44 et *Copland c. Royaume-Uni*, 2007, § 41), la Cour a considéré que les appels téléphoniques non professionnels émanant de locaux professionnels pouvaient se trouver compris dans les notions de « vie privée » et de « correspondance » visés à l'article 8. Elle a par ailleurs estimé que les messages électroniques envoyés depuis le lieu de travail devaient jouir de la même protection au titre de l'article 8, tout comme les éléments recueillis au moyen de la surveillance de l'usage qu'une

personne fait de l'Internet (*Copland c. Royaume-Uni*, 2007, § 41). Ultérieurement, la Cour a également précisé que des données clairement identifiées comme étant privées et stockées par un employé sur un ordinateur mis à sa disposition par son employeur pour l'accomplissement de ses fonctions étaient susceptibles de relever de sa « vie privée » (*Libert c. France*, 2018, § 25). En outre, un enregistrement vidéo réalisé en secret montrant le comportement de l'employé sur son lieu de travail sans avertissement touche aussi la « vie privée » (*Köpke c. Allemagne* (déc.), 2010). Puis la Cour n'a vu aucune raison de s'écarter de cette conclusion qu'il s'agisse de vidéosurveillance secrète ou non secrète de salariés sur leur lieu de travail (*Antović et Mirković c. Monténégro*, 2017, § 44 ; *López Ribalda et autres c. Espagne* [GC], 2019, § 93).

160. Dans les affaires *Halford c. Royaume-Uni*, 1997 (§§ 50-51) et *Copland c. Royaume-Uni,* 2007 (§ 48), la Cour a jugé que, faute à l'époque, d'une disposition de droit interne autorisant la collecte des données personnelles provenant, respectivement, des appels téléphoniques non professionnels des employés et des messages électroniques envoyés depuis le lieu de travail, l'ingérence qui en découlait pour leur droit au respect de la vie privée n'était pas « prévue par la loi ». Dans l'affaire *Köpke c. Allemagne* (déc.), 2010, la Cour a déclaré manifestement mal fondé le grief tiré de la collecte des données par un employeur avec l'aide d'une agence de détectives privés, à travers la surveillance vidéo secrète, d'une caissière de supermarché soupçonnée de vol. Même si, à l'époque des faits, les conditions dans lesquelles un employeur pouvait recourir à la surveillance vidéo d'un employé n'était pas encore énoncées dans la législation, la jurisprudence de la Cour fédérale du travail avait développé d'importantes garanties contre les ingérences arbitraires dans le droit d'un employé au respect de sa vie privée.

161. L'existence de soupçons raisonnables que des irrégularités graves avaient été commises et l'ampleur des manques constatés pouvaient apparaître comme des justifications sérieuses pour des mesures de collecte des données personnelles prises par les employeurs sur le lieu de travail (*López Ribalda et autres c. Espagne* [GC], 2019, § 134). En revanche, de simples soupçons que des détournements ou d'autres irrégularités aient été commis par des employés ne sauraient justifier la mise en place d'une surveillance secrète par l'employeur (*ibidem*, § 134).

162. Dans l'affaire *Bărbulescu c. Roumanie* [GC], 2017 (§ 121), la Cour a défini un certain nombre de critères auxquels les mesures de contrôle de la correspondance et des communications des employés sur leur lieu de travail doivent se conformer pour ne pas enfreindre l'article 8. Dans ce contexte, les autorités nationales doivent tenir compte des facteurs suivants : L'employé a-t-il été informé de la possibilité que l'employeur prenne des mesures de surveillance de sa correspondance et de ses autres communications ainsi que de la mise en place de telles mesures ? Quelle a été l'étendue de la surveillance opérée par l'employeur et le degré d'intrusion dans la vie privée de l'employé ? L'employeur a-t-il fourni des raisons à l'appui de la surveillance des communications de l'employé ? Aurait-il été possible de mettre en place un système de surveillance reposant sur des moyens et des mesures moins intrusifs que l'accès direct au contenu des communications de l'employé ? Quelles ont été les conséquences de la surveillance pour l'employé qui en a fait l'objet ? L'employé s'est-il vu offrir des garanties adéquates, notamment lorsque les mesures de surveillance de l'employeur avaient un caractère intrusif ? Enfin, pour assurer le respect effectif de ces exigences, les employés concernés doivent bénéficier d'une voie de recours devant un organe juridictionnel indépendant ayant compétence pour examiner, au moins en substance, le respect de ces critères ainsi que la licéité des mesures contestées (*ibidem*, § 122).

163. Ultérieurement, dans l'affaire *López Ribalda et autres c. Espagne* [GC], 2019 (§ 116), la Cour a précisé que ces critères étaient transposables aux mesures de vidéosurveillance qu'un employeur mettrait en place sur le lieu de travail. Dans l'arrêt *Florindo de Almeida Vasconcelos Gramaxo c. Portugal*, 2022 (§ 115), la Cour a en outre appliqué ces critères dans le contexte d'une surveillance par GPS qu'un employeur avait mise en place pour contrôler les distances parcourues par un employé avec son véhicule de fonction.

164. La Cour a conclu à la violation de l'article 8 dans les affaires où elle a constaté l'omission des juridictions nationales de s'assurer que la mise en place par un employeur des mesures de surveillance était proportionnée et s'accompagnait de garanties adéquates et suffisantes. Dans l'affaire *Bărbulescu c. Roumanie* [GC], 2017 (§§ 108-141), les juridictions nationales avaient omis de déterminer les raisons spécifiques qui avaient justifié la mise en place des mesures de surveillance, ou si l'employeur avait pu faire usage de mesures moins intrusives pour la vie privée et la correspondance de l'employé ou si ce dernier avait été préalablement averti par son employeur de la possibilité que ses communications soient surveillées. En revanche, dans l'affaire *Libert c. France*, 2018 (§§ 37-53), la Cour a conclu à l'absence de violation de l'article 8 quant à l'ouverture de fichiers personnels stockés sur un ordinateur professionnel, dont le contenu pornographique découvert a servi de base au licenciement de l'employé, après avoir observé que le droit interne, tel qu'interprété et appliqué par les juridictions nationales, contenait suffisamment de garanties contre l'arbitraire, notamment le fait que l'employeur ne pouvait ouvrir les fichiers identifiés comme étant personnels qu'en présence de l'employé.

165. Pour la Cour, seul un impératif prépondérant relatif à la protection d'intérêts publics ou privés importants pourrait justifier un manquement de l'employeur à fournir aux employés les informations préalables sur des mesures susceptible de porter atteinte à la protection des données des employés (*López Ribalda et autres c. Espagne* [GC], 2019, § 133). Avant de mettre en place des mesures de collecte de leurs données, les employeurs doivent informer les employés de façon claire de l'existence et des modalités d'une telle collecte, ne serait-ce que de manière générale (*ibidem*, § 131). L'exigence de transparence et le droit à l'information qui en découle revêtent un caractère fondamental, en particulier dans le contexte des relations de travail, où l'employeur dispose à l'égard des salariés de pouvoirs importants dont il convient d'éviter tout abus. Cependant, l'information donnée à la personne faisant l'objet d'une surveillance et son ampleur ne sont que l'un des critères à prendre en compte pour apprécier la proportionnalité d'une telle mesure dans un cas donné. Si une telle information fait défaut, les garanties découlant des autres critères devront revêtir d'autant plus d'importance (*ibidem*, § 131).

166. En cas d'absence d'information préalable, il est important de savoir si les employés ayant fait l'objet d'une mesure de surveillance disposaient de voies de recours au niveau national spécifiquement destinées à assurer la protection effective du droit au respect à la vie privée. Dans le cadre des mesures dont les employés seraient frappés sur le lieu de travail, cette protection peut être assurée par différents moyens qui peuvent relever du droit du travail mais aussi du droit civil (*ibidem*, § 136).

167. S'agissant plus spécifiquement de la vidéosurveillance des employés, la Cour a précisé, dans l'affaire *López Ribalda et autres c. Espagne* [GC], 2019 (§ 125), qu'il était nécessaire de distinguer, dans l'analyse de la proportionnalité, les différents lieux dans lesquels celle-ci est réalisée à l'aune de l'attente en matière de protection de la vie privée que le salarié peut raisonnablement avoir. Cette atteinte est très importante dans les endroits relevant de l'intimité, tels que des toilettes ou des vestiaires, où se justifie une protection accrue, voire une interdiction de procéder à une vidéosurveillance (*ibidem*, §§ 125, 61, 65, citant les instruments internationaux pertinents). Elle demeure forte dans les espaces de travail fermés, tels que les bureaux. Elle est manifestement réduite dans les endroits visibles ou accessibles aux collègues ou à un large public (*ibidem*, § 125).

168. À cet égard, dans l'affaire *Köpke c. Allemagne* (déc.), 2010, la Cour a déclaré irrecevable, pour défaut manifeste de fondement, le grief de la requérante, caissière dans un supermarché, relatif à une mesure de vidéosurveillance secrète mise en œuvre par son employeur avec l'aide d'une agence de détectives privés. La Cour a observé en particulier que la mesure litigieuse avait été limitée dans le temps (deux semaines) et n'avait concerné que la zone accessible au public et entourant la caisse, que les éléments vidéo obtenus avaient été traités par un nombre limité de personnes travaillant pour l'agence de détectives et par du personnel de l'employeur, et qu'ils n'avaient été utilisés que dans le cadre du licenciement de la requérante et de la procédure devant les juridictions du travail.

169. En revanche, dans l'arrêt *Antović et Mirković c. Monténégro*, 2017 (§§ 55-60), la Cour a conclu à la violation de l'article 8, jugeant que l'atteinte alléguée à la vie privée des requérants, deux professeurs d'université, ayant résulté de l'installation d'un système de vidéosurveillance dans leurs lieux d'enseignement, n'était pas prévue par la loi.

170. Dans l'affaire *López Ribalda et autres c. Espagne* [GC], 2019 (§ 137), la Cour a conclu à la non-violation de l'article 8 au regard à une vidéosurveillance en partie visible et en partie cachée des caissières et vendeuses d'un supermarché, compte tenu, entre autres, des garanties importantes offertes par le cadre normatif espagnol, y compris les voies de recours que les requérantes n'avaient pas empruntées.

171. De même, l'affaire *Florindo de Almeida Vasconcelos Gramaxo c. Portugal*, 2022 (§§ 105-125) concernait le licenciement du requérant sur le fondement des données kilométriques qui avaient été recueillies au moyen d'un système GPS installé par l'employeur de l'intéressé sur son véhicule de fonction. La Cour a conclu à la non-violation de l'article 8 au motif que les juridictions internes avaient correctement mis en balance les intérêts concurrents en jeu, c'est-à-dire, d'un côté, le droit du requérant au respect de sa vie privée et, de l'autre, le droit de l'employeur au bon fonctionnement de son entreprise, en tenant compte du but légitime poursuivi par l'entreprise, à savoir le droit de contrôler ses dépenses.

172. Des principes similaires s'appliquent également dans d'autres contextes, notamment en ce qui concerne le contrôle par un parti politique des communications électroniques de ses membres, même si les structures organisationnelles internes des partis politiques se distinguent de celles des entreprises privées et si les liens juridiques qui existent entre un employeur et un employé et entre un parti politique et ses membres sont fondamentalement différents (*Tena Arregui c. Espagne*, 2024, §§ 38 et 41).

c. Collecte des données en vue d'être exploitées comme éléments de preuve dans les affaires judiciaires

173. La collecte des éléments de preuve matériels dans le cadre des affaires judiciaires soulève des questions liées à la protection des données personnelles des individus, quelle que soit leur position dans la procédure en cause, qu'ils soient des parties, des témoins, ou de simples tiers.

i. Saisies et perquisitions

174. Dans plusieurs affaires, la Cour a souligné que les États contractants pouvaient estimer nécessaire de recourir à des mesures telles que des perquisitions et des saisies pour établir la preuve matérielle de certaines infractions (*Vasylchuk c. Ukraine*, 2013, § 79 ; *K.S. et M.S. c. Allemagne*, 2016, § 43). Son contrôle porte alors sur le caractère pertinent et suffisant des motifs invoqués pour justifier pareilles mesures, ainsi que le respect du principe de proportionnalité par rapport au but recherché (*Smirnov c. Russie*, 2007, § 44). La gravité de l'infraction qui a motivé la perquisition et la saisie ; les circonstances dans lesquelles le mandat a été émis, en particulier les autres éléments de preuve qui étaient disponibles à l'époque ; le contenu et l'étendue du mandat, eu égard en particulier à la nature des lieux perquisitionnés et aux garanties prises pour que la mesure n'ait pas d'effets déraisonnables ; la façon dont la perquisition a été menée ; et l'étendue des répercussions possibles sur le respect de la vie privée de la personne visée sont des éléments importants à prendre en compte lors de la mise en balances des différents intérêts en jeu (*ibidem*, § 44 ; *Modestou c. Grèce*, 2017, § 42 et les références citées). La Cour exige également que le droit interne offre des garanties adéquates et suffisantes contre l'arbitraire (*Vinci Construction et GTM Génie Civil et Services c. France*, 2015, § 66 ; *Modestou c. Grèce*, 2017, § 43 ; *Reznik c. Ukraine*, 2025, § 58). L'existence d'un « contrôle efficace » des mesures attentatoires à l'article 8 figure parmi ces garanties (*Modestou c. Grèce*, 2017, § 42).

175. Dans l'affaire *Trabajo Rueda c. Espagne*, 2017 (§§ 44-47), une mesure de saisie de l'ordinateur personnel du requérant qui avait permis l'accès de la police à toutes les archives personnelles stockées sur l'ordinateur au motif qu'il contenait des éléments pédopornographiques a été jugée contraire à l'article 8. La Cour n'a pas été persuadée de l'urgence qui aurait contraint la police à saisir les archives de l'ordinateur personnel du requérant et à accéder à toutes les données stockées sans obtenir au préalable l'autorisation judiciaire normalement requise, alors que cette autorisation aurait pu être obtenue relativement rapidement.

176. Dans l'affaire *K.S. et M.S. c. Allemagne*, 2016 (§§ 32-58), la Cour n'a pas jugé contraire à l'article 8 la perquisition au domicile des requérants en vertu d'un mandat délivré sur la base d'éléments contenant des données à caractère personnel, copiées illégalement par un employé d'une banque puis vendues aux services secrets, relatives à leurs avoirs dans une banque à l'étranger. La législation et la pratique allemandes offraient des garanties adéquates et effectives contre les abus. Et les juridictions nationales n'avaient pas outrepassé leur marge d'appréciation en fondant le mandat de perquisition sur les données provenant de l'étranger. La Cour a, entre autres, attaché une importance particulière au fait qu'au moment où le mandat de perquisition avait été délivré, la série de données litigieuses était l'une des rares séries à avoir été achetées par les autorités allemandes (*ibidem*, § 51). Aussi, le simple fait qu'aucune règle absolue n'interdisait l'utilisation dans un procès pénal de preuves recueillies en violation des règles procédurales ne signifiait pas que les autorités aient délibérément recueilli les données en violation du droit international et du droit interne (*ibidem*, § 51). En outre, le support des données ne contenait aucune information étroitement liée à l'identité des requérants, mais seulement des informations relatives à leur situation financière qu'ils étaient tenus de remettre aux autorités fiscales nationales (*ibidem*, § 53 ; comparer avec l'affaire *G.S.B. c. Suisse*, 2015, § 93, concernant la transmission de données bancaires aux autorités fiscales d'un autre État en application d'un accord bilatéral).

177. Les perquisitions effectuées dans les locaux des sociétés pour collecter des éléments matériels de preuve soulèvent des questions liées à la protection de leurs données, sous l'angle du droit au respect de leur « correspondance » et « domicile », garanti par l'article 8. Par exemple, dans l'affaire *Bernh Larsen Holding AS et autres c. Norvège*, 2013 (§§ 104-175), la Cour n'a pas conclu à la violation de l'article 8 s'agissant d'une décision enjoignant à une société de remettre une copie de l'intégralité des données du serveur informatique qu'elle partageait avec d'autres sociétés. Même si la loi applicable n'exigeait pas l'autorisation préalable d'une autorité judiciaire, la Cour a pris en compte l'existence de garanties effectives et adéquates contre les abus, les intérêts tant des sociétés que de leurs employés, et l'intérêt public relatif à la réalisation de contrôles fiscaux efficaces (*ibidem*, §§ 172-175). En revanche, la Cour a constaté la violation de l'article 8 dans l'affaire *DELTA PEKÁRNY a.s. c. République tchèque*, 2014 (§§ 92-93), concernant l'inspection de locaux commerciaux en vue de rechercher des indices et des preuves de l'existence d'une entente illicite sur les prix contraire aux règles de concurrence. La Cour s'est référée à l'absence d'autorisation préalable d'un juge, de contrôle effectif *a posteriori* de la nécessité de la mesure, et de réglementation relative à une éventuelle destruction des données obtenues.

178. Dans l'affaire *Buck c. Allemagne*, 2005 (§§ 30-53), les perquisitions au domicile et dans les locaux professionnels en relation avec une infraction routière commise par un tiers ont constitué une violation de l'article 8. Compte tenu des circonstances spéciales de l'affaire, en particulier de ce que la perquisition et la saisie en question avaient été ordonnées à propos d'une simple contravention, dont on pensait qu'elle avait été commise par un tiers, et qu'elles visaient également le domicile privé du requérant, la Cour a conclu que l'ingérence ne saurait être tenue pour proportionnée aux buts légitimes poursuivis (*ibidem*, § 52).

179. Concernant des perquisitions dans les locaux professionnels de journalistes, leurs domiciles et les véhicules de certains et les saisies massives visant à identifier leurs sources, la Cour a conclu à la violation de l'article 8 dans l'affaire *Ernst et autres c. Belgique*, 2003 (§§ 110-117). En matière de lutte contre la violation du secret de l'instruction, la législation des États contractants et leur

pratique, qui peuvent prévoir des visites domiciliaires et des saisies, doivent offrir des garanties adéquates et suffisantes contre les abus. Or tel ne fut pas le cas en l'espèce étant donné qu'aucune infraction n'était reprochée aux requérants et que les différents mandats de perquisition étaient rédigés en des termes larges, ne donnant aucune information sur l'instruction en cause, sur les lieux précis à visiter et sur les objets à saisir, octroyant ainsi de larges pouvoirs aux enquêteurs. En outre, les requérants avaient été laissés dans l'ignorance quant aux motifs concrets des perquisitions (voir aussi le paragraphe 355 ci-dessous du présent guide concernant la violation de l'article 10 dans cette affaire).

180. S'agissant des saisies opérées dans le cabinet d'un avocat, elles doivent impérativement être assorties des garanties spéciales de procédure, capables de préserver la confidentialité des données qui est la base de la relation de confiance qui existe entre l'avocat et son client[8]. Dans l'affaire *Kırdök et autres c. Turquie*, 2019 (§§ 52-58), la saisie des données électroniques de plusieurs avocats par les autorités judiciaires pour les besoins d'une procédure pénale dirigée à l'encontre d'un autre avocat qui partageait le même bureau qu'eux, et le refus de les restituer ou de les détruire a emporté une violation de l'article 8. La Cour a accordé du poids au fait qu'aucune procédure de filtrage des documents ou des données électroniques protégés par le secret professionnel n'avait été observée pendant la perquisition. Et le refus de retourner les données saisies au motif que, n'étant pas encore transcrites, il ne pouvait pas être établi à qui elles appartenaient, n'était pas clairement prévu par la loi, et était contraire à l'essence même du secret professionnel, qui appelait la confidentialité de ces données.

181. Dans l'affaire *Kruglov et autres c. Russie*, 2020 (§§ 123-138), la Cour a estimé que les saisies des ordinateurs et des disques durs renfermant des informations personnelles et des documents couverts par le secret professionnel des requérants, avocats de profession, ou de leurs clients, lors des perquisitions menées par la police à leurs domicile et bureaux, sans avoir procédé à aucun filtrage des données ainsi saisies, étaient contraires à l'article 8. Entre autres, l'existence d'une autorisation judiciaire préalable a eu un effet limité, puisque les tribunaux nationaux n'ont jamais tenté de mettre en balance l'obligation de protéger la confidentialité des données contre les besoins de l'enquête pénale, par exemple, en examinant la possibilité d'obtenir les renseignements auprès d'autres sources (*ibidem*, §§ 126-129). Plus généralement, la Cour voit comme une atteinte disproportionnée aux droits protégés par l'article 8 de la Convention le fait même que les appareils électroniques d'un avocat, qui peuvent contenir des éléments couverts par le secret professionnel, soient saisis, emportés et consultés par des représentants des autorités sans qu'aucun contrôle externe ni aucune autre garantie ne soit exigés (*Reznik c. Ukraine*, 2025, § 76, et les références qui y sont citées).

182. La Cour a également conclu à une violation de l'article 8 dans l'affaire *Smirnov c. Russie*, 2007 (§§ 36-49), au sujet des perquisition et saisie de nombreux documents ainsi que l'unité centrale de l'ordinateur d'un avocat, effectuées à son domicile, sans aucune justification ni garantie ; dans l'affaire *Wieser et Bicos Beteiligungen GmbH c. Autriche*, 2007 (§§ 42-68), par rapport aux fouilles et la saisie des données électroniques d'un avocat en méconnaissance des garanties procédurales prévues par la loi ; dans l'affaire *Robathin c. Autriche*, 2012 (§ 52), relativement à l'autorisation insuffisamment motivée concernant la recherche et la saisie de toutes données électroniques se trouvant dans un cabinet d'avocat ; dans l'affaire *Särgava c. Estonie*, 2021 (§§ 107-108), relativement aux garanties procédurales jugées insuffisantes pour protéger des données couvertes par le secret professionnel lors de la saisie, puis de l'examen de l'ordinateur et du téléphone portables d'un avocat ; et dans l'affaire *Reznik c. Ukraine*, 2025 (§§ 73-77), concernant des garanties procédurales insuffisantes pour assurer la protection des droits garantis par l'article 8 au requérant,

[8] Voir aussi le *Guide sur l'article 8 de la Convention - droit au respect de la vie privée et familiale* pour plus de détails sur les garanties de procédure applicables aux saisies opérées dans les cabinets d'avocat.

un avocat dont le domicile avait été perquisitionné dans le contexte d'une procédure pénale dirigée contre son client et dont les appareils de stockage des données avaient été saisis, puis examinés par des experts.

183. Dans l'affaire *Vinci Construction et GTM Génie Civil et Services c. France*, 2015 (§§ 69-81), la Cour a conclu à la violation de l'article 8 pour la fouille et les saisies de données informatiques de sociétés dont des messages électroniques relevant de la confidentialité s'attachant aux relations entre un avocat et son client. Le juge saisi, tout en envisageant la présence d'une correspondance émanant d'un avocat parmi les documents retenus par les enquêteurs, s'était contenté d'apprécier la régularité du cadre formel des saisies litigieuses, sans procéder à l'examen concret qui s'imposait.

184. Dans l'affaire *André et autres c. France*, 2008 (§§ 37-49), la visite domiciliaire et la saisie de documents dans un cabinet d'avocats par des agents du fisc en vue de découvrir des éléments à charge contre une société cliente de ce cabinet ont constitué une violation de l'article 8. La visite domiciliaire litigieuse avait pour but la découverte chez les requérants, en leur seule qualité d'avocats de la société soupçonnée de fraude, de documents susceptibles d'établir la fraude présumée de celle-ci et de les utiliser à charge contre elle. À aucun moment les requérants n'ont été accusés ou soupçonnés d'avoir commis une infraction ou participé à une fraude commise par leur cliente (*ibidem*, § 46).

185. Une nouvelle saisie, réalisée cinq minutes après la restitution de matériaux illégalement confisqués a constitué une violation de l'article 8 dans l'affaire *Visy c. Slovaquie*, 2018 (§§ 33-47). Le requérant n'avait pas pu bénéficier de garanties effectives contre l'arbitraire et les abus quant à la deuxième saisie.

186. En matière de terrorisme, dans l'affaire *Sher et autres c. Royaume-Uni*, 2015 (§§ 171-176), la Cour a été saisie de la question du mandat de perquisition étendu en cas de soupçons d'activité terroriste. À ses yeux, la complexité qui caractérise les affaires de ce type était apte à justifier une perquisition fondée sur des termes qui étaient plus larges que ceux qui sont d'ordinaire admissibles. Si l'on devait imposer, au titre de l'article 8, une obligation de décrire en détail dans un mandat de perquisition la nature exacte des éléments à rechercher et à saisir, on risquerait de gravement compromettre l'efficacité de l'enquête dans des cas où de nombreuses vies sont potentiellement menacées. Dans les affaires de cette nature, il y a lieu d'accorder une certaine latitude à la police pour apprécier, sur la base des éléments découverts au cours de la perquisition, lesquels de ceux-ci peuvent être liés à des activités terroristes et les saisir pour un plus ample examen (*ibidem*, § 74).

187. S'agissant du pouvoir, pour les autorités douanières, de consulter et de copier les données électroniques des particuliers, il a emporté, dans l'affaire *Ivashchenko c. Russie*, 2018 (§§ 59-95), une violation de l'article 8 en l'absence de soupçons raisonnables de méfaits. La fouille de l'ordinateur portable du requérant, la copie de ses données personnelles et professionnelles puis leur communication à des fins d'expertise, ainsi que la rétention de ces données pendant environ deux ans, ont excédé ce qui pourrait être considéré comme des procédures de « routine » peu intrusives et pour lesquelles le consentement est généralement donné. Le requérant n'a pas été en mesure de choisir s'il souhaitait se présenter à la douane avec ses biens, et s'exposer à leur éventuelle inspection. (Voir aussi l'affaire *Gillan et Quinton c. Royaume-Uni,* 2010, §§ 61-67, concernant le pouvoir d'arrêter et de fouiller des personnes sans raisons plausibles de les soupçonner d'avoir commis une infraction ayant constitué une violation de l'article 8. La Cour y précise que le caractère public de la fouille, impliquant la gêne occasionnée par le fait d'avoir des informations personnelles exposées à la vue d'autrui, peut même dans certains cas aggraver l'ingérence dans la vie privée de l'individu concerné en y ajoutant un élément d'humiliation et d'embarras. Le pouvoir discrétionnaire dont jouit chaque policier constitue un motif de préoccupation : non seulement celui-ci n'est pas tenu de démontrer l'existence d'un motif raisonnable de soupçonner une infraction, mais il n'est même pas obligé d'avoir le moindre soupçon subjectif à l'égard de la personne qui fait l'objet de l'interpellation et de la fouille).

ii. Acte médicaux obligatoires visant un prélèvement d'échantillons cellulaires

188. De façon générale, le recours aux divers actes médicaux obligatoires visant à faire prélever des échantillons cellulaires, tels que des échantillons de sang ou de salive, n'est pas interdit en tant que tel, dans le contexte de l'administration de la preuve dans les procédures civiles ou pénales (*Jalloh c. Allemagne* [GC], 2006, § 70 ; *Caruana c. Malte* (déc.), 2018, § 41 ; *D.H. et autres c. Macédoine du Nord*, 2023, § 52).

189. Dans l'affaire *D.H. et autres c. Macédoine du Nord*, 2023 (§§ 52-53), en particulier, la Cour a considéré que la décision de prélever des échantillons sanguins sur les requérantes, travailleuses du sexe, au motif qu'elles étaient soupçonnées de propager des maladies sexuellement transmissibles, était conforme aux exigences de l'article 8, l'acte médical ayant été ordonné par un juge et pratiqué par un docteur en médecine dans une clinique, et la requérante n'ayant à aucun moment allégué qu'elle avait été soumise dans ce cadre à un usage excessif de la force ou que l'acte en cause avait eu des effets délétères sur sa santé. Elle a donc rejeté le grief en question pour défaut manifeste de fondement.

190. Dans l'affaire *Mikulić c. Croatie*, 2002 (§ 64), la Cour a estimé que l'absence de moyens de nature à contraindre le père prétendu à se soumettre à un test ADN n'était conforme au principe de proportionnalité que si d'autres moyens étaient offerts grâce auxquels les intérêts du demandeur à l'action en recherche de paternité pouvaient être assurés. La Cour a constaté la violation de l'article 8 puisque de tels moyens faisaient défaut en droit interne, privant l'intéressée de voir mettre fin, sans délai inutile, à l'incertitude visant son identité personnelle face au refus de son père présumé de se soumettre à des tests ADN (*ibidem*, §§ 65-66).

191. Dans l'affaire *Mifsud c. Malte*, 2019 (§§ 61-78), l'injonction imposée au requérant, par les tribunaux nationaux, de subir un test génétique contre sa volonté, lors d'une procédure en reconnaissance de paternité, en application du droit maltais, n'était pas contraire à l'article 8. Avant d'ordonner à l'intéressé de se soumettre à un test ADN, les juridictions internes ont procédé à la nécessaire mise en balance des intérêts en présence, dans le cadre d'une procédure judiciaire à laquelle le requérant a participé, représenté par le conseil de son choix, et dans laquelle ses droits procéduraux ont été respectés tout autant que ceux de la partie adverse. Les juridictions nationales ont ainsi ménagé un juste équilibre entre l'intérêt, pour la fille putative du requérant, de faire établir un lien de paternité, et celui, pour le requérant, de ne pas subir un test ADN (*ibidem*, § 77). Dans l'ensemble, le processus décisionnel a été équitable et a dûment préservé les intérêts du requérant protégés par l'article 8.

192. Dans l'affaire *Boljević c. Serbie*, 2020 (§§ 50-56), le rejet pour prescription, par les juridictions nationales, d'une demande de réexamen d'une décision définitive rendue quarante et une années auparavant, ayant fait droit à l'action en désaveu de paternité d'un homme et alors que les tests ADN n'existaient pas, a été jugée par la Cour contraire à l'article 8. À ses yeux, le fait que les délais impartis dans le cadre de la procédure en reconnaissance de paternité visaient à protéger la sécurité juridique n'était pas une raison suffisante pour priver le requérant du droit de connaître la vérité sur un aspect important de son identité personnelle, sans mettre en balance les intérêts en jeu dans son cas. Le droit interne concernant les délais de réouverture des procédures n'a pas permis aux autorités de procéder à un tel exercice de mise en balance, tenant compte des circonstances très particulières de l'affaire du requérant, à savoir qu'il n'avait pris connaissance de la procédure en reconnaissance de paternité que lorsque la personne qu'il pensait être son père biologique était décédée. Pour la Cour, la vie privée d'une personne décédée ne pouvait pas, en tout état de cause, être affectée par une demande de prélèvement d'ADN. La Cour en avait décidé préalablement de même dans les affaires *Succession Kresten Filtenborg Mortensen c. Danemark* (déc.), 2006, concernant l'exhumation d'une dépouille aux fins d'examens génétiques et *Jäggi c. Suisse*, 2006 (§ 42), dans laquelle le refus des juridictions d'autoriser une expertise ADN sur un défunt demandée

par son fils présumé voulant établir avec certitude sa filiation avait constitué une violation de l'article 8 (*ibidem*, §§ 34-44).

193. Dans l'affaire *Caruana c. Malte* (déc.), 2018 (§§ 28-42), la Cour a déclaré manifestement mal fondé un grief tiré de l'obligation à laquelle l'épouse de l'auteur présumé d'un meurtre a été soumise de subir prélèvement buccal. À ses yeux, le prélèvement buccal constitue un acte d'une importance mineure qui ne cause en général ni lésion corporelle ni souffrance physique ou moral. Le meurtre étant une infraction grave, il était à la fois raisonnable et nécessaire de recueillir autant d'éléments que possible (*ibidem*, § 41). En outre, la Cour a distingué la situation d'un témoin de celle d'un accusé, dont le refus de se soumettre à pareille mesure dans le cadre d'une procédure pénale peut avoir une incidence sur une éventuelle déclaration de culpabilité et sur les sanctions qui y sont attachées (*ibidem*, § 40).

194. Dans l'affaire *Dragan Petrović c. Serbie*, 2020 (§§ 79-84), le prélèvement buccal dans le cadre d'une enquête pour meurtre a constitué une violation de l'article 8 en l'absence de dispositions légales prévisibles. Aussi, le fait que le requérant ait accepté de donner un échantillon de sa salive aux policiers était sans pertinence pour la question de savoir s'il avait subi ou non une ingérence dans sa vie privée, car il ne l'avait fait que sous la menace, en cas de refus, d'un prélèvement de sang coercitif (*ibidem*, § 79).

195. La Cour a aussi conclu à la violation de l'article 8 s'agissant d'une collecte des données médicales de témoins de Jehova qui avaient refusé des transfusions sanguines (*Avilkina et autres c. Russie*, 2013), voir aussi le paragraphe 188 ci-dessous du présent guide.

196. Le prélèvement d'organes à des fins de transplantation à l'insu et sans le consentement des proches parents de la personne décédée (*Petrova c. Lettonie*, 2014, §§ 87-98) et le manque de précision du droit national sur le consentement des parents proches à des prélèvements de tissus sur le corps d'une personne décédée (*Elberte c. Lettonie*, 2015, §§ 105-117) ont constitué des violations de l'article 8.

d. Collecte de données à caractère personnel dans le contexte de la santé

197. La Cour a eu à traiter de la question de la collecte des données sensibles dans le domaine de la santé. Dans l'affaire *L.H. c. Lettonie*, 2014 (§§ 47-60), la collecte de données médicales concernant une patiente d'un hôpital public par un organisme d'État (« l'organisme ») chargé de contrôler la qualité des soins médicaux n'a pas été jugé conforme à l'article 8, en l'absence de loi précisément formulée et protégeant contre l'arbitraire. L'organisme avait recueilli les données en question sur une période de sept ans, sans discernement et sans procéder à une évaluation préalable de la question de savoir si celles-ci seraient déterminantes, pertinentes ou importantes pour atteindre l'objectif poursuivi par l'enquête. L'organisme n'était pas tenu de demander et d'obtenir le consentement à la collecte des données de l'intéressé (*ibidem*, § 53). La portée des données privées, pouvant être recueillies, n'était pas limitée (*ibidem,* § 57). De plus, la pertinence et la suffisance des raisons de la collecte ne semblaient pas avoir été examinées par les juridictions nationales (*ibidem*, § 57). Dans ces circonstances, l'obligation légale de l'organisme de maintenir la confidentialité des données personnelles devenait, pour la Cour, moins pertinente (*ibidem*, § 58).

198. Dans l'affaire *Surikov c. Ukraine*, 2017 (§§ 75-95), la collecte et la conservation de données personnelles relatives à la santé mentale d'une personne pendant une très longue période ainsi que leur diffusion et utilisation à des fins dépourvues de lien avec les raisons ayant initialement motivé leur collecte ont constitué une atteinte disproportionnée dans le droit au respect de la vie privée du sujet des données en violation de l'article 8. Si les employeurs peuvent avoir un intérêt légitime à obtenir des informations sur la santé de leurs employés, en particulier dans le contexte de leur attribuer certaines fonctions liées à des aptitudes, responsabilités ou compétences spécifiques, la collecte et le traitement des informations pertinentes doivent être licites et de manière à établir un

juste équilibre entre les intérêts de l'employeur et les préoccupations du candidat pour le poste brigué quant au respect de sa vie privée (*ibidem*, § 91).

199. Dans l'affaire *Z c. Finlande*, 1997 (§§ 106-110), la Cour a conclu à la non-violation de l'article 8 relativement à la saisie des fichiers médicaux et leur adjonction au dossier d'enquête sans le consentement préalable de la patiente au cours de poursuites pénales intentées contre son mari. Le processus décisionnel n'avait donné lieu à aucune irrégularité et des recours étaient apparemment disponibles pour contester la saisie et annuler la limite de durée indiquée dans l'ordonnance relative à la confidentialité.

200. Dans l'affaire *Drelon c. France*, 2022 (§§ 79-100), le requérant avait tenté d'effectuer un don de sang dans un site de collecte de l'Établissement français du sang, lequel avait refusé sa candidature en raison de son homosexualité présumée. Même si le requérant avait refusé de répondre aux questions concernant sa sexualité qui lui avaient été posées au cours de l'entretien médical préalable au don, les données comprenaient une contre-indication propre aux hommes ayant eu un rapport sexuel avec un homme. Ayant pris note de leur nature sensible, la Cour a admis que la collecte et la conservation des données litigieuses reposaient sur des motifs pertinents et suffisants, à savoir la protection de la santé et la nécessité d'assurer la sécurité transfusionnelle. Dans le même temps, elle a noté que les données collectées reposaient sur de simples spéculations et non sur une base factuelle avérée. Elle a aussi relevé le caractère excessif de la durée de conservation des données, qui avait rendu possible l'utilisation de ces données de manière répétée à l'encontre du requérant, entraînant son exclusion automatique du don de sang. Au vu de ces éléments, la Cour a conclu à la violation de l'article 8 de la Convention.

e. Transmission obligatoire de données à caractère personnel

201. L'obligation, pesant sur les opérateurs de téléphonie mobile, les fournisseurs des services Internet, les établissements bancaires, les sportifs de haut niveau, les hôpitaux de transmettre aux autorités les données à caractère personnel en leur possession en vertu d'une loi ou d'un ordre des autorités a été examinée par la Cour dans un certain nombre d'affaires.

202. Lorsqu'il s'agit de lutter contre le crime organisé et le terrorisme, la Cour a admis que les méthodes d'enquête devaient être adaptées aux moyens de communication modernes. Dans l'affaire *Breyer c. Allemagne*, 2020 (§§ 81-110), l'obligation légale pour les opérateurs de téléphonie mobile de recueillir des données personnelles des utilisateurs de cartes SIM prépayées et de les tenir à la disposition des autorités, en vertu d'une loi sur les télécommunications autorisant diverses autorités publiques à demander l'extraction et la transmission de ces données sans avoir à disposer d'une décision de justice ou à en notifier les personnes concernées, n'a pas été jugée contraire à l'article 8. La conservation des données ne concernait qu'un ensemble restreint de données et aucune donnée concernant des communications particulières n'était conservée ; ainsi l'ingérence a été relativement limitée (*ibidem*, §§ 92-95). Il existait en outre certaines garanties : l'assurance de sécurité technique, une durée de conservation limitée, des données se bornant aux informations nécessaires pour identifier clairement l'abonné concerné ; des possibilités de consultation et d'utilisation futures des données conservées encadrées ; une surveillance par une autorité indépendante ; et la possibilité ouverte à quiconque estimait que ses droits avaient été violés d'interjeter appel, même si le niveau d'examen et de contrôle n'était pas un élément déterminant, dans l'appréciation de la proportionnalité de la collecte et de la conservation de l'ensemble limité de données ici en cause (*ibidem*, §§ 96-107).

203. En revanche, la Cour a estimé que la mise en œuvre d'une obligation légale imposant aux fournisseurs de services Internet d'extraire les données de connexion conservées de l'un de leurs abonnés et de les transmettre à la police a emporté une violation de l'article 8 car les dispositions juridiques utilisées par la police manquaient de clarté et n'offraient aucune protection contre une

ingérence arbitraire, en l'absence notamment de surveillance indépendante des pouvoirs de police en jeu (*Benedik c. Slovénie*, 2018, §§ 132-134).

204. Dans l'affaire *Sommer c. Allemagne*, 2017 (§ 63), l'inspection du compte bancaire d'un avocat a emporté une violation l'article 8 vu le seuil peu élevé pour cette inspection, l'étendue des demandes de renseignements, la divulgation ultérieure, le stockage continu des renseignements personnels et l'insuffisance des garanties procédurales.

205. S'agissant d'une collecte des données médicales des témoins de Jehova qui avaient refusé des transfusions sanguines, la Cour a estimé, dans l'affaire *Avilkina et autres c. Russie*, 2013 (§ 54), que la collecte par le parquet de données sur les requérants auprès des établissements médicaux qui les avaient pris en charge, sans en informer les sujets des données et sans leur donner la possibilité de s'y opposer, a été contraire à l'article 8. Pour donner suite aux plaintes qu'il avait reçues contre l'organisation religieuse en question, le parquet disposait d'autres moyens tels que d'interroger les individus concernés ou de solliciter leur consentement (*ibidem*, § 48).

206. Dans l'affaire *Fédération nationale des associations et syndicats de sportifs (FNASS) et autres c. France*, 2018 (§§ 155-191), l'obligation légale imposée aux sportifs de haut niveau, inscrits dans un « groupe cible », de fournir à l'avance leur localisation afin de procéder à des contrôles inopinés pour lutter contre le dopage sous peine de sanction en cas de trois manquements pendant une période de dix-huit mois consécutifs n'a pas été jugée contraire à l'article 8. Sans sous-estimer l'impact que les obligations de localisation ont sur la vie privée des requérants, la Cour a estimé que réduire ou supprimer les obligations imposées aux sportifs de haut niveau serait de nature à accroître les dangers du dopage pour leur santé et pour la santé de toute la communauté sportive, et irait à l'encontre de la communauté de vue européenne et internationale sur la nécessité d'opérer des contrôles inopinés (*ibidem*, § 191).

207. Dans l'affaire *Aycaguer c. France*, 2017 (§§ 45-47), la Cour a conclu à la violation de l'article 8 car la condamnation pénale du requérant, pour avoir refusé de se soumettre au prélèvement biologique obligatoire destiné à l'enregistrement de son profil ADN dans le fichier national automatisé des personnes condamnées, ne pouvait pas passer pour une mesure nécessaire dans une société démocratique. Les agissements du requérant ayant donné lieu à une obligation de se soumettre à un prélèvement biologique obligatoire s'inscrivaient dans un contexte politique et syndical, et concernaient de simples coups de parapluie en direction de gendarmes restés non identifiés, pour lesquels il s'était vu condamnés à deux mois d'emprisonnement avec sursis. Or, aucune différenciation n'avait été prévue dans le système national automatisé des empreintes génétiques en fonction de la nature et de la gravité de l'infraction commise, malgré l'importante disparité des situations susceptibles de se présenter, comme celle du requérant en attestait (*ibidem*, § 43). Enfin le requérant n'avait pas eu accès à une procédure d'effacement des données mémorisées (procédure prévue uniquement pour les personnes soupçonnées, et non pour celles ayant été condamnées) (*ibidem*, § 43).

2. Conservation des données à caractère personnel

208. La mémorisation par une autorité publique de données relatives à la vie privée d'un individu, quelle que soit la manière dont celles-ci ont été obtenues, constitue une ingérence dans le droit au respect de la vie privée du sujet des données, au sens de l'article 8, que ces données aient été utilisées par la suite ou non (*Amman c. Suisse* [GC], 2000, § 69 ; *Rotaru c. Roumanie* [GC], 2000, § 46 ; *S. et Marper c. Royaume-Uni* [GC], 2008, § 67 ; *M.K. c. France,* 2013, § 29 ; *Aycaguer c. France,* 2017 § 33). Compte tenu du caractère intrinsèquement privé de ces informations, la Cour se doit de procéder à un examen rigoureux de toute mesure prise par un État pour autoriser leur conservation par les autorités sans le consentement de la personne concernée (*S. et Marper c. Royaume-Uni* [GC], 2008, § 104).

a. Le fichage à des fins de lutte contre la criminalité

209. L'intérêt des personnes concernées et de la collectivité dans son ensemble à voir protéger les données à caractère personnel peut s'effacer devant l'intérêt légitime que constitue la prévention des infractions pénales (*S. et Marper c. Royaume-Uni* [GC], 2008, § 104). Pour protéger leur population comme elles en ont le devoir, les autorités nationales sont amenées à constituer des fichiers contribuant efficacement à la répression et à la prévention de certaines infractions, notamment les plus graves, comme celles de nature sexuelle (*B.B. c. France*, 2009, § 62 ; *Gardel c. France*, 2009, § 63 ; *M.B. c. France,* 2009, § 54 ; *N.F. et autres c. Russie*, 2023, § 44). Alors que le prélèvement initial des données personnelles est destiné à relier une personne donnée à l'infraction particulière qu'elle est soupçonnée avoir commise, la conservation de ces données dans des fichiers et des bases de données tend à un objectif plus large, à savoir contribuer à l'identification des futurs délinquants (*S. et Marper c. Royaume-Uni* [GC], 2008, § 100). La Cour ne saurait mettre en doute les objectifs de prévention de tels fichiers (*Gardel c. France*, 2009, § 63 ; *B.B. c. France*, 2009, § 62 ; *M.B. c. France,* 2009, § 54). La lutte contre la criminalité, et notamment contre le crime organisé et le terrorisme, qui constitue l'un des défis auxquels les sociétés européennes doivent faire face à l'heure actuelle, dépend dans une large mesure de l'utilisation des techniques scientifiques modernes d'enquête et d'identification (*S. et Marper c. Royaume-Uni* [GC], 2008, § 105). En même temps, puisque 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, il est essentiel que la législation interne ménage des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article (*ibidem*, § 103 ; *Glukhin c. Russie*, 2023, § 75).

210. La Cour a examiné une série d'affaires relatives à la conservation dans des fichiers destinés à la répression et à la prévention de la criminalité des données personnelles des individus qui avaient été condamnés pour des infractions mineures (*M.K. c. France*, 2013, §§ 6, 8, 41 ; *Aycaguer c. France*, 2017, §§ 8, 43), graves (*B.B. c. France*, 2009, §§ 6, 62 ; *Gardel c. France*, 2009, §§ 8, 9, 63 ; *M.B. c. France,* 2009, §§ 6, 54 ; *Peruzzo et Martens c. Allemagne* (déc.), 2013, §§ 6, 12, 37-38 ; *Trajkovski et Chipovski c. Macédoine du Nord*, 2020, §§ 6, 12), ou pour une série d'infractions qui n'étaient ni mineures ni particulièrement graves (*P.N. c. Allemagne*, 2020, §§ 6, 81). D'autres affaires portent sur la conservation dans des fichiers destinés à la répression et à la prévention de la criminalité des données personnelles des individus qui avaient été soupçonnés d'avoir commis une infraction, mais qui ont finalement été relaxés (*S. et Marper c. Royaume-Uni* [GC], 2007, §§ 10, 11, 113 ; *M.K. c. France*, 2013, §§ 7, 9, 42 ; *Brunet c. France*, 2014, §§ 6, 7, 40), acquittés (*S. et Marper c. Royaume-Uni* [GC], 2008, §§ 10, 113), ou simplement mis en garde à l'issue de la procédure, sans qu'aucune décision de condamnation n'ait été prise à leur encontre (*M.M. c. Royaume-Uni*, 2012, §§ 7-9). Dans une affaire, les données à caractère personnel concernant les requérants avaient été recueillies et conservées dans une base de données du ministère de l'Intérieur au seul motif que les intéressés avaient en différentes occasions fait l'objet de poursuites pénales. Étaient consignés dans le système d'enregistrement en question non seulement les condamnations pénales - indépendamment de la nature et de la gravité des infractions en question, et même lorsque les condamnations avaient été levées ou effacées - mais aussi les cas où un individu avait fait l'objet de poursuites pénales et où la procédure pénale avait par la suite été abandonnée pour des « motifs non disculpatoires » (*N.F. et autres c. Russie*, 2023, § 49). D'autres affaires portent, enfin, sur des mesures de nature préventive de mémorisation des données personnelles dans les fichiers de la police, sur la base de simples suspicions (*Shimovolos c. Russie*, 2011, § 16 ; *Khelili c. Suisse*, 2011, §§ 8, 9, 59 ; *Catt c. Royaume-Uni*, 2019, §§ 6, 14, 119).

211. Les éléments suivants sont importants dans l'examen de la nécessité d'une mesure de stockage des données à caractère personnel à des fins policières.

i. Caractère indiscriminé et indifférencié des données stockées

212. Dans plusieurs affaires, la Cour a mis en cause la portée large des dispositifs de fichage mis en place par les autorités, qui ne distinguaient pas selon la nature ou le niveau de gravité de l'infraction qui avait donné lieu à une condamnation (*M.K. c. France*, 2013, § 41 ; *Aycaguer c. France,* 2017, § 43 ; *Gaughran c. Royaume-Uni*, 2020, § 94 ; *N.F. et autres c. Russie*, 2023, § 49), ou selon que le sujet des données avait été condamné, acquitté, relaxé ou sous le coup d'une simple mise en garde, après avoir été soupçonné d'avoir commis une infraction (*S. et Marper c. Royaume-Uni* [GC], 2008, § 119 ; *M.M. c. Royaume-Uni*, 2012, § 198 ; *M.K. c. France*, 2013, § 42 *; Brunet c. France*, 2014, § 41 ; *N.F. et autres c. Russie*, 2023, § 49). Pour la Cour, les dispositifs mis en place par les autorités pour contribuer à la répression et à la prévention de certaines infractions ne sauraient être mis en œuvre dans une logique excessive de maximalisation des informations qui y sont placées. Sans le respect d'une nécessaire proportionnalité au regard des objectifs légitimes qui leur sont attribués, les avantages qu'ils apportent seraient obérés par les atteintes graves qu'ils causeraient aux droits et libertés que les États doivent assurer en vertu de la Convention aux personnes placées sous leur juridiction (*M.K. c. France,* 2013, § 35 ; *Aycaguer c. France,* 2017, § 34).

213. Dans l'affaire *S. et Marper c. Royaume-Uni* [GC], 2008 (§§ 119, 125), un système de fichage où il était possible de prélever et de conserver, des empreintes digitales, échantillons biologiques et profils ADN chez toute personne soupçonnée d'avoir commis des infractions pénales mais non condamnée, quel que soit son âge, la nature et la gravité des infractions, sans limitation de durée, et sans contrôle indépendant de la justification de la conservation sur la base de critères précis, a emporté un constat de violation de l'article 8. Le caractère général et indifférencié d'un tel système ne traduisait pas un juste équilibre entre les intérêts publics et privés concurrents en jeu.

214. Il existe un risque de stigmatisation lorsque les personnes, reconnues coupables d'aucune infraction et en droit de bénéficier de la présomption d'innocence, sont traitées de la même manière que des condamnés (*S. et Marper c. Royaume-Uni* [GC], 2008, § 122). Même si la conservation de données privées concernant les individus soupçonnés d'une infraction mais acquittés ou relaxés n'équivaut pas à l'expression de soupçons, l'impression qu'ils ont de ne pas être considérés comme innocents peut se trouver renforcée si les données les concernant sont conservées indéfiniment tout comme celles relatives à des personnes condamnées, alors que celles concernant des individus n'ayant jamais été soupçonnés d'une infraction doivent être détruites (*ibidem*, § 122). Donc, le fait qu'un individu a bénéficié d'une relaxe après avoir été soupçonné d'avoir commis une infraction justifie qu'il reçoive un traitement différent de celui réservé à une personne condamnée (*ibidem*, § 122 ; voir aussi dans la même sens *M.K. c. France*, 2013, § 42 ; *Brunet c. France*, 2014, § 40). Ainsi, dans l'affaire *Brunet c. France*, 2014 (§ 40), où le requérant avait bénéficié d'un classement sans suite après avoir eu recours à une médiation, la Cour a mis en cause le caractère indifférencié des données personnelles recueillies dans le fichier des autorités, sans distinction entre les individus condamnés et ceux dont les poursuites avaient été classées sans suite. Dans l'affaire *Aycaguer c. France,* 2017 (§§ 42-43), où les données à caractère personnel avaient été recueillies et conservées suite à une condamnation pour des faits qui ne présentaient aucune gravité particulière, la Cour a mis en cause la portée large du dispositif de fichage mis en place par les autorités, qui ne distinguait pas selon le degré de gravité de l'infraction ayant entraîné une condamnation, et ce nonobstant l'importante disparité des situations susceptibles de se présenter dans le champ d'application de la loi. Pour la Cour, les agissements reprochés au requérant, de simples coups de parapluie donnés en direction de gendarmes dans un contexte politique et syndical, n'étaient pas comparables avec des faits susceptibles de relever des infractions particulièrement graves, telles des infractions sexuelles, du terrorisme ou encore des crimes contre l'humanité ou de la traite des êtres humains.

215. Dans l'affaire *M.M. c. Royaume-Uni*, 2012 (§§ 187-207), l'inscription à vie d'un avertissement dans le casier judiciaire d'une personne après qu'elle ait disparu pendant une journée avec son petit-fils, un nourrisson, voulant empêcher son départ pour l'Australie à la suite de l'échec du

mariage de son fils, a emporté un constat de violation de l'article 8. La Cour a mis en cause le champ particulièrement vaste d'application du système de conservation des données, qui couvrait non seulement les condamnations, mais aussi les décisions sans condamnation telles que les mises en garde, les avertissements, les réprimandes ainsi qu'une quantité importante de données supplémentaires enregistrées par les forces de police en vertu d'une présomption générale en faveur de la conservation jusqu'à ce que la personne concernée ait atteint l'âge de cent ans (*ibidem*, § 202). À ses yeux, plus la portée du système de collecte et de conservation des données à caractère personnel est grande, et donc plus la quantité et la sensibilité des données détenues et disponibles pour la divulgation sont importantes, plus le contenu des garanties à appliquer aux différentes étapes cruciales du traitement ultérieur des données est important (*ibidem*, § 200). Il en a été de même dans l'affaire *Gaughran c. Royaume-Uni,* 2020 (§§ 94-97), au sujet de la conservation illimitée des données biométriques et des photographies du requérant condamné pour conduite en état d'ébriété qui a emporté une violation de l'article 8.

216. L'affaire *N.F. et autres c. Russie*, 2023 (§§ 49-55), concernait un système de stockage de données dans lequel des informations relatives aux procédures pénales étaient automatiquement recueillies et stockées dès lors qu'un individu avait fait l'objet de poursuites pénales. Étaient conservées dans cette base de données des informations relatives à toutes les condamnations pénales, éteintes ou non, indépendamment de la nature et de la gravité de l'infraction commise, ainsi que des informations sur les procédures pénales ayant été abandonnées pour des « motifs non disculpatoires ». La Cour a jugé excessives la portée et l'application de ce système. Elle a en outre considéré que la poursuite du traitement des données était particulièrement intrusive pour les personnes qui n'avaient été reconnues coupables d'aucune infraction pénale. Elle a également estimé que l'ingérence dans la vie privée des personnes condamnées atteignait un niveau élevé une fois leur condamnation effacée ou levée par un tribunal. Elle a jugé que faute de garanties suffisantes contre les abus et d'une possibilité de contrôle, pareil traitement était disproportionné.

217. La conservation de données relatives à des personnes non condamnées peut être particulièrement préjudiciable dans le cas de mineurs, en raison de leur situation spéciale et de l'importance que revêt leur développement et leur intégration dans la société. Il faut veiller avec un soin particulier à les protéger de tout préjudice de ce type (*S. et Marper c. Royaume-Uni* [GC], 2008, § 124).

ii. Durée du stockage des données

218. La durée pendant laquelle les autorités choisissent de conserver les données personnelles d'un individu est un élément important, quoique non décisif, à prendre en compte pour examiner si une mesure de conservation des données personnelles dans un fichier ou une base de données à des fins policières est proportionnée, ou non, au but légitime poursuivi. La Cour est parvenue à un constat de violation de l'article 8 dans les contextes :

- d'une conservation illimitée des empreintes digitales et données ADN des personnes soupçonnées d'avoir commis une infraction, mais à l'égard desquelles les procédures se sont terminées par une décision de classement sans suite ou d'acquittement (*S. et Marper c. Royaume-Uni* [GC], 2008) ;
- de la conservation illimitée des profils ADN, empreintes digitales et photographie d'un individu reconnu coupable d'une infraction, même après que sa condamnation ait été rayée de son casier judiciaire à l'expiration du délai prévu par la loi (*Gaughran c. Royaume-Uni*, 2020) ;
- de la conservation à vie dans un casier judiciaire de toutes les condamnations, acquittements, mises en garde, avertissements ou réprimandes d'un individu (*M.M. c. Royaume-Uni*, 2012) ;

- d'une conservation illimitée des profils ADN des personnes condamnées pour vols aggravés (*Trajkovski et Chipovski c. Macédoine du Nord*, 2020).
- de la conservation pour une durée maximale de quarante ans des données personnelles d'un individu condamné pour une infraction sans gravité particulière (*Ayçaguer c. France*, 2017) ;
- de la conservation pour une durée maximale de vingt-cinq ans des empreintes digitales d'un individu soupçonné d'avoir commis un vol de livres, mais non condamné (*M. K. c. France*, 2013) ;
- de la conservation pour une durée maximale de vingt ans des données personnelles d'un individu suite à une plainte pour violence sur sa compagne, classée sans suite à la suite d'une médiation (*Brunet c. France*, 2014).
- de la conservation, sans limitation de durée, de données relatives à la sanction administrative de substitution infligée au requérant (*Borislav Tonchev c. Bulgarie*, 2024).

219. En revanche, la Cour est parvenue au constat de non-violation de l'article 8 dans plusieurs affaires qui portaient sur la conservation des données personnelles, d'individus condamnés pour agressions sexuelles, pour une durée maximale de trente ans à l'issue de laquelle l'effacement des données intervenait automatiquement car des procédures avaient été mise en place pour permettre l'effacement des données dès qu'elles n'étaient plus pertinentes (*B.B. c. France*, 2009, § 67 ; *Gardel c. France*, 2009, § 69 ; *M.B. c. France,* 2009, § 59). La Cour a également déclaré manifestement mal fondée une affaire relative à la conservation, sans limitation de durée, des données personnelles de personnes condamnées pour des infractions graves, assortie de contrôles à intervalles réguliers qui ne devaient pas dépasser dix ans, susceptibles de déterminer si le maintien du stockage des données était toujours nécessaire (*Peruzzo et Martens c. Allemagne* (déc.), 2013, §§ 44-49). Et dans l'affaire *P.N. c. Allemagne*, 2020 (§§ 87-90), la Cour a conclu à la non-violation de l'article 8 s'agissant de la conservation pendant cinq ans, subordonnée à des garanties et à un contrôle individualisé, des données d'un récidiviste destinées à l'identifier à la suite de l'ouverture d'une nouvelle procédure pénale à son encontre.

220. L'élément déterminant quand il s'agit de rechercher si un État a outrepassé sa marge d'appréciation lorsqu'il décide de conserver sans limitation de durée des données personnelles de personnes reconnues coupables d'une infraction n'est pas la durée de conservation des données, mais le fait de savoir si des garanties effectives ont été mises en place (*Gaughran c. Royaume-Uni*, 2020, § 88). Dès lors qu'il décide de s'accorder à lui-même le pouvoir le plus étendu en matière de conservation des données, à savoir celui de les conserver sans limitation de durée, l'État se place à la limite de sa marge d'appréciation et doit veiller à l'existence de certaines garanties effectives (*ibidem*, § 88). L'existence, ou non, d'un contrôle indépendant de la justification de leur maintien dans le système de fichage, exercé sur la base de critères précis tels la gravité de l'infraction, la force des soupçons pesant sur la personne, ses antécédents, ou toute autre circonstance particulière, est une garantie importante pour veiller au caractère proportionné de la durée de conservation des données (*ibidem*, § 94 ; *S. et Marper c. Royaume-Uni* [GC], 2008, § 119 ; *B.B. c. France*, 2009, § 68 ; *Gardel c. France*, 2009, § 69 ; *M.B. c. France,* 2009, § 60).

221. L'absence d'une période maximum pour la conservation des données personnelles n'est pas nécessairement incompatible avec l'article 8 (*Peruzzo et Martens c. Allemagne* (déc.), 2013, § 46 ; *Gaughran c. Royaume-Uni*, 2020, § 88), mais les garanties procédurales sont d'autant plus nécessaires là où la mémorisation des données dépend entièrement de la diligence avec laquelle les autorités veillent au caractère proportionné de la durée de leur conservation (*Peruzzo et Martens c. Allemagne* (déc.), 2013, § 46 ; *Ayçaguer c. France*, 2017, § 38).

222. Dans l'affaire *Peruzzo et Martens c. Allemagne* (déc.), 2013 (§ 44), relative à la conservation illimitée des données biométriques des personnes condamnées pour des infraction graves et susceptibles d'être répétées, la Cour a été satisfaite de constater que le droit interne obligeait

l'Office fédéral de la criminalité de vérifier à des intervalles réguliers, ne dépassant pas dix ans, si le maintien de la conservation des données était encore nécessaire ou si les données pouvaient être supprimées, en tenant compte dans chaque cas de la finalité pour laquelle les données ont été conservées ainsi que de la nature et de la gravité des circonstances de chaque affaire ayant donné lieu à un mesure de fichage (*ibidem*, § 46). Pour la Cour, la durée de telles intervalles n'était pas déraisonnable compte tenu du fait que les profils ADN ne pouvaient être obtenus que de condamnés ayant commis des infractions atteignant un certain niveau de gravité (*ibidem*, §§ 48-49).

223. Dans l'affaire *Gaughran c. Royaume-Uni*, 2020 (§ 96), la conservation sans limitation de durée, des empreintes digitales, profil ADN et photographie, d'un individu reconnu coupable de conduite en état d'ivresse a emporté un constat de violation de l'article 8. Les autorités n'avaient pas tenu compte de la gravité de l'infraction commise ou de la nécessité persistante de conserver ces données indéfiniment, et elles n'offraient pas une réelle possibilité de réexamen (*ibidem*, § 96).

224. Une période maximale de mémorisation des données à caractère personnel prévue par le droit interne peut être, en pratique, assimilable à une norme, plutôt qu'à un maximum si les chances de succès d'une demande d'effacement avant l'échéance du délai fixé par la loi sont hypothétiques (*M. K. c. France*, 2013, §§ 44-47 ; *Brunet c. France*, 2014, §§ 41-45 ; *Ayçaguer c. France*, 2017, §§ 44-46). La Cour a conclu à la violation de l'article 8 dans plusieurs affaires où le système national prévoyait des périodes maximales de mémorisation de vingt ou vingt-cinq ans pour des faits classés sans suite (*M. K. c. France*, 2013, §§ 44-47 ; *Brunet c. France*, 2014, §§ 41-45), voire une période maximale de mémorisation de quarante ans pour des faits sans aucune gravité particulière qui avaient donné lieu à une décision de condamnation (*Ayçaguer c. France*, 2017, § 42).

225. Dans l'affaire *Catt c. Royaume-Uni*, 2019 (§ 120), la conservation dans une base de données de la police relative à l'extrémisme national pendant au moins six ans, date à laquelle elles seraient soumises à un examen planifié, des données à caractère personnel du requérant a emporté un constat de violation de l'article 8. Le requérant dépendait entièrement de la diligence avec laquelle les autorités appliqueraient les garanties du code de pratique applicable, très souples par nature, pour veiller au caractère proportionné de la durée de conservation de ses données. L'absence de garanties permettant la suppression des données, dès que la poursuite de leur conservation devient disproportionnée, est particulièrement préoccupante lorsqu'il s'agit de conserver sans limitation de durée des données révélant des opinions politiques, qui bénéficient d'un niveau de protection accru (*ibidem*, §§ 122-123).

226. Les conséquences des changements de politique, concernant la durée de conservation des données personnelles dans un casier judiciaire, sur les perspectives d'emploi du sujet des données sont examinées dans l'affaire *M.M. c. Royaume-Uni*, 2012 (§ 204). Aux yeux de la Cour, il est peu probable que la conservation indifférenciée et inconditionnée de toutes les condamnations, acquittements, mises en garde, avertissements et réprimandes d'un individu soit conforme aux exigences de l'article 8 en l'absence de dispositions légales claires et détaillées précisant les garanties applicables et exposant les règles régissant, entre autres, la durée de leur conservation (*ibidem*, § 199).

227. Voir aussi, dans un contexte différent, la question de la limitation à dix ans, ordonnée par un tribunal, du délai de confidentialité des pièces produites au procès contenant des données médicales de nature à dévoiler l'identité et la séropositivité d'une personne dans l'affaire *Z c. Finlande*, 1997 (§§ 111-113). En l'occurrence, le délai de confidentialité de dix ans ne correspondait pas aux souhaits ou aux intérêts des parties au procès, et la production, sans le consentement de la requérante, des informations dont il s'agissait avait déjà entraîné une grave ingérence dans sa vie privée et familiale. Le surcroît d'ingérence qu'elle subirait si les renseignements et éléments en question devaient tomber dans le domaine public au bout de dix ans ne s'appuyait pas sur des motifs impérieux.

iii. Garanties visant la destruction ou l'effacement des données stockées[9]

228. Pour la Cour, la suppression des données d'une base où elles ont été recueillies à des fins policières n'est pas une tâche d'une complexité excessive (*Catt c. Royaume-Uni*, 2019, § 127). Il serait totalement contraire à la nécessité de protéger le droit à la vie privée consacré par l'article 8 qu'un État puisse créer une base de données dans laquelle il serait difficile d'examiner ou de modifier les données, puis qu'il puisse invoquer la manière dont cette base de données a été conçue pour justifier son refus de supprimer des informations y figurant (*ibidem*, § 127).

229. L'existence au niveau national d'une procédure judiciaire d'effacement des données capable d'assurer un contrôle indépendant de la justification de leur conservation sur la base de critères précis et présentant des garanties suffisantes et adéquates du respect de la vie privée du sujet des données est un élément important dans la mise en balance des différents intérêts en jeu (*S. et Marper c. Royaume-Uni* [GC], 2008, § 119 ; *Gardel c. France*, 2009, § 69).

230. La Cour est parvenue à un constat de non-violation de l'article 8 dans des affaires où, bien qu'il s'agissait de mémorisation des données pour de « longues » périodes, jusqu'à trente ans (*B.B. c. France*, 2009, §§ 66, 68 ; *Gardel c. France*, 2009, §§ 67, 69 ; *M.B. c. France,* 2009, §§ 58, 60) voire pour des périodes illimitées (*Peruzzo et Martens c. Allemagne* (déc.), 2013, § 46), le sujet des données avait bénéficié d'une procédure judiciaire assurant un contrôle indépendant de la justification de la conservation de ses données sur la base de critères précis, lui permettant d'obtenir l'effacement des données avant l'échéance maximale prévue par la loi ou, s'agissant d'une conservation illimitée, dès qu'elle n'était plus pertinente (voir, *a contrario*, *S. et Marper c. Royaume-Uni* [GC], 2008, § 119).

231. Ainsi, dans les affaires *B.B. c. France*, 2009 (§ 68), *Gardel c. France*, 2009 (§ 69), et *M.B. c. France,* 2009 (§ 60), la Cour a jugé que la procédure judiciaire d'effacement des données, ouverte sur simple demande du sujet des donnés auprès du procureur de la République, dont la décision était susceptible de recours juridictionnels, assurait un contrôle indépendant de la justification de la conservation des informations sur la base de critères précis et présentait des garanties suffisantes et adéquates. Voir aussi le paragraphe 204 ci-dessus du présent guide s'agissant de l'affaire *Peruzzo et Martens c. Allemagne* (déc.), 2013 (§ 44).

232. Dans l'affaire *P.N. c. Allemagne*, 2020 (§§ 81, 88), concernant la conservation des données personnelles d'un délinquant adulte dont les infractions n'étaient ni mineures ni particulièrement graves, la règle qui voulait que ces données soient supprimées au bout de cinq ans, en l'absence d'ouverture d'une nouvelle enquête pénale visant le sujet des données dans ce délai, n'a pas été jugé contraire à l'article 8. La nécessité de conserver les données en question dans les fichiers de police pouvait faire l'objet d'un réexamen par celle-ci, susceptible de contrôle juridictionnel, et le requérant pouvait ainsi obtenir la suppression de ses données si son comportement démontrait que les données n'étaient plus nécessaires au travail de la police (*ibidem*, § 88).

233. L'absence de garanties effectives pour obtenir l'effacement des données personnelles lorsqu'elles n'apparaissent plus pertinentes au regard de la finalité du fichier est particulièrement préoccupante s'agissant des catégories sensibles des données personnelles conservées, qui appellent une protection accrue (*Catt c. Royaume-Uni*, 2019, § 123).

234. La possibilité prévue en droit interne d'obtenir l'effacement des données s'avère une garantie « théorique et illusoire » et non « concrète et effective » lorsque le droit de présenter à tout moment une demande d'effacement de ces données au juge risque de se heurter à l'intérêt des services d'enquêtes de disposer d'un fichier ayant le plus de références possibles, et si les intérêts en présence sont, ne serait-ce que partiellement, contradictoires (*M.K. c. France,* 2013, § 44). La

[9] Voir aussi la partie ci-dessous du présent guide sur le « Droit à l'effacement ».

garantie d'obtenir l'effacement des données a également un effet limité dans le cas où les autorités refusent, suite à une demande du sujet des données, de supprimer les données concernées ou de motiver leur décision de les conserver (*Catt c. Royaume-Uni*, 2019, § 122). Il en est de même lorsque des demandes de suppression ne sont accordées que dans des circonstances exceptionnelles, ou sont écartées lorsque le sujet des données avait reconnu l'infraction et le fait que les données étaient exactes (*M.M. c. Royaume-Uni*, 2012, § 202).

235. Pour la Cour, les individus à l'égard desquels une décision de condamnation a été prise devraient également, à l'instar des personnes acquittées ou relaxées, se voir offrir une possibilité concrète de présenter une requête en effacement de leurs données stockés dans les fichiers des autorités (*B.B. c. France*, 2009, § 68 ; *Brunet c. France*, 2014, §§ 41-43 ; *Ayçaguer c. France*, 2017, § 44). Dans l'affaire *Ayçaguer c. France*, 2017 (§ 44), où une procédure d'effacement n'avait été mise en place que pour les personnes soupçonnées d'avoir commis une infraction, et non pour celles qui ont été condamnées, la Cour est parvenue à un constat de violation de l'article 8. À ses yeux, le régime de conservation des profils ADN dans le fichier national des infractions n'offrait pas, en raison tant de sa durée que de l'absence de possibilité d'effacement, un juste équilibre entre les intérêts publics et privés concurrents en jeu (*ibidem*, § 45).

236. Dans l'affaire *Khelili c. Suisse*, 2011 (§§ 68-70), la Cour a conclu à la violation de l'article 8 après avoir souligné les incertitudes et les difficultés auxquelles l'intéressée s'était heurtée en cherchant à obtenir l'effacement de la mention « prostituée » du dossier de police censée représenter sa profession, alors qu'elle n'avait jamais été condamnée pour exercice illicite de la prostitution. La Cour nota qu'il n'avait pas été allégué que la suppression de la mention litigieuse du dossier de police aurait été impossible ou difficile pour des raisons techniques (*ibidem*, § 68).

iv. Garanties destinées à réglementer l'accès des tiers et à préserver l'intégrité et la confidentialité des données

237. La Cour a examiné dans plusieurs affaires la question de savoir si le droit interne contenait, ou non, des garanties aptes à protéger efficacement les données à caractère personnel mémorisées dans les fichiers des autorités contre des usages impropres et abusifs (*S. et Marper c. Royaume-Uni* [GC], 2008, § 103 ; *B.B. c. France*, 2009, § 61 ; *Gardel c. France*, 2009 § 62 ; *M.M. c. Royaume-Uni*, 2012, § 195 ; *M.K. c. France,* 2013, § 35 ; *Brunet c. France*, 2014, § 35 ; *Ayçaguer c. France*, 2017, § 38). Elle a constaté l'existence de telles garanties lorsque, par exemple,

- la consultation des données recueillies dans le fichier étaient exclusivement accessible à des autorités astreintes à une obligation de confidentialité (*B.B. c. France*, 2009, § 69 ; *Peruzzo et Martens c. Allemagne* (déc.), 2013, § 47) ;
- les données mémorisées obéissaient à des modalités de consultation suffisamment encadrées, régissant les personnes habilitées à consulter le fichier (*M.K. c. France,* 2013, § 37 ; voir, *a contrario*, *Khelili c. Suisse*, 2011, § 64) ;
- l'identité de la personne dont l'échantillon d'ADN avait été prélevé n'était pas divulguée aux experts chargés d'établir le profil ADN, qui étaient en outre tenus de prendre des mesures adéquates afin d'empêcher toute utilisation non autorisée du matériel cellulaire examiné (*Peruzzo et Martens c. Allemagne* (déc.), 2013, § 45) ; le matériel cellulaire devait être détruit sans délai une fois qu'il n'était plus nécessaire pour établir le profil ADN et seuls les profils ADN extraits de ce matériel cellulaire pouvaient être conservés dans la base de données de l'Office fédéral de la police criminelle (*ibidem*, § 45) ; et les profils ADN retenus ne pouvaient être communiqués aux autorités compétentes qu'à des fins clairement circonscrites, visant la prévention de dangers et l'assistance judiciaire internationale (*ibidem*, § 47).

238. Dans l'affaire *Gardel c. France*, 2009 (§ 70), où le périmètre des autorités publiques ayant accès aux données stockées dans un fichier avait été élargi à plusieurs reprises de façon à ne plus se limiter

qu'aux autorités judiciaires et de police mais à englober désormais des organes administratifs, la Cour a été satisfaite de constater que la consultation était exclusivement accessible à des autorités astreintes à une obligation de confidentialité et dans des circonstances précisément déterminées.

239. Dans l'affaire *P.N. c. Allemagne*, 2020 (§ 89), rien n'indiquait que les données d'identification d'un délinquant adulte conservées par les autorités pendant une durée maximale de cinq ans étaient insuffisamment protégées contre des abus tels qu'un accès ou une diffusion non autorisés.

240. En revanche, dans l'affaire *M.M. c. Royaume-Uni*, 2012 (§ 204), relative à la conservation à vie d'un avertissement sur le casier judiciaire d'un individu et à la divulgation de ces données à un futur employeur dans le cadre d'une recherche d'emploi, la Cour a mis en cause les défaillances dans la procédure destinée à réglementer l'accès des tiers aux antécédents judiciaires des personnes briguant un emploi, qui ne permettait aucune appréciation, à quelque stade que ce soit, de la pertinence des données pour l'emploi brigué ou pour savoir si le sujet des données pouvait être perçu comme continuant à présenter un risque. De même, dans l'arrêt *N.F. et autres c. Russie*, 2023 (§ 51), qui concernait une base de données renfermant des informations sur des procédures pénales qui soit avaient été abandonnées pour des « motifs non disculpatoires », soit avaient donné lieu à des condamnations, la Cour a observé que la réglementation en vigueur n'établissait aucune distinction quant aux buts et autres modalités importantes du traitement des données en question, et qu'elle n'offrait donc aucune possibilité réelle de procéder, conformément aux exigences de l'article 8 de la Convention, à une analyse de proportionnalité concernant l'accès éventuel aux données concernées par des tiers.

b. Conservation de données à caractère personnel dans le contexte de la santé

241. La Cour a eu à traiter de la question de la conservation des données sensibles dans le domaine de la santé. Dans l'affaire *Malanicheva c. Russie* (déc.), 2016 (§§ 13, 15-18), la Cour a estimé que le fonctionnement effectif des établissements de santé nationaux et la prise de décision des tribunaux rendaient nécessaire le stockage et le partage des informations pertinentes. Elle a rejeté pour défaut manifeste de fondement les griefs tirés de la présence du nom de la requérante au registre hospitalier des personnes souffrant de troubles psychiatriques et les prétendument fausses références à divers aspects de sa santé mentale dans les communications internes subséquentes entre les établissements de santé et dans leurs observations devant les tribunaux. Rien n'indiquait que les renseignements en question conservés par les autorités aient été rendus accessibles au public ou aient été utilisés à d'autres fins que de décider des soins médicaux les plus appropriés pour le sujet des données.

242. Dans l'arrêt *Drelon c. France*, 2022 (§ 98), qui concernait la conservation jusqu'en 2278 de données à caractère personnel relatives à l'homosexualité présumée du requérant qui avaient été collectées en 2004, la Cour a considéré que la durée de la période en question était excessive.

243. Auparavant, la Commission a déclaré manifestement mal fondée et rejetée une affaire concernant la mémorisation dans le dossier d'un hôpital psychiatrique de données relatives à l'internement d'office d'une patiente dont l'illégalité avait été reconnue par les tribunaux nationaux (*Yvonne Chave née Jullien c. France*, 1991). Pour la Commission, la conservation d'informations concernant les patients mentaux sert non seulement l'intérêt légitime d'assurer le fonctionnement efficace de la fonction publique hospitalière, mais aussi celui de la protection des droits des patients eux-mêmes puisqu'elle contribue à prévenir les risques d'internement arbitraire, et constitue un moyen d'investigation à la disposition des autorités administratives ou judiciaires chargées du contrôle des établissements psychiatriques. En l'espèce, les données à caractère personnel de l'intéressée consignées sur le registre de l'hôpital psychiatrique étaient protégées par des règles de confidentialité appropriées.

244. Voir aussi le paragraphe 182 ci-dessus du présent guide concernant la violation de l'article 8 dans l'affaire *Surikov c. Ukraine*, 2017 (§ 75-95).

c. Conservation en ligne, à des fins journalistiques, des données à caractère personnel

245. La Cour a souligné la fonction accessoire mais néanmoins d'une importance certaine de la presse, qui consiste à constituer des archives à partir d'informations déjà publiées et à les mettre à la disposition du public. À cet égard, la mise à disposition d'archives sur Internet contribue grandement à la préservation et à l'accessibilité de l'actualité et des informations puisque les archives numériques constituent une source précieuse pour l'enseignement et les recherches historiques, notamment en ce qu'elles sont immédiatement accessibles au public et généralement gratuites (*Times Newspapers Ltd c. Royaume-Uni (nos 1 et 2)*, 2009, §§ 27 et 45 ; *Węgrzynowski et Smolczewski c. Pologne*, 2013, § 59 ; *M.L. et W.W. c. Allemagne*, 2018, § 90 ; voir aussi *Hurbain c. Belgique* [GC], 2023, § 180, où la Cour s'est livrée à un examen sous l'angle de l'article 10).

3. Divulgation des données à caractère personnel

246. Dans plusieurs affaires, la Cour a eu l'occasion d'examiner différentes mesures entraînant la divulgation des données à caractère personnel d'un individu, par le responsable de leur traitement, auprès :

- d'un autre individu ou d'une personne morale (*Mockutė c. Lituanie*, 2018, §§ 99-100, sur la transmission par un hôpital d'informations relatives à la santé d'une patiente à un membre de sa famille et à des journalistes ; *Y. c. Turquie* (déc.), 2015, §§ 70-72, sur la divulgation d'informations sur la séropositivité d'un patient par des ambulanciers au personnel d'un hôpital ; *Radu c. République de Moldova*, 2014, § 27, sur la révélation, par un hôpital, d'informations médicales sur l'état de santé d'une patiente auprès de son employeur ; *M.C. c. Royaume-Uni*, 2021, § 46, sur la divulgation par les autorités, à un employeur potentiel, d'informations concernant les antécédents pénaux de la requérante) ;
- d'une autorité publique (*M.S. c. Suède*, 1997, § 35, sur la divulgation des renseignements médicaux d'une patiente par un service de gynécologie à la caisse de sécurité sociale ; *P.T. c. République de Moldova*, 2020, §§ 5-6, 29-31, sur la présence non nécessaire de données médicales sensibles sur une attestation destinée à être produite dans diverses situations) ;
- du public (*Hájovský c. Slovaquie*, 2021 §§ 46-49, sur la publication dans un journal télévisé d'informations relevant l'identité et l'image non floutée d'un particulier, prises à son insu et au moyen d'un stratagème ; *Peck c. Royaume-Uni*, 2003, § 63, sur la transmission aux médias d'une vidéo provenant d'une télévision en circuit fermé filmant une personne tentant de se suicider dans un lieu public ; *Bremner c. Turquie*, 2015, §§ 71-85, sur la diffusion à la télévision de l'image sans floutage ou voilage d'un particulier obtenue en caméra cachée ; *Khadija Ismayilova c. Azerbaïdjan*, 2019, §§ 108-132, sur l'enregistrement vidéo secret d'une journaliste à son domicile et la diffusion de ces vidéos au public ; *Z c. Finlande*, 1997, §§ 70-71, sur la divulgation dans une décision de justice transmise à la presse de l'identité et de l'état de santé d'un individu ; *Apostu c. Roumanie*, 2015, §§ 121-132, sur la divulgation à la presse d'éléments d'un dossier d'instruction ; *Montera c. Italie* (déc.), 2002, sur la divulgation au public d'un rapport d'une commission parlementaire concernant la vie privée et la déontologie professionnelle d'un magistrat ; *Von Hannover c. Allemagne*, 2004, §§ 61-81, sur la publication dans la presse à sensation de photos concernant la vie privée d'une princesse ; *Polanco Torres et Movilla Polanco c. Espagne*, 2010, §§ 44-54, sur un article de presse, fondé sur les déclarations d'un ancien comptable, accusant l'épouse d'un haut magistrat d'être impliquée dans des opérations irrégulières avec une société ; *Alkaya c. Turquie*, 2012, §§ 30-31, sur la divulgation par un quotidien national à grand tirage de l'adresse domiciliaire complète d'une actrice célèbre ; *Mityanin et Leonov c. Russie*, 2018, §§ 111-121, sur la diffusion dans la presse de la photographie d'un suspect accompagnée de déclarations l'accusant d'agissements délictueux et criminels ; *Bogomolova c. Russie*,

2017, §§ 54-58, sur la divulgation d'une photographie d'un enfant figurant sur la page de couverture d'une brochure intitulée « Les enfants ont besoin d'une famille », ayant été publiée par un centre d'assistance psychologique, médicale et sociale ; *L.B. c. Hongrie* [GC], 2023, sur la publication obligatoire, sur la liste des principaux contribuables débiteurs disponible sur le site Internet de l'autorité fiscale, de données à caractère personnel concernant le requérant, dont son nom et l'adresse de son domicile).

a. L'incidence du consentement préalable

247. Le consentement préalable du sujet des données à la transmission, révélation ou publication de ses données s'avère un élément important, quoique non décisif, pour déterminer, dans une affaire, si de telles opérations s'analysent en une ingérence dans son droit au respect de la vie privée (*M.S. c. Suède*, 1997, §§ 31, 35 ; *M.M. c. Royaume-Uni*, 2012, §§ 186, 189) ou si elles pouvaient passer pour « prévues par la loi », au sens de l'article 8 § 2 (*Radu c. République de Moldova*, 2014, § 27 ; *Mockutė c. Lituanie*, 2018, § 101). La Cour a conclu à une violation de l'article 8 dans plusieurs affaires où la divulgation de données à caractère personnel par le responsable de leur traitement avait eu lieu sans le consentement de l'individu concerné (*Radu c. République de Moldova*, 2014, §§ 30, 32 ; *Mockutė c. Lituanie*, 2018, §§ 103, 106 ; *Peck c. Royaume-Uni*, 2003, §§ 85-87 ; *Sõro c. Estonie*, 2015, §§ 17-19, § 64).

248. Pour qu'il soit valide, le consentement du sujet des données doit être éclairé et non équivoque (*M.S. c. Suède*, 1997, § 32 ; *Konovalova c. Russie*, 2014, §§ 47-48). Dans une affaire qui concernait la transmission du dossier médical d'un individu par un organe public (le service de gynécologie d'un hôpital) à un autre (la Caisse de sécurité sociale), sans le consentement du sujet des données, la question était de savoir si, en engageant une procédure en indemnisation, le sujet des données avait renoncé à son droit à la confidentialité de ses données (*M.S. c. Suède*, 1997, §§ 31-32). La Cour a jugé que, dès lors que cette transmission dépendait non seulement de la présentation par l'individu concerné d'une demande d'indemnisation mais également d'une série d'éléments dont la maîtrise lui échappait, il ne saurait inférer de sa demande d'indemnisation qu'il ait renoncé d'une manière non équivoque à la confidentialité de son dossier médical. Ainsi, l'article 8 était applicable en l'espèce.

249. Le fait que la divulgation des données personnelles d'un individu a eu lieu à sa demande ou avec son consentement ne le prive pas de la protection offerte par l'article 8 lorsque l'individu n'a pas réellement eu le choix de les donner ou non, par exemple lorsqu'un employeur a exigé la divulgation de données personnelles inscrites sur le casier judiciaire d'un individu en recherche d'emploi (*M.M. c. Royaume-Uni*, 2012, § 189). Dans l'affaire *M.M. c. Royaume-Uni* (2012, §§ 187-207), où la requérante avait demandé la divulgation à un potentiel employeur d'informations sur un avertissement inscrit sur son casier judiciaire, la Cour a constaté la violation de l'article 8 en l'absence de garanties suffisantes dans le système national de divulgation de données relatives aux antécédents judiciaires d'une personne, qui ne permettait aucune appréciation, à quelque stade que ce soit, de la pertinence des données pour l'emploi brigué ou du point de savoir si le sujet des données pouvait être perçu comme continuant à présenter un risque (*ibidem*, § 204). Dans l'affaire *M.C. c. Royaume-Uni*, 2021, §§ 47-57, la Cour a pris note des modifications législatives intervenues à la suite de l'arrêt *M.M. c. Royaume-Uni* et elle a constaté que le nouveau régime encadrant la divulgation d'informations relatives aux antécédents judiciaires d'une personne était compatible avec les exigences de l'article 8 : il distinguait de différentes manières différents types d'infraction, il permettait de savoir de manière certaine à tout moment quelles condamnations seraient divulguées, et il fixait une durée limitée de divulgation qui variait en fonction de l'âge de l'auteur de l'infraction et de la gravité estimée de l'infraction.

250. Recueillir le consentement du sujet des données n'est pas toujours possible lorsque, par exemple, les séquences provenant des enregistrements avec des caméras de télévision en circuit fermé installées par les autorités sur la voie publique, destinées à aider à l'identification des

délinquants et à la prévention de la criminalité, montrent un grand nombre de personnes (*Peck c. Royaume-Uni*, 2003, § 81). Pour la Cour, un système de caméras de télévision en circuit fermé, dont la divulgation des images ainsi capturées serait subordonnée au consentement de l'individu concerné, risque dans la pratique de compromettre toute action destinée à vanter l'efficacité d'un tel système de surveillance dans la détection et la prévention des infractions, rôle rendu plus efficace encore par la publicité donnée aux résultats (*ibidem*, § 81). En pareilles circonstances, ou si les particuliers dont l'image a été ainsi capturée refusent de donner leur consentement à la diffusion de leurs images, il incombe au responsable du traitement d'envisager d'autres solutions, qui peuvent consister à masquer les images avant de les divulguer (*ibidem*, § 82) ou à veiller à ce que le destinataire des données les masque lui-même, de manière adéquate et suffisante (*ibidem*, § 83).

251. Dans l'affaire *Peck c. Royaume-Uni*, 2003 (§ 87), la communication par une municipalité, dans son communiqué de presse et au profit des médias, des images saisies par la télévision en circuit fermé filmant un individu tentant de se suicider dans un lieu public a emporté une violation de l'article 8. La Cour a considéré que, dès lors que la séquence en question portait et attirait l'attention sur un seul individu, l'opérateur de télévision en circuit fermé qui avait alerté la police et observé son intervention aurait pu se renseigner pour identifier le requérant et ainsi demander son accord à la divulgation des images (*ibidem*, § 81).

252. La diffusion, dans un reportage d'une émission télévisée filmé en caméra cachée, de l'image sans floutage ou voilage d'un particulier a été jugée contraire à l'article 8 dans l'affaire *Bremner c. Turquie*, 2015 (§§ 71-85). Eu égard notamment à l'absence de notoriété du requérant, rien ne laissait supposer qu'une telle diffusion ait une valeur d'information ou qu'elle ait été utilisée à bon escient.

253. En outre, eu égard à l'effet dissuasif que risque d'avoir une obligation de notification préalable, aux doutes quant à l'efficacité d'une telle obligation et à la vaste marge d'appréciation laissée aux autorités nationales dans ce domaine, la Cour a conclu que l'article 8 n'exigeait pas une obligation légale, pour un journal, de notifier une personne avant la publication d'informations sur sa vie privée dans l'affaire *Mosley c. Royaume-Uni*, 2011 (§ 132).

254. Dans certaines circonstances, la divulgation des données sur la santé mentale d'un individu, sans son consentement, auprès d'un membre proche de sa famille peut emporter une méconnaissance du droit au respect de sa vie privée. Dans l'affaire *Mockuté c. Lituanie*, 2018 (§ 100), la Cour a jugé que vu la divulgation à la mère d'une patiente d'informations sur la santé de sa fille adulte sans qu'elle y ait consenti n'a pas, compte tenu des relations tendues entre ces deux personnes adultes, été conforme au droit garanti par l'article 8.

255. Concernant les personnes arrêtées ou poursuivies, la Cour a conclu à une violation de l'article 8 dans des cas où des services de police avaient donné à la presse des photographies des requérants sans leur accord (*Sciacca c. Italie*, 2005, §§ 29-31 ; *Khoujine et autres c. Russie*, 2008, §§ 115-118 ; *Margari c. Grèce*, 2023, §§ 54-60) ou avaient invité des équipes de télévision à filmer le requérant au poste de police, sans son consentement, en vue de la diffusion de ces images à la télévision (*Toma c. Roumanie*, 2009, §§ 90-93 ; *Khmel c. Russie*, 2013, § 41), dans un cas où le ministère de l'Intérieur avait publié sur son site Internet des photographies des requérantes qui avaient été prises lors de leur garde à vue et sur lesquelles l'identité des intéressées n'avait pas été dissimulée (*D.H. et autres c. Macédoine du Nord*, 2023, §§ 63-65), dans un cas où l'affichage d'une photographie du requérant sur le panneau des personnes recherchées n'était pas prévu par la loi (*Guiorgui Nikolaïchvili c. Géorgie*, 2009, §§ 129-131) et dans un cas où les règles et procédures en place ne respectaient pas l'exigence de « qualité de la loi » (*Negru c. République de Moldova*, 2023, §§ 29-35.

256. L'absence du consentement préalable du sujet des données à la transmission, révélation ou publication de ses données n'entraîne pas nécessairement un constat de violation de l'article 8, lorsque d'autres l'impératifs légitimes, tels que la nécessité d'enquêter sur des infractions pénales et de garantir la publicité des procédures judiciaires (*Avilkina et autres c. Russie,* 2013, § 45 ;

Z c. Finlande, 1997, § 97), la nécessité de préserver la santé publique (*Y. c. Turquie* (déc.), 2015, § 74), la sécurité nationale (*Anchev c. Bulgarie* (déc.), 2017, § 100) ou le bien-être économique d'un pays (*M.S. c. Suède*, 1997, § 38) entrent en jeu.

b. Divulgation des données dans le contexte des procédures judiciaires

257. Dans plusieurs affaires, la Cour a examiné différentes mesures prises par les autorités dans le contexte des procédures judiciaires ayant entraîné la divulgation de données personnelles des parties ou des tierces parties, par exemple :

- le fait, pour un tribunal, de reproduire, dans un jugement de divorce, un extrait d'une pièce médicale personnelle (*L.L. c. France*, 2006, § 46), et d'ordonner la limitation à dix ans du délai de confidentialité des pièces produites contenant des données médicales (*Z c. Finlande*, 1997, §§ 112-113),
- la divulgation de données psychiatriques confidentielles lors d'une audience publique (*Panteleyenko c. Ukraine*, 2006, § 57) ; et la vérification d'un certificat médical apporté comme preuve pour étayer une demande d'ajournement (*Stokłosa c. Pologne* (déc.) 2021, §§ 43-44),
- la divulgation de l'identité et de la séropositivité d'un individu dans un arrêt transmis à la presse (*Z c. Finlande*, 1997, § 113),
- la divulgation de l'identité complète d'une tierce partie dans un jugement sans que celle-ci en eût été préalablement informée (*Vicent Del Campo c. Espagne*, 2018, §§ 47-51), ou
- l'utilisation d'un langage et d'arguments dévoilant, dans le jugement rendu, des données personnelles de la victime, véhiculant des préjugés sur le rôle de la femme susceptibles de faire obstacle à une protection effective des droits des victimes de violences de genre en dépit d'un cadre législatif satisfaisant (*J.L. c. Italie*, 2021, §§ 136-142) ;
- la publication dans la presse (*Margari c. Grèce*, 2023, § 54), ou sur une liste publique recensant les personnes recherchées affichée dans la partie publique d'un poste de police (*Negru c. République de Moldova*, 2023, § 24), de photographies et de données à caractère personnel concernant des défendeurs dans une procédure pénale ;
- la publication sur une base de données judiciaires officielle en ligne accessible au public du nom complet et de l'adresse de la requérante, ainsi que du texte intégral des décisions de justice la déboutant de sa demande de dommages et intérêts pour abus sexuels (*A.P. c. Arménie*, 2024, § 159).

258. Pour la Cour, la nécessité de préserver la confidentialité des données à caractère personnel des parties ou des tierces parties dans le contexte des procédures judiciaires peut parfois s'effacer devant les nécessités d'enquêter sur des infractions pénales et de garantir la publicité des procédures judiciaires (*Avilkina et autres c. Russie,* 2013, § 45 ; *Z c. Finlande*, 1997, § 97). Il convient d'accorder aux autorités nationales compétentes une certaine latitude pour établir un juste équilibre entre, d'une part, la protection de la publicité des procédures judiciaires, nécessaire pour préserver la confiance dans les cours et tribunaux et, d'autre part, les intérêts d'une partie ou d'une tierce personne à la confidentialité de ses données (*C.C. c. Espagne*, 2009, § 35). Toute mesure susceptible de révéler au public des données à caractère personnel d'un individu, qu'il soit partie ou tierce partie à une procédure judiciaire, doit répondre à un besoin social impérieux (*Vicent Del Campo c. Espagne*, 2018, § 46) et se limiter autant que faire se peut à celles rendues strictement nécessaires par les spécificités de la procédure (*L.L. c. France*, 2006, § 45 ; *Margari c. Grèce*, 2023, § 47).

259. Pour déterminer, dans une affaire donnée, s'ils existaient des raisons suffisantes pour justifier la révélation, dans le texte d'une décision de justice, de l'identité d'un individu et des autres données personnelles le concernant, un élément important consiste à savoir si d'autres mesures, moins intrusives, étaient possibles en vertu du droit et de la pratique nationale. Il peut s'agir,

notamment, de la possibilité, pour une juridiction nationale, de ne pas mentionner dans son arrêt de noms permettant d'identifier l'intéressé (*Z c. Finlande*, 1997, § 113 ; *Vicent Del Campo c. Espagne*, 2018, § 50), de décider que l'exposé complet des motifs resterait confidentiel pendant une période donnée et de publier à la place une version abrégée de la motivation et du dispositif et une référence succincte à la législation appliquée (*Z c. Finlande*, 1997, § 113), ou de limiter l'accès au texte d'un arrêt ou à certaines de ses parties (*Vicent Del Campo c. Espagne*, 2018, § 50). Pour la Cour, de telles mesures sont généralement considérées de nature à réduire l'impact produit par un jugement sur le droit du sujet des données à la protection de sa vie privée.

260. Dans l'affaire *Panteleyenko c. Ukraine,* 2006 (§ 82), la tenue d'une audience à huis clos aurait également pu permettre, aux yeux de la Cour, d'éviter la divulgation, au public, lors d'une audience publique, d'informations confidentielles sur la santé mentale d'un individu obtenues auprès d'un hôpital psychiatrique et sur le traitement psychiatrique qu'il y avait subi, même si elle n'aurait pas nécessairement empêché que celles-ci soient portées à la connaissance des parties et versées au dossier de l'affaire.

261. Dans l'affaire *Frâncu c. Roumanie*, 2020 (§§ 72-73), le manquement d'une cour d'appel à assurer la confidentialité des informations médicales concernant le requérant en rejetant une demande de huis clos dans une affaire de corruption visant un maire a été jugée contraire à l'article 8. Aux yeux de la Cour, en se bornant à énoncer, sans fournir davantage d'explications, que le cas du requérant ne correspondait à « aucune des situations » prévues par la disposition du code de procédure pénale relative au huis clos, la juridiction en cause n'a pas ménagé un juste équilibre entre l'intérêt général à assurer la transparence de la procédure judiciaire et, d'autre part, l'intérêt du justiciable à préserver la confidentialité des données concernant son état de santé. À supposer que la notoriété d'un accusé puisse constituer l'un des éléments à prendre en compte dans l'analyse de proportionnalité d'une demande d'examen d'une affaire à huis clos, en l'espèce aucun examen individualisé de la proportionnalité d'une telle mesure n'a été fait par la cour d'appel.

262. Dans l'affaire *Khadija Ismayilova c. Azerbaïdjan*, 2019 (§§ 105-132), la Cour a jugé que la révélation par les autorités de poursuite d'informations à caractère privé, divulguant des données personnelles sensibles comme le nom et l'adresse de la requérante, journaliste de profession ainsi que les noms de ses amis, membres de la famille et collègues dans un communiqué de presse qui prétendait fournir un rapport d'avancement sur une enquête pénale, a emporté un constat de violation de l'article 8 (*ibidem*, §§ 142-150).

263. Dans l'affaire *M.P. c. Portugal*, 2021, §§ 48-49, la production par l'ex-mari de la requérante, sans qu'elle y ait consenti, dans le cadre d'une procédure de divorce, de messages électroniques échangés par son épouse sur un site de rencontres auxquels elle semblait lui avoir donné accès n'a pas emporté une violation de l'article 8, le tribunal aux affaires familiales n'en ayant finalement pas tenu compte et l'accès du public aux dossiers de ce type de procédures étant, par ailleurs, restreint.

264. Dans l'affaire *J.S. c. Royaume-Uni* (déc.), 2015 (§§ 71-73), la Cour a rejeté, pour défaut manifeste de fondement, un grief tiré de la révélation, dans un communiqué de presse publié par le parquet, d'informations personnelles qui n'allait pas au-delà de ce qui est généralement fourni aux médias en réponse à des questions sur une procédure judiciaire, et qui ne révélaient ni le nom du requérant (un mineur accusé d'avoir agressé un professeur), ni son âge ou son école, ni aucune autre information personnelle.

265. Dans l'affaire *L.L. c. France*, 2006 (§§ 46), où le juge s'était fondé, de façon subsidiaire, dans le cadre d'une procédure de divorce sur une correspondance privée entre un médecin spécialiste et le médecin traitant du requérant contenant une pièce médicale confidentielle, le fait que le juge ou l'officier d'investigation aurait pu écarter la divulgation, dans la motivation d'un jugement, des données médicales en question tout en parvenant à la même conclusion était un élément important à prendre en compte. Puisque toute personne pouvait se procurer une copie de la motivation de la décision, sans justifier d'un intérêt, l'ingérence subie par le requérant dans son droit au respect de sa

vie privée n'était pas justifiée au regard du rôle fondamental joué par la protection des données à caractère personnel, nonobstant que les débats entre les parties à un divorce ne soient pas publics et la décision opposable aux tiers ne contienne que le dispositif (*ibidem*, §§ 47, 33).

266. Dans l'affaire *Vicent Del Campo c. Espagne*, 2018 (§§ 53, 56), le fait que le requérant, tiers à une procédure judicaire, s'était trouvé privé d'une quelconque possibilité de demander à une juridiction avant le prononcé de l'arrêt, de s'abstenir de communiquer son identité a constitué une violation de l'article 8. L'intéressé n'avait pas été informé, interrogé, cité à comparaître ou prévenu de quelque manière que ce soit.

267. Dans une affaire dans laquelle les juridictions nationales ont fixé à dix ans le délai de confidentialité des pièces du dossier révélant la séropositivité et l'identité de la requérante, la Cour a constaté la violation de l'article 8, estimant que les autorités judicaires n'avaient pas accordé suffisamment de poids aux intérêts liés à la protection des données à caractère personnel des parties et des tiers qui pouvaient en être affectés (*Z c. Finlande*, 1997, §§ 111-112). À ses yeux, l'ingérence grave dans le droit au respect de la vie privée du sujet des données qui découlait de la production, lors d'une procédure judicaire, sans son consentement, des informations concernant son état de santé, serait amplifiée si les éléments en question devaient tomber dans le domaine public au bout de dix ans (*ibidem*, § 112). En revanche, dans l'affaire *Y. c. Turquie* (déc.), 2015 (§§ 81-82), le fait que l'identité et la séropositivité du requérant avaient été dévoilées dans une seule décision d'incompétence rendue par un tribunal administratif qui n'avait fait l'objet d'aucune publication ou publicité et n'avait pas été rendue accessible au public, tandis qu'aucune des autres décisions rendue dans le cadre de la même procédure n'en faisait état, n'a pas été jugée de nature à avoir porté atteinte au droit au respect de la vie privée du sujet des données.

268. Dans l'affaire *Drakšas c. Lituanie*, 2012 (§ 60), la divulgation, dans le contexte de la procédure d'impeachment, des enregistrements des conversations téléphoniques interceptés par les services secrets entre le requérant, un politicien connu, et le président visé par la procédure de destitution, lors d'une audience publique devant la Cour constitutionnelle retransmise en direct par les chaînes de télévision nationales, n'a pas emporté un constat de violation de l'article 8. Pour la Cour, en tant que personne publique, le requérant s'était inévitablement et consciemment exposé à un contrôle attentif de ses faits et gestes tant par les journalistes que par la masse des citoyens. Dès lors, la divulgation, prévue par la loi, de ses conversations téléphoniques non privées, mais de nature politique ou commerciale, pendant une procédure constitutionnelle était nécessaire à la protection des droits d'autrui.

269. Dans l'affaire *A.P. c. Arménie*, 2024 (§§ 150-162), la Cour a jugé que la publication des données à caractère personnel de la requérante, ainsi que du texte intégral des décisions de justice la déboutant de sa demande de dommages et intérêts pour abus sexuels, s'analysaient en une atteinte à son droit au respect de sa vie privée. Les informations en question avaient été publiées sur une base de données judiciaires officielle en ligne accessible au public, alors que l'intéressée avait spécifiquement demandé à ce que ces éléments d'information ne soient pas publiés. La Cour a jugé que la publication litigieuse était dépourvue de base légale en droit interne, et elle a conclu que l'ingérence n'était pas « prévue par la loi » au sens de l'article 8 de la Convention.

270. Voir aussi le paragraphe 255 ci-dessus du présent guide sur la divulgation à la presse, par des services de police, des photographies des personnes arrêtées ou poursuivies sans leur accord et les paragraphes 80 à 82 ci-dessus du présent guide s'agissant des obligations positives incombant à l'État dans les affaires portant sur la question de la divulgation des données à caractère personnel du fait des particuliers.

c. Divulgation des données pour la protection de la santé publique

271. Le droit d'un individu à la protection du caractère confidentiel de ses données médicales n'est pas absolu et doit être concilié avec d'autres droits et intérêts légitimes, tel le droit à une procédure

contradictoire de son employeur (*Eternit c. France* (déc.), 2012, § 37). Il peut s'effacer devant la nécessité de défendre un aspect primordial de l'intérêt public, tel que la sécurité du personnel hospitalier et la protection de la santé publique (*Y. c. Turquie* (déc.), 2015, § 74).

272. Dans certaines circonstances, lorsque le traitement des patients au sein des hôpitaux et du système de santé est en jeu, la transmission de l'information relative à la condition d'un patient peut s'avérer pertinente et nécessaire aux fins d'assurer non seulement un traitement médical approprié du patient mais aussi de veiller à la protection des droits et des intérêts du personnel soignant impliqué dans son traitement et des autres patients, en permettant que les mesures de précaution requises puissent être adoptées (*Y. c. Turquie* (déc.), 2015, § 74). Lorsque le personnel de santé court lui-même un risque d'infection en raison de leur exposition dans le cadre de leur travail, la sécurité du personnel hospitalier et la protection de la santé publique peuvent justifier la transmission de l'information relative à l'état de santé d'un patient entre les différents intervenants médicaux impliqués dans sa prise en charge afin d'éviter tout risque de transmission intra hospitalière de la maladie (*ibidem*, § 78).

273. Les modalités de transmission des données sensibles telles que des données sur la santé d'un patient doivent se faire dans le souci d'éviter toute forme de stigmatisation du sujet des données et en offrant des garanties suffisantes pour écarter tout risque d'abus (*Y. c. Turquie* (déc.), 2015, § 79). Le destinataire de l'information doit être soumis aux règles de confidentialité propres aux professionnels de santé ou à des règles de confidentialité comparables (*ibidem*, § 74).

274. Dans l'affaire *Y. c. Turquie* (déc.), 2015 (§§ 78-79), la Cour a rejeté, pour défaut manifeste de fondement, une requête relative à la divulgation de l'information concernant la séropositivité d'un patient entre les différents intervenants médicaux d'un hôpital impliqués dans sa prise en charge, estimant que la sécurité du personnel hospitalier et la protection de la santé publique pouvaient légitimement la justifier, nonobstant l'absence du consentement du sujet des données. Elle a accordé du poids au fait que, selon le droit interne, chacun des intervenants médicaux était tenu de respecter la confidentialité des données qui lui étaient transmises de par sa situation ou sa profession, sous peine de s'exposer à des poursuites disciplinaires ou pénales.

d. Divulgation des données pour la protection de la sécurité nationale

275. Dans une série d'affaires relatives au démantèlement de l'héritage des anciens régimes communistes, la Cour a examiné la question de la révélation au public des données relatives au passé lointain d'un individu collectées et mémorisées dans le but de protéger la sécurité nationale (*Sõro c. Estonie*, 2015, § 58 ; *Anchev c. Bulgarie* (déc.), 2017, § 100). Les questions relatives à l'individualisation des mesures mises en œuvre pour le démantèlement, leur encadrement et les garanties apportées sont importantes.

276. Ainsi, dans l'affaire *Sõro c. Estonie*, 2015 (§§ 56-64), la révélation d'informations indiquant que le requérant avait été employé en tant que chauffeur dans les anciens services de sécurité, a emporté un constat de violation de l'article 8. Bien que le requérant ait été informé à l'avance que la publication aurait lieu et bien qu'il ait été en mesure de contester la communication, il n'existait pas de procédure permettant d'évaluer la tâche spécifique accomplie individuellement par les employés des services de sécurité et ainsi de différencier selon le danger qu'ils pouvaient représenter dans un système démocratique plusieurs années après la fin de leur carrière au sein desdits services (*ibidem*, § 61). Pour la Cour, l'écoulement d'un grand laps de temps entre la publication des données à caractère personnel et la restauration de l'indépendance de l'Estonie a nécessairement amoindri les dangers que le requérant pouvait initialement représenter pour le nouveau système démocratique (*ibidem*, § 62). Même si la loi sur la divulgation n'imposait pas en elle-même des limitations au nouvel emploi du requérant, le requérant a été contraint de quitter son poste en raison de l'attitude de ses collègues à son égard, ce qui démontre la gravité de l'atteinte portée au droit du requérant au respect de sa vie privée (*ibidem*, § 63).

277. En revanche, dans l'affaire *Anchev c. Bulgarie* (déc.), 2017 (§§ 92-116), où le processus de divulgation était fortement encadré et il était associé à un certain nombre de garanties contre l'arbitraire et les abus, notamment le fait qu'il avait était confié à une commission indépendante spéciale, dont les décisions pouvaient faire l'objet d'un contrôle juridictionnel public à deux niveaux de juridiction, la révélation au public des données relatives au passé lointain du requérant n'a pas été jugé incompatible avec l'article 8. La divulgation n'ayant pas entraîné de sanctions ou d'incapacités juridiques, l'ingérence n'a pas outrepassé l'importante marge d'appréciation dont jouissent les autorités (*ibidem*, §§ 106-113). La Cour a déclaré que sa conclusion aurait pu être différente si l'État avait eu recours à des mesures impliquant un degré supérieur d'intrusion dans la sphère personnelle du sujet des données, telles que l'interdiction d'exercer un métier ou la privation partielle du droit de vote (*ibidem*, § 113).

e. Divulgation des données pour la protection du bien-être économique du pays

278. Des mesures, réputées assurer la protection du bien-être économique du pays, qui portent atteinte à la confidentialité des données recueillies ou mémorisées par des autorités, ne sont pas nécessairement contraires à l'article 8 si elles sont assorties de garanties effectives et satisfaisantes (*M.S. c. Suède*, 1997, § 41). Dans la mise en balance des intérêts en jeu, le fait de savoir si le droit interne encadre ou non, les mesures que les responsables du traitement des données sont susceptibles de prendre, que leur responsabilité est engagée en cas de non-respect des exigences légales, et qu'une obligation d'observer des règles et garanties analogues, notamment une obligation de confidentialité, pèse sur le destinataire des données sont des éléments importants à prendre en compte (*ibidem*, § 43).

279. Dans l'affaire *M.S. c. Suède*, 1997 (§§ 31-44), la transmission du dossier médical d'un individu par un organe public (le service de gynécologie d'un hôpital) à un autre (la Caisse de sécurité sociale), chargé d'apprécier si l'intéressée remplissait les conditions légales pour l'obtention d'une prestation qu'elle avait elle-même sollicitée, n'a pas emporté une violation de l'article 8. Pour la Cour, cette communication était potentiellement décisive pour l'allocation de fonds publics à des demandeurs remplissant certains critères et pouvait donc être considérée comme visant à protéger le bien-être économique du pays (*ibidem*, § 38). La divulgation des données confidentielles de l'individu concerné était assortie de garanties effectives et satisfaisantes contre les abus : la législation nationale mettait comme condition à la communication des données que les informations soient pertinentes pour l'application de la loi sur l'assurance invalidité professionnelle (*ibidem*, §§ 18, 43) ; le personnel du service de gynécologie aurait pu voir sa responsabilité civile et/ou pénale engagée s'il avait omis de se conformer à ces conditions (*ibidem*, §§ 22, 43) ; et le destinataire des données avait une obligation analogue de respecter leur confidentialité (*ibidem*, §§ 20, 22, 43).

280. L'affaire *L.B. c. Hongrie* [GC], 2023 (§§ 20-29) concernait la publication sur la liste des principaux contribuables débiteurs, consultable sur le site Internet de l'autorité fiscale nationale, de données à caractère personnel concernant le requérant (dont son nom et l'adresse de son domicile). Présentée dans la législation pertinente comme un outil pour lutter contre le non-respect de la réglementation fiscale, la publication systématique et obligatoire de pareilles données s'appliquait à tous les contribuables qui, à la fin du trimestre, étaient redevables de montants d'impôts importants pendant une période de plus de 180 jours consécutifs. La Cour a souligné que le choix d'un tel régime général par le législateur n'était pas problématique en soi, pas plus que ne l'était en tant que telle la publication de données de contribuables. Elle a aussi dit que les États contractants jouissaient d'une ample marge d'appréciation pour déterminer, aux fins notamment d'assurer le bon fonctionnement de la perception de l'impôt dans son ensemble, la nécessité d'établir un régime de divulgation de données à caractère personnel concernant les contribuables ne s'acquittant pas de leurs obligations de paiement. Elle a toutefois ajouté que la latitude dont les États contractants jouissaient à cet égard n'était pas illimitée et elle a précisé que dans pareil contexte, elle devait se convaincre que les autorités nationales compétentes, aux niveaux législatif, exécutif ou judiciaire,

avaient correctement mis en balance les intérêts concurrents et, dans ce cadre, dûment tenu compte non seulement i) de l'intérêt public à la divulgation des informations en question, mais aussi ii) de la nature des informations divulguées, iii) des répercussions sur l'exercice par les personnes concernées du droit au respect de leur vie privée et du risque d'atteinte à celui-ci, iv) de la portée potentielle du support utilisé pour la diffusion de l'information, en particulier celle d'Internet, ainsi que v) des principes fondamentaux de la protection des données, notamment ceux relatifs à la limitation des finalités, à la limitation de la conservation, à la minimisation des données et à leur exactitude. Elle a aussi précisé que l'existence de garanties procédurales pouvait également jouer un rôle important dans ce cadre (*ibidem*, § 128).

281. Sur les faits de la cause, la Cour a mis en exergue deux caractéristiques du régime de publication en cause : l'inclusion parmi les données à caractère personnel devant être publiées de l'adresse du domicile du contribuable, et le fait que l'autorité fiscale nationale ne disposait d'aucun pouvoir d'appréciation pour procéder à une appréciation individualisée de la proportionnalité de la mesure. En tenant compte de ces éléments, elle a analysé la qualité du contrôle opéré par le législateur et identifié les lacunes suivantes : i) absence d'appréciation de la nécessité et de la complémentarité de la mesure générale litigieuse (tout particulièrement en ce qui concerne l'obligation de publier l'adresse du domicile du contribuable débiteur) au regard des outils existants visant le même but dissuasif, ii) absence de prise en considération de l'impact sur le droit au respect de la vie privée et, en particulier, du risque d'usage impropre de l'adresse du domicile du contribuable débiteur par d'autres membres du public, iii) absence de prise en considération de la portée potentielle du support utilisé pour la diffusion des informations en question (Internet), qui supposait un accès illimité à des informations assez sensibles (nom et adresse du domicile de l'intéressé), avec le risque que la republication soit une conséquence naturelle, probable et prévisible de la publication initiale, et iv) absence de prise en considération des exigences en matière de protection des données énoncées par le droit national et de l'UE et de la possibilité de prendre des mesures pour concevoir des réponses suffisamment adaptées eu égard au principe de la minimisation des données. Dans ce contexte, elle a conclu que, nonobstant l'ample marge d'appréciation dont l'État défendeur jouissait, l'ingérence litigieuse n'était pas « nécessaire dans une société démocratique » (*ibidem*, §§ 129-140).

f. Divulgation en masse des données à caractère personnel

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

B. Droits des personnes concernées

283. La jurisprudence de la Cour reconnait aux sujets des données à caractère personnel un certain nombre de prérogatives qui leur permettent d'assurer la jouissance de leur droit garanti par l'article 8 de la Convention.

1. Droit d'accès à ses propres données

284. Les individus dont les données personnelles ont été recueillies et conservées par les autorités ont un intérêt, protégé par l'article 8, de recevoir les informations : recueillies sur eux par les anciens services secrets pendant les régimes totalitaires et conservées dans les archives de l'État (*Haralambie c. Roumanie*, 2009, § 79 ; *Jarnea c. Roumanie*, 2011, § 50 ; *Joanna Szulc c. Pologne*, 2012, § 87) ; nécessaires concernant leur santé ou les risques pour leur santé auxquels ils avaient été exposés (*Roche c. Royaume-Uni* [GC], 2005, § 155 ; *K.H. et autres c. Slovaquie*, 2009, § 44 ; *Yonchev c. Bulgarie*, 2017, § 46) ; pour connaître et comprendre leurs enfance et développement précoce (*Gaskin c. Royaume-Uni,* 1989, § 41) ; ou pour retracer leurs origines, notamment l'identité de leur parents (*Odièvre c. France* [GC], 2003, §§ 43-44 ; *Godelli c. Italie*, 2012, §§ 62-63 ; *M.G. c. Royaume-Uni*, 2002, § 27).

285. Dans ces différents contextes, pèse sur les autorités l'obligation positive inhérente à un respect effectif de la vie privée, garantie par l'article 8, de prévoir une procédure efficace et accessible permettant aux intéressés d'avoir accès à toutes les informations pertinentes et appropriées nécessaires aux fins spécifiques (*Roche c. Royaume-Uni* [GC], 2005, § 162 ; *Haralambie c. Roumanie*, 2009, § 86 ; *Joanna Szulc c. Pologne*, 2012, §§ 86, 94).

286. En revanche, lorsque l'État peut légitimement craindre que l'accès à des informations comportant des données à caractère personnel risque de compromettre l'efficacité du système de surveillance secrète destiné à protéger la sécurité nationale ou à lutter contre le terrorisme, il peut refuser l'accès aux informations recueillies et conservées dans un fichier tenu secret sans que cela ne soit incompatible avec l'obligation positive que pèse sur les autorités en vertu de l'article 8 (*Leander c. Suède*, 1987, § 66 ; *Segerstedt-Wiberg et autres c. Suède*, 2006, § 102). Pour déterminer si l'État est en droit de considérer que les intérêts de la sécurité nationale et de la lutte contre le terrorisme prévalent sur les intérêts d'une personne à avoir accès à l'intégralité des informations sur elle conservées dans des services de sécurité, la Cour doit être convaincue de l'existence de garanties suffisantes contre arbitraire. La qualité de la loi (*ibidem*, §§ 79-80) et les garanties mises en place, notamment la possibilité d'un contrôle de la mesure litigieuse et les recours dont la personne concernée dispose au niveau national (*ibidem*, §§ 52-68), sont des critères importants à prendre en compte dans la mise en balance des intérêts en jeu (*ibidem*, § 103). Des principes semblables sont applicables dans le contexte des expulsions d'étrangers. Dans l'affaire *Hassine c. Roumanie*, 2021, §§ 55-69, le requérant, un ressortissant tunisien résidant légalement en Roumanie, avait été expulsé du pays pour des raisons de sécurité nationale et interdit de séjour en Roumanie pour cinq ans sur la base de renseignements émanant des services secrets roumains. Ces renseignements, classés secrets, indiquaient selon les autorités qu'il participait à des activités de nature à porter atteinte à la sécurité nationale. Ni le requérant ni son avocat n'avaient été autorisés à en prendre connaissance. La Cour a jugé que la procédure administrative d'expulsion du requérant n'avait pas présenté les garanties procédurales requises, et elle a conclu à la violation de l'article 1 du Protocole n° 7.

287. La destruction immédiate de données collectées, dès le moment où elles sont considérées comme étant dépourvues d'intérêt aux fins de la collecte en cause, n'est pas, en elle-même, contraire à la Convention, même lorsque pareille mesure a eu pour effet d'empêcher les personnes concernées de consulter les données en question. Cela étant, les personnes concernées peuvent avoir un intérêt légitime à obtenir une copie de la décision rendue par l'autorité compétente à l'effet d'ordonner la destruction des éléments interceptés ainsi que de l'« acte » de destruction (*Denysyuk et autres c. Ukraine*, 2025, §§ 108-109). En outre, il est impératif de mettre en place et de rendre publiques des règles et directives claires définissant la procédure de contrôle et de destruction des documents interceptés, y compris des règles concernant le contrôle des procédures pertinentes par un organe indépendant (*Denysyuk et autres c. Ukraine*, 2025, §§ 110-113).

288. Dans une affaire relative à l'inscription de longue durée des données personnelles du requérant dans le fichier d'information Schengen, la Cour a jugé que l'impossibilité pour l'intéressé

d'accéder personnellement à l'intégralité des renseignements qu'il demandait ne saurait entraver le droit au respect de sa vie privée au regard de l'impératif de protéger la sécurité nationale (*Dalea c. France* (déc.), 2010). Même si l'intéressé ne s'était pas vu offrir la possibilité de s'opposer au motif précis de cette inscription, il avait eu connaissance de toutes les autres données le concernant figurant dans le fichier Schengen et le signalement se fondait sur des considérations tenant à la sûreté de l'État, à la défense et la sécurité publique (*ibidem*, faisant référence à *Leander c. Suède*, 1987, § 66).

289. Lorsque seule une partie des documents d'un fichier conservé par les autorités sur une personne comptant des données à caractère personnel a été classée secret défense, les autorités pourraient permettre à l'intéressé d'y avoir un accès partiel (*Yonchev c. Bulgarie*, 2017, §§ 55-59). Ainsi, dans une affaire où était en cause le refus des autorités de permettre au requérant, un ancien policier, de consulter certaines pièces de son dossier personnel, en l'occurrence ses évaluations psychologiques, la Cour a conclu à une violation de l'article 8 en raison de l'existence, au niveau national, des règles trop formelles, selon lesquelles, lorsqu'un seul des documents du dossier avait été classé secret, le reste devait être automatiquement également considéré comme classé et donc soumis aux règles de protection des informations classifiées (*ibidem*, § 60).

290. Si la législation interne prévoyait expressément un droit d'accès au fichier personnel recueilli et conservé par les anciens services de sécurité pendant les régimes totalitaires des anciens États communistes, l'État était tenu d'offrir une procédure effective et accessible permettant à l'intéressé d'avoir accès, dans un délai raisonnable, à l'ensemble des informations pertinentes (*Haralambie c. Roumanie*, 2009, § 86 ; *Jarnea c. Roumanie*, 2011, § 50 ; *Antoneta Tudor c. Roumanie*, 2013, § 34 ; *Joanna Szulc c. Pologne*, 2012, §§ 86, 94). La Cour a conclu à la violation de l'article 8 dans une affaire où le requérant n'a pu avoir accès qu'à une partie d'un fichier à son nom, recueilli et conservé par les anciens services secrets (*Jarnea c. Roumanie*, 2011, §§ 54-60) et dans deux autres affaires où l'accès aux documents les concernant n'a pu avoir lieu que dix ans après la première demande des intéressés (*Joanna Szulc c. Pologne*, 2012, §§ 93-95 ; *Antoneta Tudor c. Roumanie*, 2013, §§ 34-40). Des défaillances du système d'archivage ou des erreurs matérielles telles qu'une erreur dans l'inscription de la date de naissance du requérant dans le fichier personnel identifié à son nom, ne saurait justifier un délai de six années d'attente avant d'avoir accès à ses données personnelles (*Haralambie c. Roumanie,* 2009, § 95). L'âge avancé d'un individu qui fait une demande d'accès à ce type d'information rend d'autant plus urgent son intérêt à retracer son parcours personnel lors de l'époque du régime totalitaire (*ibidem*, § 93 *in fine*).

291. En matière d'informations relatives à la santé ou aux risques pour la santé, le droit d'accès aux données à caractère personnel s'étend à la mise à disposition, en faveur de la personne concernée, de copies des dossiers dont elle fait l'objet (*K.H. et autres c. Slovaquie*, 2009, § 47). Il appartient au détenteur de tels dossiers de définir les mesures à prendre pour permettre au sujet des données d'en copier les pièces et de déterminer qui devrait supporter les frais occasionnées (*ibidem*, § 48). Le sujet des données ne doit pas être contraint de justifier sa demande. Il revient aux autorités de démontrer l'existence de raisons impérieuses de refuser un tel service (*ibidem* § 48). Dans l'affaire *K.H. et autres c. Slovaquie*, 2009 (§§ 50-58), des anciennes patientes d'un hôpital se sont retrouvées dans l'impossibilité de photocopier les dossiers originaux, recueillis et conservés par un hôpital public, qui contenaient des informations qu'elles jugeaient importantes du point de vue de leur intégrité morale et physique. Pour la Cour, la possibilité, que leur avait accordée l'hôpital, de prendre des notes exclusivement manuscrites à partir des dossiers originaux ne leur offrait pas un accès effectif aux documents pertinents concernant leur santé.

292. Lorsqu'un État s'engage dans des activités dangereuses susceptibles d'avoir des conséquences néfastes cachées sur la santé des personnes qui y participent, les autorités ont une obligation positive d'offrir aux intéressés une « procédure effective et accessible » qui leur permet d'avoir accès à « l'ensemble des informations pertinentes et appropriées » et d'évaluer ainsi tout risque pour leur santé auquel ils avaient pu être exposé (*McGinley et Egan c. Royaume-Uni*, 1998, § 101 ;

Roche c. Royaume-Uni [GC], 2005, § 161-162). Un délai d'attente déraisonnable, par exemple lorsque les services d'information et d'études sanitaires ont débuté des processus de recherche et de divulgation des documents pertinents près de dix ans après que l'intéressé se soit lancé dans leur recherche, est constitutif d'une défaillance de l'État, contraire à l'article 8, à remplir son obligation positive inhérente au respect de la vie privée du sujet des données, nonobstant les difficultés liées à l'ancienneté et à la dispersion de ces documents (*ibidem*, § 166).

293. S'agissant de l'accès aux données à caractère personnel d'une personne confiée, dans son enfance, aux services sociaux à la suite du décès de ses parents ou compte tenu de leur incapacité à en assumer la garde, un système qui subordonne l'accès aux dossiers à l'acceptation des « informateurs », à savoir des personnes à l'origine de ces pièces, peut en principe être compatible avec l'article 8 du fait de la marge d'appréciation de l'État. Il doit toutefois sauvegarder les intérêts de quiconque cherche à consulter des pièces relatives à sa vie privée et familiale et, au cas où un informateur ne répond pas ou ne donne pas son consentement, il n'est compatible avec le principe de proportionnalité que s'il charge un organe indépendant de prendre la décision finale sur l'accès aux données (*Gaskin c. Royaume-Uni*, 1989, § 49). Dans les affaires dans lesquelles le système national ne prévoyait pas de recours auprès d'un tel organe en cas de refus des services sociaux de donner accès à toutes les pièces du dossier en possession, y compris lorsqu'une tierce partie concernée ou à l'origine de l'information ne consentait pas à la divulgation, la Cour a trouvé une violation de l'article 8 (*ibidem,* § 49 ; *M.G. c. Royaume-Uni*, 2002, §§ 30-32).

294. Pour la Cour, un enfant né hors mariage qui cherche la détermination du lien juridique avec son père naturel a un intérêt vital, défendu par la Convention, d'obtenir les informations qui lui sont indispensables pour découvrir la vérité sur un aspect important de son identité personnelle (*Mikulić c. Croatie*, 2002, § 64 ; *Boljević c. Serbie*, 2020, § 50). Un système qui ne prévoit pas de moyens de contraindre le père prétendu à se conformer à un ordre du tribunal lui enjoignant de se soumettre à des tests ADN, peut en principe être jugé compatible avec les obligations découlant de l'article 8, eu égard à la marge d'appréciation de l'État (*Mikulić c. Croatie*, 2002, § 64). Toutefois, l'absence de toute mesure procédurale contraignante en question n'est conforme au principe de proportionnalité que si le système en question offre d'autres moyens grâce auxquels une autorité indépendante peut statuer rapidement sur l'action en recherche de paternité (*ibidem*, § 64). La Cour a conclu à une violation de l'article 8 lorsque, en cas de refus du père prétendu de coopérer à la procédure médicale, le système national n'offrait ni mesures de nature à le contraindre à participer aux tests ADN, ni d'autres moyens grâce auxquels une autorité indépendante pourrait statuer rapidement sur l'action en recherche de paternité (*ibidem*, § 64). L'intérêt que peut avoir un individu à connaître son ascendance ne cesse nullement avec l'âge, bien au contraire (*Jäggi c. Suisse*, 2006, § 40, sur le refus d'autoriser une expertise ADN sur un défunt demandée par son fils présumé voulant établir avec certitude sa filiation ; *Boljević c. Serbie*, 2020, § 54).

295. S'agissant des enfants nés d'accouchements anonymes, la question de l'accès aux 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 (*Odièvre c. France* [GC], 2003, § 43 ; *Godelli c. Italie,* 2012, § 62). Face à la diversité des systèmes et traditions juridiques, les États doivent jouir d'une certaine marge d'appréciation pour maintenir la confidentialité de l'identité des parents biologiques (*Odièvre c. France* [GC], 2003, § 46 ; *Godelli c. Italie,* 2012, § 65). Un système national ayant permis à l'intéressée d'avoir accès à des informations non identifiantes sur sa mère et sa famille biologique, lui permettant d'établir quelques racines de son histoire dans le respect de la préservation des intérêts des tiers, assorti d'une possibilité, qui s'ouvrait à elle en vertu d'une loi récemment adoptée, de faire appel à un organe indépendant chargé de faciliter la recherche des origines biologiques afin d'obtenir la réversibilité du secret de l'identité de sa mère sous réserve de l'accord de celle-ci, a été jugé conforme à l'article 8 (*Odièvre c. France* [GC], 2003, § 49 ; voir aussi, concernant l'accès de personnes nées par procréation médicalement assistée avec tiers donneur aux informations

relatives au donneur, *Gauvin-Fournis et Silliau c. France*, 2023, §§ 113-33). En revanche, un système qui donne une préférence aveugle à la mère désireuse de maintenir son anonymat, et qui ne donne aucune possibilité à l'enfant adopté et non reconnu à la naissance de demander soit l'accès à des informations non identifiantes sur ses origines, soit la réversibilité du secret, n'a pas été jugé conforme aux exigences de l'article 8 (*Godelli c. Italie*, 2012, §§ 70-72).

2. Droit de rectification

296. La Cour a examiné plusieurs affaires relatives à la mémorisation, par les autorités, de données fausses ou dont l'exactitude était contestée par l'intéressé (*Rotaru c. Roumanie* [GC], 2000, §§ 42-44, §§ 55-63, concernant l'impossibilité de réfuter les données concernant la supposée participation d'un individu à un mouvement légionnaire dans un dossier recueilli par le service de sécurité ; *Cemalettin Canlı c. Turquie*, 2008, §§ 34-37, concernant la présence dans une procédure judiciaire de données personnelles incomplètes recueillies par la police ; *Khelili c. Suisse*, 2011, § 56, concernant le maintien dans les fichiers de la police de la mention « prostituée » comme profession d'une personne qui a toujours contestée l'exercer).

297. L'impossibilité pour un individu de faire rectifier un signalement le concernant dans le fichier du système d'information Schengen (*Dalea c. France* (déc.), 2010) ou l'inscription de son origine ethnique dans les registres officiels (*Ciubotaru c. Moldova*, 2010, § 59) constitue une ingérence dans son droit au respect de la vie privée. Dans certaines circonstances, notamment lorsque des considérations tenant à la sûreté de l'État, à la défense et la sécurité publique entrent en jeu, une telle ingérence n'est pas nécessairement incompatible avec l'article 8 (*Dalea c. France* (déc.), 2010). L'existence de garanties contre l'arbitraire et la possibilité de la faire contrôler, de manière contradictoire, par un organe indépendant et impartial, habilité à se pencher sur toutes les questions de fait et de droit pertinentes, pour trancher sur la légalité de la mesure et sanctionner un éventuel abus des autorités sont essentielles (*ibidem*, faisant référence à *Leander c. Suède*, 1987, § 66).

298. Des informations de nature personnelle fausses ou incomplètes recueillies et conservées par les autorités peuvent rendre plus difficile la vie quotidienne du sujet des données (*Khelili c. Suisse*, 2011, § 64), s'avérer diffamatoires (*Rotaru c. Roumanie* [GC], 2000, § 44) ou peuvent écarter un certain nombre de garanties procédurales importantes prévues par la loi pour protéger les droits des sujets des données (*Cemalettin Canlı c. Turquie*, 2008, §§ 35, 40-42). Dans une affaire où un fichier de la police intitulé « note d'information sur les autres infractions » avait été produit devant une juridiction nationale faisant état de deux actions pénales dirigées dans le passé pour appartenance à des organisations illégales contre l'individu mis en examen, la Cour a conclu à une violation de l'article 8. En l'occurrence, non seulement les informations indiquées dans le fichier étaient fausses, mais il n'y était nulle part fait mention de l'acquittement de l'intéressé au cours de la première action pénale et de l'abandon des poursuites au cours de la seconde action pénale (*ibidem*, § 42). L'absence de mention concernant l'issue desdites procédures était contraire aux obligations posées sans équivoque par les règles de droit interne, écartant un certain nombre de garanties procédurales importantes prévues par la loi pour protéger les droits du requérant (*ibidem*, 2008, § 42).

299. Le fait d'imposer à un individu qui demande la rectification de ses données personnelles sur les registres officiels de l'État une exigence qui crée, pour lui, un obstacle insurmontable peut s'avérer incompatible avec l'obligation de l'État de garantir le respect effectif de sa vie privée (*Ciubotaru c. Moldova*, 2010, §§ 51-59). Dans une affaire relative à l'impossibilité, pour le requérant, de faire modifier l'inscription de son origine ethnique dans les registres officiels, l'exigence de prouver que ses parents appartenaient à une certaine ethnie a créé pour le sujet des données un obstacle insurmontable à l'enregistrement d'une identité ethnique autre que celle attribuée à ses parents par les autorités (*ibidem*, § 57).

300. Dans le contexte des demandes de rectification des registres d'état civil pour tenir compte de la nouvelle situation d'une personne transsexuelle ayant subi une opération, l'existence d'une nécessaire cohérence, dans l'ordre interne, des pratiques administratives et juridiques est un élément important à prendre en compte afin d'apprécier la nécessité, sous l'angle de l'article 8, des telles demandes (*Christine Goodwin c. Royaume-Uni* [GC], 2002, § 78). Dans une affaire relative au refus des autorités de modifier le registre des naissances, la Cour s'est dit frappée du fait que la conversion sexuelle de l'intéressée, qui avait été opérée en toute légalité, et qui avait été prise en charge par le service national de santé, n'avait pas débouché sur une pleine consécration en droit, comme l'étape ultime et l'aboutissement du processus de transformation long et difficile subi par l'intéressée (*ibidem*, § 78, opérant un revirement de jurisprudence pour tenir compte de l'évolution de la science et de la société depuis des arrêts plus anciens, notamment dans les affaires *Rees c. Royaume-Uni*, 1986, §§ 42-44, *Cossey c. Royaume-Uni,* 1990, §§ 39-40, et *Sheffield et Horsham c. Royaume-Uni* [GC], 1998, §§ 60-61). Lorsqu'un État autorise le traitement et l'intervention chirurgicale permettant de soulager la situation d'une personne transsexuelle, finance tout ou partie des opérations et va jusqu'à consentir à l'insémination artificielle d'une femme qui vit avec un transsexuel, il paraît illogique qu'il refuse de reconnaître les implications juridiques du résultat auquel le traitement conduit (*Christine Goodwin c. Royaume-Uni* [GC], 2002, § 78), ce d'autant plus lorsque les difficultés que pose la rectification d'un sexe initialement inscrit dans le registre des naissances sont loin d'être insurmontables (*ibidem*, § 91).

301. Dans l'affaire *S.V. c. Italie*, 2018 (§ 72), le refus des autorités d'autoriser le changement de prénom d'une personne transsexuelle en cours du processus de transition sexuelle et avant l'aboutissement de l'opération de conversion sexuelle était basé sur une procédure judiciaire rigide qui avait placé la requérante pendant une période déraisonnable de deux ans et demi dans une situation anormale lui inspirant des sentiments de vulnérabilité, d'humiliation et d'anxiété.

302. La Cour a considéré dans l'affaire *Hämäläinen c. Finlande* [GC], 2014 (§§ 87-89), qu'il n'était pas disproportionné de poser comme condition préalable à la reconnaissance juridique d'un changement de sexe que le mariage d'un homme devenu femme avec une autre femme soit transformé en partenariat enregistré, celui-ci représentant une option sérieuse qui offrait aux couples de même sexe une protection juridique pratiquement identique à celle du mariage, le droit finlandais interdisant le mariage homosexuel. Par conséquent, on ne saurait dire que, du fait des différences mineures qui existaient entre ces deux formes juridiques d'union, le système en vigueur ne permettait pas à l'État finlandais de remplir les obligations positives qui lui incombaient. Voir aussi l'affaire *A.P., Garçon et Nicot c. France*, 2017, sur les conditions légales d'un changement d'état civil pour les personnes transgenres telles que l'irréversibilité de la transformation de l'apparence (§§ 116-135), la réalité du syndrome transsexuel (§§ 138-144) et l'obligation de subir un examen médical (§§ 149-154).

3. Droit à l'effacement

303. La question du droit à l'effacement des données personnelles après l'écoulement d'un certain laps de temps a été abordée par la Cour dans divers contextes et, en particulier s'agissant :

- du « droit à l'oubli » concernant une décision ou une pratique des médias consistant à (re)publier ou garder disponibles sur leurs sites web des informations ou des archives comportant des données à caractère personnel, dont les nom, prénom et photographies des intéressés, qui avaient été divulguées dans le passé (*Węgrzynowski et Smolczewski c. Pologne*, 2013 ; *M.L. et W.W. c. Allemagne*, 2018 ; *Biancardi c. Italie*, 2021 ; *Mediengruppe Österreich GmbH c. Autriche*, 2022 ; *Hurbain c. Belgique* [GC], 2023) ;
- de la possibilité pour des individus accusés ou seulement soupçonnés d'avoir commis une infraction d'obtenir, passé un certain délai, l'effacement de leurs données à caractère personnel (profile ADN, photos d'identité et empreintes digitales), recueillies par les

autorités dans des bases de données visant à prévenir et à combattre la criminalité (*B.B. c. France*, 2009 ; *Gardel c. France*, 2009 ; *M.B. c. France*, 2009 ; *M. K. c. France*, 2013 ; *Brunet c. France*, 2014 ; *Ayçaguer c. France*, 2017 ; *Catt c. Royaume-Uni*, 2019 ; *Gaughran c. Royaume-Uni*, 2020) ;

- de l'impossibilité pour un individu d'obtenir l'effacement de ses antécédents de son casier judiciaire passé un certain délai (*M.M. c. Royaume-Uni*, 2012) ;
- de la conservation prolongée dans les archives de la Sécurité des données personnelles des requérants qui ne répondaient plus à l'exigence de « nécessité dans une société démocratique » compte tenu de leur nature et de leur ancienneté (*Segerstedt-Wiberg et autres c. Suède*, 2006).

a. « Droit à l'oubli »

304. Si la notion de « droit à l'oubli » est née récemment et est toujours en voie de construction, son application en pratique connaît déjà beaucoup de particularités (*Hurbain c. Belgique* [GC], 2023, §§ 191 and 194). Cette notion s'est forgée pour la première fois dans la pratique judiciaire nationale dans le cadre de la reprise par la presse d'informations à caractère judiciaire déjà divulguées par le passé, la personne revendiquant un « droit à l'oubli » cherchant dans la pratique à obtenir la condamnation de la personne ayant repris ces informations (*ibidem*, § 194). Ensuite, une nouvelle modalité de ce « droit à l'oubli » s'est développée dans la pratique judiciaire nationale dans le contexte de la numérisation des articles de presse qui a engendré leur diffusion extensive sur les sites Internet des journaux concernés. L'effet de cette diffusion a été simultanément renforcé par le référencement réalisé par les moteurs de recherche. Cette modalité, consacrée au niveau terminologique comme le « droit à l'oubli numérique », a concerné des demandes de suppression ou de modification des données disponibles sur Internet ou de limitation de leur accès, demandes adressées à l'éditeur de presse ou à l'exploitant d'un moteur de recherche. Dans ce cas, n'est plus en cause la réapparition d'une information, mais la permanence d'une information sur Internet (*ibidem*, § 195). En effet, de manière générale, le « droit à l'oubli » peut donner lieu en pratique à différentes mesures qui peuvent être prises par les exploitants de moteurs de recherche ou par les éditeurs de presse. Ces mesures visent soit le contenu même d'un article archivé, comme, par exemple, la suppression, la modification ou l'anonymisation d'un article, soit la limitation de l'accessibilité de l'information. Dans ce dernier cas, la limitation de l'accès peut s'effectuer à la fois par les moteurs de recherche et par les éditeurs de presse. (*ibidem*, § 175).

305. Dans sa pratique, la Cour a eu à connaître de plusieurs affaires relatives à des demandes de suppression, de modification, d'anonymisation ou de désindexation d'articles de presse renfermant des données à caractère personnel. Elle a examiné ces affaires sous l'angle soit de l'article 8, lorsque les personnes l'ayant saisie invoquaient leur droit au respect de leur vie privée (*Węgrzynowski et Smolczewski c. Pologne*, 2013 ; *M.L. et W.W. c. Allemagne*, 2018), soit de l'article 10, lorsqu'elle était saisie par des journalistes, des éditeurs ou des propriétaires de médias qui invoquaient leur droit à la liberté d'expression (*Biancardi c. Italie*, 2021 ; *Mediengruppe Österreich GmbH c. Autriche*, 2022 ; *Hurbain c. Belgique* [GC], 2023).

306. Plus spécifiquement, l'affaire *Biancardi c. Italie*, 2021, a donné à la Cour l'occasion, pour la première fois, de statuer sur la compatibilité avec l'article 10 de la condamnation au civil d'un journaliste pour non-désindexation d'informations publiées sur Internet. Au cœur de l'affaire se trouvait le défaut de désindexation par le requérant des informations sensibles publiées, qui portaient sur des poursuites pénales engagées contre des particuliers, et sa décision de garder aisément accessible l'article. L'anonymat des protagonistes dans l'article en ligne n'était pas en cause dans cette affaire. La Cour a relevé que l'article était resté en ligne et aisément accessible pendant huit mois, alors que les intéressés en avaient formellement demandé la suppression. La sévérité de la sanction – mise en jeu de la responsabilité civile et non pénale – et le montant de l'indemnité octroyée n'ont pas été jugés excessifs par la Cour.

307. Dans le contexte de la publication initiale d'informations relatives au passé d'un individu, la Cour a eu à connaître de l'affaire *Mediengruppe Österreich GmbH c. Autriche*, 2022, qui concernait l'interdiction que les juridictions internes avaient faite à un quotidien de publier des informations concernant un individu qui était indirectement lié à la campagne électorale d'un candidat à l'élection présidentielle. Le quotidien en question avait publié une photographie du frère du chef de bureau du candidat, qui était actif dans les « milieux de droite », et il avait révélé que l'intéressé était un « néonazi condamné ». Or, plus de vingt ans séparaient cette condamnation de la publication de l'article en cause, et quelque dix-sept ans s'étaient écoulés depuis la libération de l'intéressé. De plus, la condamnation avait déjà été effacée du casier judiciaire de l'intéressé au moment de la publication de l'article en cause. La juridiction supérieure nationale avait pointé une absence de lien temporel et avait interdit à la société requérante de publier des photographies du frère du chef de bureau sans avoir obtenu le consentement de l'intéressé s'il était indiqué dans le même article qu'il s'agissait d'un néo-nazi qui avait été condamné. Concluant à la non-violation de l'article 10, la Cour a tenu compte, en particulier, du délai qui s'était écoulé entre la condamnation, la libération et la publication de l'article en question, de la perte de notoriété de l'intéressé, du fait que l'intéressé n'avait fait l'objet d'aucune condamnation pénale auparavant, de l'importance de la réinsertion sociale des personnes ayant purgé leur peine, et de l'intérêt légitime et très important de ces personnes à ne plus se voir confrontées à leur condamnation après un certain laps de temps.

308. En ce qui concerne les archives web des médias comportant des données à caractère personnel relatives à un individu ayant fait l'objet d'une publication par le passé, la Cour a souligné que ce contexte était différent comparé à celui d'affaires concernant des publications initiales (*Hurbain c. Belgique* [GC], 2023, § 205), et que c'était donc principalement la question de la permanence de telles informations sur Internet, et non celle de leur publication initiale, qui se posait (*ibidem*, § 174).

309. Dans ce contexte, la Cour a considéré dans l'affaire *Węgrzynowski et Smolczewski c. Pologne* (2013 §§ 60-70) que le refus des tribunaux d'ordonner le retrait d'un article portant atteinte à la réputation d'un avocat et disponible dans les archives Internet d'un journal ne s'analysait pas en une violation de l'article 8. Elle a admis que ce n'était pas le rôle des autorités judiciaires de réécrire l'histoire en ordonnant le retrait du domaine public de toute trace de publications passées qui, par des décisions judiciaires définitives, avaient été jugées constituer des atteintes injustifiées à la réputation d'individus (*ibidem*, § 65). Elle a rappelé en outre que l'intérêt légitime du public à l'accès aux archives électroniques publiques de la presse est protégé par l'article 10 (*ibidem*, § 65). Elle a ajouté qu'il importait de noter que les juridictions polonaises avaient indiqué qu'il serait souhaitable d'ajouter à l'article figurant sur le site Internet du journal un commentaire informant le public de l'issue de la première procédure. Elle y a vu un signe que les tribunaux internes étaient conscients de l'incidence que pouvaient avoir les publications sur Internet sur la protection effective des droits des individus et de l'importance qu'il y avait à diffuser des informations complètes sur des décisions judiciaires concernant un article litigieux mis en ligne sur le site Internet du journal. Or, a-t-elle fait observer, l'avocat n'avait pas demandé l'ajout à l'article litigieux d'une référence aux jugements rendus en sa faveur (*ibidem*, §§ 66-67).

310. Dans l'affaire *M.L. et W.W. c. Allemagne*, 2018, deux individus, qui avaient été condamnés pour meurtre et avaient été libérés quatorze années plus tard, après avoir purgé leur peine de prison, demandaient sans succès que des archives web de journaux et de radios cessent d'afficher leurs photos et de mentionner leurs identités complètes (noms et prénoms) afin qu'ils puissent refaire leur vie à l'abri des regards. La Cour a conclu à la non-violation de l'article 8, estimant que l'intérêt du public à disposer d'archives au contenu véridique et objectif devait primer (*ibidem*, § 116). En particulier, la Cour a eu égard au fait que les reportages litigieux contribuaient toujours, au moment de l'introduction de leurs demandes d'anonymisation, à un débat d'intérêt général, à la circonstance que les requérants n'étaient pas de simples personnes inconnues du public, au comportement des requérants envers la presse à laquelle ils s'étaient adressés postérieurement à leur condamnation en vue d'obtenir la révision de celle-ci, à la circonstance que les reportages relataient les faits de

manière objective et sans l'intention de présenter les requérants d'une manière dénigrante ou de nuire à leur réputation, ainsi qu'à l'accessibilité limitée des informations litigieuses (*ibidem*, §§ 98-115).

311. Dans l'affaire *Hurbain c. Belgique* [GC], 2023, la Cour a réexaminé sa jurisprudence existante et ajusté les critères à appliquer pour la mise en balance des droits respectifs découlant des articles 8 et 10 concernant le maintien à disposition d'une version archivée électronique d'un article qui divulguait des données à caractère personnel concernant un individu. L'affaire avait été portée devant la Cour par un éditeur de presse qui avait été condamné par les juridictions internes à anonymiser une version archivée en ligne d'un article publié une vingtaine d'années auparavant et donnant une version fidèle d'un accident mortel, au nom du « droit à l'oubli » du conducteur à l'origine de cet accident.

312. Dans son arrêt, la Cour a reconnu les effets négatifs du maintien à disposition de certaines informations sur Internet, et en particulier l'impact considérable sur la manière dont la personne concernée était perçue par l'opinion publique, ainsi que les risques liés à la création d'un profil de la personne concernée et à une présentation fragmentée et déformée de la réalité. Elle a néanmoins expliqué que la prétention à l'oubli ne constitue pas un droit autonome protégé par la Convention et, pour autant qu'elle est couverte par l'article 8, ne peut concerner que certaines situations et informations (*ibidem*, § 199).

313. La Cour a ensuite précisé que la mise en balance des droits pertinents (de valeur égale) devant être effectuée lors de l'examen d'une demande d'altération d'un contenu journalistique archivé en ligne doit prendre en considération les critères suivants : i) la nature de l'information archivée ; ii) le temps écoulé depuis les faits, depuis la première publication et depuis la mise en ligne de la publication ; iii) l'intérêt contemporain de l'information ; iv) la notoriété de la personne revendiquant l'oubli et son comportement depuis les faits ; v) les répercussions négatives dues à la permanence de l'information sur Internet ; vi) le degré d'accessibilité de l'information dans des archives numériques, et vii) l'impact de la mesure sur la liberté d'expression, plus précisément la liberté de la presse (*ibidem*, § 205).

314. La Cour a également souligné que le plus souvent, il faudra tenir compte de plusieurs critères à la fois afin de décider de la protection à accorder à la vie privée face aux autres intérêts en présence et aux moyens qui ont été mis en œuvre pour donner effet à cette protection dans un cas donné. Elle a ajouté que la protection de la vie privée dans le contexte d'une revendication à l'oubli ne saurait donc être considérée en faisant abstraction des moyens avec lesquels elle a été mise en œuvre concrètement, et que, sous cet angle, il s'agira de procéder à une mise en balance en vue de conclure si, eu égard au poids des intérêts concurrents et à l'intensité des moyens mis en œuvre dans le cas concret, le poids donné au « droit à l'oubli », à travers le droit au respect de la vie privée, ou à la liberté d'expression a été excessif ou non. Elle a également précisé que les critères à appliquer n'ont pas tous le même poids, et qu'il convient donc d'accorder une attention particulière à une pondération adéquate entre, d'une part, les intérêts des particuliers à l'origine de la demande et, d'autre part, l'impact de pareilles demandes sur les éditeurs. Elle a considéré que le principe de la préservation de l'intégrité des archives de presse implique de veiller à ce que les modifications et *a fortiori* suppressions d'archives soient limitées au strict nécessaire, de façon à prévenir tout effet dissuasif de telles mesures sur l'exercice par la presse de sa mission d'information et d'archivage (*ibidem*, §§ 206 et 211).

315. Lorsqu'elle a appliqué les critères évoqués ci-dessus dans les circonstances du cas d'espèce dont elle se trouvait saisie, la Cour a noté que les juridictions nationales avaient pris en compte de manière cohérente la nature et la gravité des faits de nature judiciaire relatés dans l'article litigieux, l'absence d'actualité ou d'intérêt historique ou scientifique de celui-ci, ainsi que l'absence de notoriété de l'individu concerné. Elle a également relevé que les juridictions en question avaient attaché de l'importance au préjudice grave souffert par l'intéressé à la suite du maintien en ligne de

l'article litigieux en libre accès, qui était de nature à créer un « casier judiciaire virtuel », eu égard notamment au temps qui s'était écoulé depuis la publication de l'article d'origine. Elle a ajouté qu'après un examen des mesures envisageables pour la mise en balance des droits en présence, les juridictions concernées avaient conclu que l'anonymisation litigieuse ne constituait pas, pour le requérant, une charge exorbitante et excessive, tout en représentant, pour l'individu concerné, la mesure la plus efficace pour la protection de sa vie privée (*ibidem*, § 255). Elle a donc estimé que les juridictions internes avaient dûment mis en balance les intérêts en jeu, et elle a conclu à la non-violation de l'article 10 (*ibidem*, § 256).

b. Autres contextes

316. Dans l'affaire *M.M. c. Royaume-Uni*, 2012 (§§187-207), l'inscription à vie d'un avertissement dans le casier judiciaire d'une personne a emporté un constat de violation de l'article 8. Pour la Cour, la condamnation ou l'avertissement infligé dans le passé à un individu deviennent, au fil du temps, partie intégrante de sa vie privée, qui doit être respectée. Bien que les données figurant dans le casier judiciaire soient, dans un certain sens, des informations publiques, leur mémorisation systématique dans les fichiers centraux signifie qu'elles peuvent être divulguées bien après l'événement, lorsque tout le monde, hormis la personne concernée, aura vraisemblablement oublié l'incident. La Cour a jugé préoccupant le fait que des critères de contrôle qui permettraient l'effacement de ces données étaient très restrictifs et que les demandes de suppression n'étaient accordées que dans des circonstances exceptionnelles (*ibidem*, § 202).

317. Pour la Cour, lorsqu'un État se place aux confins de sa marge d'appréciation en s'attribuant le pouvoir le plus étendu en matière de conservation des données, celui de conserver des données sans limitation de durée, l'existence de certaines garanties effectives permettant la suppression des données à caractère personnel dès que la poursuite de leur conservation devient disproportionnée est déterminante (*Catt c. Royaume-Uni*, 2019, § 119 ; *Gaughran c. Royaume-Uni*, 2020, § 94). Dans une affaire où les données biométriques et les photographies du requérant, condamné pour conduite en état d'ébriété, avaient été conservées conformément à la politique de conservation illimitée des données personnelles de toute personne reconnue coupable d'une infraction, la Cour est parvenue à un constat de violation de l'article 8 (*ibidem*, § 98). Aucune disposition ne permettait au requérant de présenter une demande d'effacement si la conservation des données le concernant n'apparaissait plus pertinente compte tenu de la finalité du fichier, au regard de la nature de l'infraction qu'il avait commise, de son âge lors de sa commission, du temps écoulé depuis lors et de sa personnalité actuelle. La police n'avait le pouvoir d'effacer les données biométriques et les photographies de personnes reconnues coupables que dans des cas exceptionnels. Les possibilités de réexamen étaient tellement restreintes qu'elles en devenaient presque hypothétiques (*ibidem*, § 94).

318. L'absence de garanties effectives concernant l'effacement des données personnelles lorsqu'elles n'apparaissent plus pertinentes au regard de la finalité du fichier est particulièrement préoccupante s'agissant des catégories sensibles des données personnelles conservées, qui appellent une protection accrue (*Catt c. Royaume-Uni*, 2019, § 112). Dans une affaire relative à la conservation dans une base de données de la police de données sensibles relatives à un manifestant pacifique, révélant ses opinions politiques, la Cour a conclu à la violation de l'article 8 (*ibidem*, § 128). En l'absence de toute règle fixant la durée maximale de conservation de pareilles données, le requérant dépendait entièrement de la diligence avec laquelle les autorités appliqueraient les garanties du code de pratique applicable, très souples par nature, pour veiller au caractère proportionné de la durée de conservation des données le concernant. Pour la Cour, la garantie d'obtenir l'effacement des données a un effet limité dans le cas où les autorités refusent, suite à une demande du sujet des données, de supprimer les données concernées ou de motiver leur décision de les conserver (*ibidem*, §§ 118 et 122).

319. Dans plusieurs affaires relatives à la conservation des données personnelles des individus condamnés pour des agressions sexuelles, la Cour est parvenue à un constat de non-violation de l'article 8 après avoir constaté que les sujets des données pouvaient présenter une demande d'effacement si la conservation des données les concernant n'apparaissait plus pertinente compte tenu, entre autres, du temps écoulé depuis leur condamnation (*B.B. c. France*, 2009, §§ 66-68 ; *Gardel c. France*, 2009, §§ 67-69 ; *M.B. c. France*, 2009, §§ 58-60). Dans le même temps, l'absence de toute possibilité de demander l'effacement des données n'emporte pas nécessairement violation de l'article 8 et doit être appréciée à la lumière du but poursuivi par la conservation de ces données, de la nature des données ainsi que des garanties offertes aux personnes concernées contre le risque d'arbitraire et d'abus. En particulier, la Cour a jugé que lorsque les données pertinentes conservées dans une base de données interne du ministère de la Justice ne présentent pas un caractère « sensible » au sens de l'article 6 de la *Convention 108*, qu'elles se limitent à des informations factuelles et des éléments objectifs relatifs aux procédures judiciaires auxquelles une personne est partie, et que leur traitement vise la bonne administration de la justice et le bon fonctionnement des services publics concernés et s'accompagne de garanties appropriées (possibilité de veiller à l'exactitude des données et limitation dans le temps de leur conservation), l'absence de procédure permettant d'obtenir l'effacement anticipé de ces données n'est pas disproportionnée (*L.F. c. France* (déc.), 2024, §§ 44-47).

320. Dans l'affaire *Peruzzo et Martens c. Allemagne* (déc.), 2013 (§ 46), relative à la conservation des données personnelles dans un fichier suite à une condamnation pour des faits graves liés à un trafic de stupéfiants, la Cour a été satisfaite du fait que, bien qu'il n'y ait pas de délais maximaux prescrits par la loi pour le stockage des profils ADN, l'Office fédéral de la criminalité était tenue de vérifier à intervalles réguliers, qui ne devaient pas dépasser dix ans, si le maintien du stockage des données était toujours nécessaire compte de la finalité pour laquelle les données avaient été conservées ainsi que de la nature et de la gravité des circonstances de l'affaire.

321. Dans l'affaire *Ayçaguer c. France*, 2017 (§ 44), la Cour est parvenue à un constat de violation de l'article 8 estimant que le régime de conservation des profils ADN dans le fichier national des infractions, auquel le requérant s'était opposé en refusant le prélèvement de ses données personnelles, n'offrait pas une protection suffisante à l'intéressé en raison tant de sa durée que de l'absence de possibilité d'effacement (*ibidem*, § 45). La Cour a souligné que les personnes condamnées devraient, à l'instar des personnes soupçonnées d'avoir commis une infraction, relaxées ou acquittées, se voir offrir une possibilité concrète de présenter une requête en effacement des données mémorisées et ce afin que la durée de conservation soit proportionnée à la nature des infractions et aux buts des restrictions (*ibidem*, § 45 ; *B.B. c. France*, 2009, § 68 ; *Brunet c. Francee*, 2014, §§ 41-43).

322. La possibilité prévue en droit interne d'obtenir l'effacement des données s'avère une garantie « théorique et illusoire » et non « concrète et effective » lorsque le droit de présenter à tout moment une demande d'effacement de ces données au juge risque de se heurter à l'intérêt des services d'enquêtes de disposer d'un fichier ayant le plus de références possibles, et si les intérêts en présence sont, ne serait-ce que partiellement, contradictoires (*M. K. c. France*, 2013, §§ 44-47).

323. Dans l'affaire *Segerstedt-Wiberg et autres c. Suède*, 2006 (§§ 73-92), la conservation dans les dossiers des services de la sûreté de l'État des données à caractère personnel très anciennes des requérants, qui avaient trait à leur participation à une réunion politique, au fait qu'il avaient préconisé d'opposer une résistance violente aux contrôles de police durant des manifestations ou à leur appartenance à un certain parti politique, a emporté une violation de l'article 8. Pour la Cour, l'intérêt de l'État à la protection de la sécurité nationale et à la lutte contre le terrorisme qui justifiait le fait de recueillir et conserver ces informations devait être mis en balance avec la gravité de l'ingérence dans l'exercice par chacun des requérants de son droit au respect de sa vie privée. Compte tenu de la nature de ces renseignements et de leur ancienneté, les motifs ayant justifié la

conservation des informations relatives aux intéressés, bien que pertinents, ne sauraient être considérés comme suffisants près de trente ans après avoir été recueillis (*ibidem*, § 90).

4. Droit de jouir de garanties spéciales de procédure et d'un cadre procédural efficace pour faire valoir ses droits

324. Bien que l'article 8 ne contienne aucune exigence procédurale explicite, il est important, pour la jouissance effective des droits garantis par cet article, que le processus décisionnel pertinent soit équitable et de nature à respecter dûment les intérêts qu'il protège. Il doit permettre au demandeur de faire valoir ses droits dans des conditions d'équité, y compris en matière de preuve (*I. c. Finlande*, 2008, § 44 ; *Ciubotaru c. Moldova*, 2010, § 51). Le fait d'imposer une exigence qui crée un obstacle insurmontable pour une personne qui demande la rectification de ses données d'identité sur les registres officiels de l'État peut s'avérer incompatible avec l'obligation positive de l'État de garantir le respect effectif du droit au respect de sa vie privée (*ibidem*, §§ 51-59). Dans une affaire relative à la divulgation de la séropositivité de la requérante, la Cour, en constatant une violation de l'article 8, a accordé du poids au fait que l'État avait imposé une charge de la preuve trop lourde à la requérante dans le cadre d'une procédure civile au cours de laquelle elle avait demandé réparation pour la diffusion d'informations sur son état de santé (*I. c. Finlande*, 2008, § 44).

325. Des restrictions imposées par la loi au pouvoir octroyé aux tribunaux nationaux pour réparer le préjudice subi suite à la divulgation, par voie de presse, d'informations confidentielles sur la santé des personnes identifiées, et pour dissuader la répétition de tels abus sont de nature à entraver l'effectivité d'un éventuel recours, privant les intéressés des mesures de protection de leur vie privée qu'ils étaient en droit d'espérer. Ainsi, dans les affaires *Armonienė c. Lituanie*, 2008 (§§ 47-48) et *Biriuk c. Lituanie*, 2008 (§§ 46-47), la Cour est parvenue à un constat de violation de l'article 8 en raison du plafonnement, par la loi sur la diffusion d'informations au public en vigueur à l'époque des faits, des dommages-intérêts alloués aux requérants par les tribunaux nationaux suite à la révélation de leur séropositivité dans le plus grand quotidien national, sans leur consentement et en dévoilant leur identité. En outre, la Cour a conclu à l'ineffectivité d'un recours purement indemnitaire dans un cas où le requérant se plaignait d'une situation continue découlant d'une protection inadéquate de données personnelles le concernant qui étaient conservées dans une base de données détenue par l'État (le Service d'information sur les contribuables), et où, pendant longtemps, les autorités n'avaient pas empêché les abus en matière d'accès à la base de données en question (*Casarini c. Italie* (déc.), 2024, § 89).

326. La défaillance de l'État de prévoir, au niveau national, l'exercice d'un contrôle indépendant de la nécessité de conserver des données à caractère personnel recueillies dans le cadre d'une procédure pénale ou à la suite d'une procédure pénale terminée par un acquittement, un classement sans suite ou une condamnation, est un élément important à prendre en compte pour déterminer si une telle conservation des données est conforme ou non avec l'article 8 (*S. et Marper c. Royaume-Uni* [GC], 2008, §§ 119, 125). Dans une affaire relative à la conservation non limitée dans le temps des échantillons cellulaires, profils ADN et empreintes digitales de deux individus après que les poursuites pénales menées contre eux aient été terminées par un acquittement et, respectivement, par une décision de classement sans suite, la Cour a conclu à une violation de l'article 8 après avoir constaté qu'il n'existait que peu de possibilités pour eux d'obtenir l'effacement des données de la base nationale ou la destruction des échantillons.

327. Dans l'affaire *Vicent Del Campo c. Espagne*, 2018 (§§ 39, 53), le fait pour le requérant, tierce partie à une procédure judiciaire, de se trouver privé de la possibilité de demander à une juridiction nationale de s'abstenir de communiquer son identité ou des informations personnelles le concernant avant le prononcé d'un arrêt, l'a privé d'un cadre procédural efficace pour faire valoir ses droits.

328. Le manquement des autorités à procéder à une analyse de proportionnalité en mettant en balance les intérêts divergents en jeu et à tenir compte du droit du requérant au respect de sa vie privée et des questions de protection des données emporte non-respect des exigences de l'article 8 de la Convention (*Liebscher c. Autriche*, 2021, §§ 64-69).

329. Dans l'affaire *M.D. et autres c. Espagne*, 2022 (§§ 65-72), qui concernait la fuite dans la presse de données à caractère personnel concernant les requérants et provenant d'une base de données de la police à laquelle seules les autorités avaient accès, la Cour, au regard de l'ampleur de cette divulgation illégale de données privées conservées par une autorité publique, a considéré que l'obligation positive tirée de l'article 8 impliquait une « obligation de mener une enquête effective » visant à déterminer dans quelles circonstances les journalistes avaient eu accès aux données et, le cas échéant, sanctionner les personnes responsables des défaillances constatées. Elle a vu dans le manquement des autorités à leur obligation de mener une telle enquête une violation de l'article 8. De même, dans l'affaire *Y.G. c. Russie*, 2022 (§§ 46-53), où le requérant alléguait qu'une base de données contenant des données à caractère personnel le concernant, y compris des informations sur son état de santé, avait été proposée à la vente, elle a considéré que face à une atteinte à la vie privée d'une telle ampleur, le requérant, s'il agissait de son propre chef et sans bénéficier de l'aide de l'État sous la forme d'une enquête officielle, ne disposait d'aucun moyen effectif pour identifier les auteurs de tels actes. Elle en a conclu que la plainte pénale que le requérant avait déposée ne constituait pas une voie de recours inappropriée au vu de ces circonstances. Elle a estimé qu'en ne menant pas d'enquête, les autorités avaient manqué à l'obligation positive qui leur incombait de veiller à offrir à l'intéressé une protection adéquate de son droit au respect de sa vie privée.

330. Dans l'affaire *Casarini c. Italie* (déc.), 2024, §§ 92-105, où un agent de la garde des finances avait, de manière illicite, consulté à plusieurs reprises les données à caractère personnel concernant le requérant qui étaient conservées dans la base de données du Service d'information sur les contribuables, puis les avait communiquées à un journaliste en vue de leur publication, la Cour a considéré qu'une plainte devant l'autorité de protection des données aurait constitué une voie de recours effective, et que cette voie de recours aurait donc dû être épuisée. L'autorité de protection des données n'était pas un organe judiciaire, certes, mais il s'agissait d'un organe administratif pleinement autonome, libre de toute pression extérieure : les procédures devant cet organe étaient contradictoires par nature, et elles donnaient lieu à des décisions ayant force obligatoire qui pouvaient être contestées devant les autorités judiciaires compétentes et étaient susceptibles d'un pourvoi en cassation devant la Cour de cassation.

331. L'effectivité des recours accessibles au niveau national aux personnes qui souhaitent avoir accès à leurs données personnelles exige que les sujets des données puissent obtenir le traitement de leurs demandes dans un délai raisonnable. Dans l'affaire *Roche c. Royaume-Uni* [GC], 2005 (§§ 166-167, 169), la Cour a conclu à une violation de l'article 8 en raison d'un délai d'attente jugé déraisonnable avant que le requérant ait pu accéder aux documents comportant des données personnelles qui lui auraient permis d'évaluer les risques pour sa santé pouvant résulter de sa participation à des tests militaires sur des gaz.

332. Des délais stricts ou des limitations procédurales nécessitent également un contrôle. Dans l'affaire *Moldovan c. Ukraine*, 2024, (§§ 52-53), le requérant se plaignait de ce que les juridictions internes saisies de sa demande de reconnaissance de son père biologique avaient appliqué d'anciennes dispositions légales rendant la preuve d'une cohabitation indispensable à la reconnaissance d'un lien de filiation malgré les tests ADN disponibles. La Cour a considéré que les effets d'une telle approche des juridictions internes étaient comparables à ceux de délais rigides ou d'autres limitations procédurales. Elle a conclu que cette approche, combinée avec le fait que la juridiction interne n'avait pas traité de manière suffisamment minutieuse les preuves génétiques qui lui avaient été soumises, s'analysait en un manquement aux obligations positives incombant aux juridictions internes en vertu de l'article 8 de la Convention.

333. Une trop grande importance accordée, par les autorités nationales, à l'exigence de confidentialité des données de trafic des utilisateurs d'Internet peut, dans certaines circonstances, s'avérer contraire à l'article 8 si elle est de nature à entraver l'efficacité d'une enquête pénale permettant d'identifier et de sanctionner l'auteur d'une infraction (*K.U. c. Finlande,* 2008, § 49). Dans l'affaire *K.U. c. Finlande*, 2008 (§§ 49-50), la Cour a conclu à la violation de l'article 8 en raison de l'inexistence d'une cadre procédural qui puisse permettre d'identifier et de traduire en justice une personne qui a publié sur Internet une annonce qui faisait d'un mineur une cible pour les pédophiles, de manière à ce que la victime puisse obtenir une réparation pécuniaire de sa part. La garantie qu'ont les utilisateurs de télécommunications et de services Internet que leur intimité sera respectée doit parfois s'effacer devant d'autres impératifs légitimes tels que la défense de l'ordre et la prévention des infractions pénales ou la protection des droits et libertés d'autrui.

334. En matière de sécurité nationale, toute personne qui fait l'objet d'une mesure basée sur ces motifs doit avoir la possibilité de faire contrôler la mesure litigieuse par un organe indépendant et impartial, habilité à se pencher sur toutes les questions de fait et de droit pertinentes et à sanctionner si nécessaire un éventuel abus des autorités. Devant cet organe de contrôle, la personne concernée doit bénéficier d'une procédure contradictoire afin de pouvoir présenter son point de vue et réfuter les arguments des autorités. Ainsi, dans l'affaire *Dalea c. France* (déc.), 2010, la Cour a jugé que l'inscription de longue durée des données personnelles du requérant dans le fichier d'information Schengen pouvait être considéré « nécessaire dans une société démocratique » puisque l'intéressé avait bénéficié d'un contrôle de la mesure litigieuse. Même s'il ne s'était pas vu offrir la possibilité de s'opposer au motif précis de cette inscription, il avait eu connaissance de toutes les autres données le concernant figurant dans le fichier Schengen.

335. L'organe indépendant et impartial devant lequel toute personne qui fait l'objet d'une mesure basée sur des motifs de sécurité nationale doit avoir la possibilité de faire contrôler la mesure litigieuse n'est pas nécessairement un organe judiciaire. Dans l'affaire *Leander c. Suède*, 1987 (§ 59), concernant l'utilisation d'un fichier secret de police pour l'embauche d'un charpentier, la Cour a conclu à la non-violation de l'article 8 en présence de garanties consistant notamment en la possibilité, pour le parlement et les institutions indépendantes, d'exercer un contrôle sur les opérations autorisant les autorités internes compétentes à recueillir et à mémoriser dans des fichiers secrets des renseignements sur des personnes, puis à les utiliser (*ibidem*, § 65) et même si le requérant ne disposait pas d'un droit à un recours juridictionnel (*ibidem*, §§ 62, 67). Pour apprécier l'efficacité d'un recours devant un organe appelé, au niveau interne, à contrôler une mesure basée sur des motifs de sécurité nationale, ce sont les pouvoirs et les garanties de procédure dont l'organe en question s'entoure qui entrent en ligne de compte (*ibidem*, §§ 77, 80, 83-84). Un recours hiérarchique auprès d'un supérieur direct de l'autorité dont les actes sont contestés ne répond pas aux critères d'indépendance requis pour pouvoir constituer une protection suffisante contre l'abus de pouvoir (*Roman Zakharov c. Russie* [GC], 2015, § 292).

336. Dans le cadre des mesures de surveillance secrète, le contrôle et la supervision de ces mesures peuvent intervenir à trois stades : lorsqu'on ordonne la surveillance, pendant qu'on la mène ou après qu'elle ait cessé. Lors des deux premiers stades, la nature et la logique même de la surveillance secrète commandent d'exercer à l'insu de l'intéressé non seulement la surveillance elle-même mais aussi le contrôle qui l'accompagne. Puisque l'intéressé sera donc empêché d'introduire un recours effectif de sa propre initiative ou de participer directement à une éventuelle procédure de contrôle, il est indispensable que les procédures existantes procurent en elles-mêmes des garanties appropriées et équivalentes afin de sauvegarder les droits de l'individu. Dans un domaine où les abus sont potentiellement 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 (*ibidem*, § 233 ; *Klass et autres c. Allemagne*, 1978, §§ 55-56 ; *Denysyuk et autres c. Ukraine*, 2025, § 88).

337. Au troisième stade, c'est-à-dire lorsque la surveillance a cessé, la question de la notification *a posteriori* de mesures de surveillance est indissociablement liée à celle de l'effectivité des recours judiciaires et donc à l'existence de garanties effectives contre les abus de pouvoir en matière de surveillance (*Roman Zakharov c. Russie* [GC], 2015, § 234). 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 (*Klass et autres c. Allemagne*, 1978, §§ 57-59 ; *Weber et Saravia c. Allemagne* (déc.), 2006, §§ 135-137) 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 (*Kennedy c. Royaume-Uni*, 2010, §§ 167, 169 ; *Roman Zakharov c. Russie* [GC], 2015, § 234).

338. Dans les affaires *Klass et autres c. Allemagne*, 1978 (§§ 57-59) et *Weber et Saravia c. Allemagne* (déc.), 2006 (§§ 135-137), la Cour a trouvé que les recours existants au niveau national étaient suffisants. Les individus dont les communications avaient été surveillées étaient notifiés dès que possible, sans compromettre le but de la surveillance. Les recours s'accompagnaient également de garanties effectives, telles, par exemple, le fait qu'une autorité indépendante avait le pouvoir de décider si une personne faisant l'objet d'une surveillance devait être avisée de cette mesure. À partir de cette notification, diverses voies de recours judiciaires s'ouvraient à l'individu, par exemple, l'introduction d'une action civile en réparation ou une demande devant la Cour constitutionnelle fédérale afin de statuer sur la violation éventuelle de la Loi fondamentale (*Klass et autres c. Allemagne*, 1978, §§ 57, 24).

339. Pour les systèmes qui ne prévoient pas de notification à la personne concernée des mesures prises à son encontre, le fait que les personnes s'estimant lésés dans leur droit au respect de la vie privée par une mesure de surveillance secrète peuvent s'adresser à un organe indépendant et impartial sans même avoir été informées au préalable que leurs communications avaient été interceptées a été jugé par la Cour comme étant une garantie importante dans une affaire où elle a conclu à la non-violation de l'article 8 (*Kennedy c. Royaume-Uni*, 2010, §§ 167, 169). En revanche, lorsque les recours offerts par le système interne sont ouverts uniquement aux personnes qui disposent d'un minimum d'informations sur la mesure incriminée, la Cour a estimé que les intéressés ne disposaient pas d'un recours effectif contre les mesures de surveillance secrètes, en méconnaissance de l'article 8 (*Roman Zakharov c. Russie* [GC], 2015, §§ 293-298, 305 ; *Denysyuk et autres c. Ukraine*, 2025, §§ 116-132).

III. Interaction avec d'autres dispositions de la Convention et de ses Protocoles

340. Hormis le droit au respect de la vie privée et familiale, du domicile et de la correspondance garanti par l'article 8 de la Convention, qui assure, de façon principale, la protection des données à caractère personnel dans le système de la Convention, des questions liées à cette protection peuvent également entrer en jeu sur le terrain d'autres dispositions de la Convention et de ses protocoles additionnels. Il s'agit alors, principalement, pour la Cour, de la mettre en balance et de la concilier avec d'autres droits et intérêts légitimes. Dans certaines affaires, la question de la protection des données à caractère personnel a permis à la Cour de déterminer la portée de l'un ou l'autre des autres droits garantis par la Convention et ses protocoles additionnels.

A. Protection des données et droits substantiels[10]

Article 9 de la Convention

> « 1. Toute personne a droit à la liberté de pensée, de conscience et de religion ; ce droit implique la liberté de changer de religion ou de conviction, ainsi que la liberté de manifester sa religion ou sa conviction individuellement ou collectivement, en public ou en privé, par le culte, l'enseignement, les pratiques et l'accomplissement des rites.
>
> 2. La liberté de manifester sa religion ou ses convictions ne peut faire l'objet d'autres restrictions que celles qui, prévues par la loi, constituent des mesures nécessaires, dans une société démocratique, à la sécurité publique, à la protection de l'ordre, de la santé ou de la morale publiques, ou à la protection des droits et libertés d'autrui. »

Article 10 de la Convention

> « 1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. Le présent article n'empêche pas les États de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisations.
>
> 2. L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire. »

Article 14 de la Convention

> « La jouissance des droits et libertés reconnus dans la présente Convention doit être assurée, sans distinction aucune, fondée notamment sur le sexe, la race, la couleur, la langue, la religion, les opinions politiques ou toutes autres opinions, l'origine nationale ou sociale, l'appartenance à une minorité nationale, la fortune, la naissance ou toute autre situation. »

Article 1 du Protocole nº 1

> « Toute personne physique ou morale a droit au respect de ses biens. Nul ne peut être privé de sa propriété que pour cause d'utilité publique et dans les conditions prévues par la loi et les principes généraux du droit international.
>
> Les dispositions précédentes ne portent pas atteinte au droit que possèdent les États de mettre en vigueur les lois qu'ils jugent nécessaires pour réglementer l'usage des biens conformément à l'intérêt général ou pour assurer le paiement des impôts ou d'autres contributions ou des amendes. »

[10] Ce chapitre doit être lu à la lumière et combiné avec les *Guide sur l'article 9*, *Guide sur l'article 10*, *Guide sur l'article 14 et de article 1 du Protocole n° 12* et le *Guide sur l'article 1 du Protocole n° 1*.

Article 2 du Protocole n° 4

« 1. Quiconque se trouve régulièrement sur le territoire d'un État a le droit d'y circuler librement et d'y choisir librement sa résidence.

2. Toute personne est libre de quitter n'importe quel pays, y compris le sien.

3. L'exercice de ces droits ne peut faire l'objet d'autres restrictions que celles qui, prévues par la loi, constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à la sûreté publique, au maintien de l'ordre public, à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

4. Les droits reconnus au paragraphe 1 peuvent également, dans certaines zones déterminées, faire l'objet de restrictions qui, prévues par la loi, sont justifiées par l'intérêt public dans une société démocratique. »

1. Protection des données et liberté de pensée, de conscience et de religion (article 9 de la Convention)

341. La Cour a jugé de la violation ou de l'absence de violation de l'article 9 dans quelques affaires qui soulevaient également la question de la protection des données personnelles.

342. Dans l'affaire *Sinan Işık c. Turquie*, 2010 (§ 37-53), la Cour a été confrontée à la question de la mention, qu'elle soit obligatoire ou facultative, de la confession du requérant sur sa carte d'identité. À ses yeux, le fait de demander par écrit aux autorités le remplacement d'une religion par une autre sur les registres civils et la carte d'identité, de même que le simple fait d'être porteur d'une carte d'identité comportant une case « religion » laissée vide, revient pour l'intéressé à divulguer contre son gré une information relative à un aspect de sa religion ou de ses convictions les plus profondes. La Cour a conclu à la violation de l'article 9 après avoir rappelé que la liberté de manifester sa religion ou sa conviction comportait un aspect négatif, à savoir le droit de ne pas être obligé de manifester sa religion ou d'agir en sorte qu'on puisse tirer comme conclusion qu'un individu a, ou n'a pas, telles convictions. Même si la case réservée à l'indication de la religion pouvait être laissée vide, le fait même de la laisser vide avait, en soi, une connotation spécifique, puisqu'elle permettrait inévitablement qu'une distinction soit faite entre les titulaires d'une carte d'identité contenant une telle information et ceux qui auront choisi de ne pas l'indiquer (*ibidem,* § 51).

343. Dans l'affaire *Alexandridis c. Grèce*, 2008 (§ 41), l'obligation pour un avocat de révéler, lors d'une prestation de serment, ne pas être chrétien orthodoxe et ne pas souhaiter prêter le serment religieux, afin de pouvoir faire une déclaration solennelle, a porté atteinte à son droit garanti par l'article 9. Les autorités étatiques n'ont pas le droit d'intervenir dans le domaine de la liberté de conscience de l'individu et de rechercher ses convictions religieuses, ou de l'obliger à manifester ses convictions concernant la divinité. Cela est d'autant plus vrai dans le cas où une personne est obligée d'agir de la sorte dans le but d'exercer certaines fonctions, notamment à l'occasion d'une prestation de serment (*ibidem*, § 38). Dans l'affaire *Dimitras et autres c. Grèce*, 2010 (§ 88), l'obligation pesant sur les requérants de révéler leurs convictions religieuses pour ne pas prêter le serment religieux en tant que témoins dans une procédure pénale a aussi emporté une violation de l'article 9. La Cour a estimé que les dispositions du code de procédure pénale, qui prévoyaient, aux fins de vérification de l'identité d'un témoin, et avant son audition, que celui-ci indiquait, parmi d'autres éléments, sa religion, se conciliaient mal avec son droit à la liberté de religion (*ibidem*, § 88).

344. Dans l'affaire *Mockutė c. Lituanie*, 2018 (§ 129), la Cour s'est dit prête à accepter que les besoins d'un traitement psychiatrique pourraient impliquer la nécessité, pour un psychiatre, de discuter de diverses questions, y compris de la religion, avec un patient. Mais de telles discussions ne

devraient pas prendre la forme d'immiscions, par des psychiatres, dans les croyances des patients afin de les « corriger » lorsqu'il n'y a pas de risque clair et imminent que de telles croyances se manifestent dans des actions dangereuses pour le patient ou d'autres personnes. Un État ne peut dicter ce qu'une personne croit ou prendre des mesures coercitives pour lui faire changer ses croyances et la portée de la marge d'appréciation des États ne saurait être plus large ou plus étroite en fonction de la nature des croyances religieuses.

345. Dans l'arrêt *Témoins de Jéhovah c. Finlande*, 2023 (§§ 80-99), la Cour était appelée à décider si un juste équilibre avait été ménagé entre le droit de la communauté requérante à la liberté de religion et le droit au respect de la vie privée des personnes (personnes concernées) auxquelles les membres de la communauté requérante rendaient visite dans le cadre de leurs activités de prédication de porte-à-porte. Au niveau interne, les autorités compétentes avaient constaté que le consentement explicite ou sans équivoque des personnes concernées était requis pendant ces activités dès lors que des données personnelles et sensibles (nom et adresse des intéressés) étaient collectées et traitées. La Cour a admis que l'application de l'obligation de recueillir le consentement des personnes concernées dans le cadre d'une activité de prédication de porte-à-porte – activité religieuse visant à manifester ou à diffuser sa foi – menée par la communauté requérante s'analysait en une ingérence dans les droits de cette communauté garantis par l'article 9 (§ 81). Dans le même temps, elle a considéré que l'ingérence litigieuse était « prévue par la loi », étant donné en particulier que la Cour administrative suprême avait interprété l'acte juridique interne pertinent, lequel avait servi de base aux mesures litigieuses et se fondait lui-même sur la directive pertinente de l'Union européenne, dans le respect de l'interprétation donnée par la Cour de justice de l'Union européenne (§§ 84-88). Elle a ajouté que la mesure litigieuse poursuivait également le but légitime de la protection des « droits et libertés d'autrui » (§ 89) et était « nécessaire dans une société démocratique ». Sur ce dernier point, elle a observé que, si l'obligation de recueillir le consentement de la personne concernée constituait une garantie appropriée et nécessaire pour empêcher toute communication ou divulgation de données personnelles et sensibles dans le cadre des activités de prédication de porte-à-porte menées par la communauté requérante, cette dernière n'avait pas démontré en quoi cette obligation était de nature à porter atteinte à la substance de son droit à la liberté de religion (§ 95). Elle a ajouté que cette obligation s'appliquait à toutes les communautés et activités religieuses (§ 96) et que la communauté requérante, en dépit d'une demande en ce sens, n'avait fait l'objet d'aucune sanction (§ 97).

2. Protection des données et liberté d'expression (article 10 de la Convention)[11]

346. De façon générale dans les affaires où la Cour a été amenée à mettre en balance et à concilier le droit à la protection de données personnelles tel qu'il est garanti par l'article 8, avec le droit à la liberté d'expression, consacré par l'article 10, la Cour a considéré que l'issue ne saurait, en principe, varier selon que l'affaire avait été portée devant elle sous l'angle de l'article 8, ou, sous l'angle de l'article 10. Pour la Cour, ces droits méritent un égal respect (*Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande* [GC], 2017, § 163 ; *Alpha Doryforiki Tileorasi Anonymi Etairia c. Grèce*, 2018, § 46).

347. Le refus par les autorités de donner accès aux organisations non-gouvernementales à certaines informations contenant des données à caractère personnel détenues par l'État a emporté une violation de l'article 10 dans les affaires :

[11] Ce chapitre doit être lu à la lumière et combiné avec le *Guide sur l'article 10* de la Convention (Voir notamment les pp. 26-47 ; 58-60 et 62-65)

- *Centre pour la démocratie et l'état de droit c. Ukraine*, 2020 (§§ 120-121), s'agissant du refus de la Commission électorale centrale de communiquer à une ONG une copie des *curriculum vitae* des chefs de partis politiques en lice aux élections législatives, au motif que les informations demandées avaient un caractère confidentiel et ne pouvaient être communiquées dans leur intégralité qu'avec le consentement des personnes concernées ;
- *Magyar Helsinki Bizottság c. Hongrie* [GC], 2016 (§§ 195-197, 200), où les autorités avaient refusé de communiquer à une ONG réalisant une étude le nom et le nombre de désignations des avocats commis d'office ;
- *Youth Initiative for Human Rights c. Serbie*, 2013 (§§ 24-26), quant au refus d'un service de renseignement de communiquer des informations à une ONG malgré une injonction en ce sens.

348. Concernant la divulgation des données personnelles dans la presse écrite ou dans les moyens d'information audio-visuels, la Cour a conclu à une violation de l'article 10 dans plusieurs affaires, parmi lesquelles :

- *N. Š. c. Croatie*, 2020 (§§ 92-117) où la requérante avait été condamnée pour avoir divulgué, dans une émission de télévision, des informations supposées confidentielles dont elle avait pris connaissance lors d'une procédure administrative sur la garde d'un enfant. En raison de leur vulnérabilité, la protection des données personnelles des enfants est essentielle (*ibidem*, § 99). Cependant, une approche trop formaliste des juridictions nationales, qui ne tient pas compte du contexte de la divulgation, et notamment du fait que les informations divulguées étaient déjà dans le domaine public, n'est pas conforme à l'article 10 (*ibidem*, §§ 115-116) ;
- *Gîrleanu c. Roumanie*, 2018 (§§ 68-100), s'agissant d'une condamnation à une amende administrative sanctionnant la divulgation d'informations militaires confidentielles dans le cadre d'une enquête journalistique.
- *Couderc et Hachette Filipacchi Associés c. France* [GC], 2015 (§§ 94-153), au sujet de la condamnation de la directrice de publication et de la société éditrice d'un hebdomadaire pour la publication d'un article et de photos révélant l'existence de l'enfant caché d'un monarque ;
- *Axel Springer AG c. Allemagne* [GC], 2012 (§§ 75-111), s'agissant de l'interdiction de rendre compte de l'arrestation et de la condamnation d'un acteur connu ;
- *Dupuis et autres c. France*, 2007 (§§ 30-32, 39-49), s'agissant de la condamnation de journalistes pour avoir utilisé et reproduit dans leur livre des éléments du dossier d'une instruction pénale en cours, incluant des données à caractère personnel de l'accusé.

349. À l'inverse, elle a abouti à un constat de non-violation de l'article 10 ou d'irrecevabilité dans plusieurs affaires, parmi lesquelles :

- *Hurbain c. Belgique* [GC], 2023 (§§ 167-257), concernant la condamnation au civil du requérant, un éditeur de presse, à anonymiser l'archive électronique en ligne d'un article mentionnant le nom complet d'un conducteur qui avait été responsable d'un accident de la route mortel survenu de nombreuses années auparavant ;
- *Biancardi c. Italie*, 2021 (§§ 67-71), concernant la condamnation au civil d'un éditeur de presse pour non-désindexation d'informations sensibles, publiées sur Internet, relatives à des poursuites pénales engagées contre un particulier, et la décision du journaliste de les maintenir aisément accessibles malgré l'opposition de l'intéressé ;
- *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande* [GC], 2017 (§§ 139-199), s'agissant d'une décision de justice interdisant la publication à grande échelle de données fiscales à caractère personnel ;

- *Bédat c. Suisse* [GC], 2016 (§§ 44-82), relativement à la condamnation d'un journaliste pour la publication d'informations couvertes par le secret de l'instruction ;
- *Mediengruppe Österreich GmbH c. Autriche*, 2022 (§§ 44-73), qui concernait l'interdiction qui avait été faite par les juridictions internes à un quotidien de publier la photographie, accompagnée de la légende « néonazi condamné », d'un individu qui était indirectement lié à la campagne d'un candidat à l'élection présidentielle, la publication en cause étant parue plus de vingt ans après la condamnation de l'intéressé ;
- *Gafiuc c. Roumanie*, 2020 (§§ 85-90), concernant le retrait d'une accréditation accordée à un journaliste pour faire des recherches dans les archives de la Sécurité à la suite de la divulgation, dans plusieurs articles qu'il avait publiés, de données personnelles sous une forme brute de différents sportifs connus, sans en apprécier la pertinence au regard du but déclaré de sa recherche, qui était le sport pendant l'ère communiste ;
- *Giesbert et autres c. France*, 2017 (§§ 77-103), s'agissant de la condamnation d'un journal pour avoir publié des actes d'une procédure pénale avant leur lecture en audience publique ;
- *Verlagsgruppe Droemer Knaur GmbH & Co. KG c. Allemagne*, 2017 (§§ 36-62), concernant l'octroi de dommages-intérêts pour le manquement d'une maison d'édition de procéder à des recherches minutieuses et avoir gravement porté atteinte aux droits de la personnalité;
- *Kurier Zeitungsverlag und Druckerei GmbH c. Autriche*, 2012 (§§ 47-56), concernant l'obligation d'indemniser une enfant victime de sévices sexuels dont l'identité avait été révélée dans un article de presse. Compte tenu de leur vulnérabilité, les victimes d'infraction doivent bénéficier d'une protection particulière de leur identité ;
- *MGN Limited c. Royaume-Uni*, 2011 (§ 152), où la Cour a jugé convaincant entre autres le fait que la révélation dans la presse de certaines données sur la thérapie suivie par une célébrité pour toxicomanie était préjudiciable et risquait fort de nuire à sa guérison ;
- *Éditions Plon c. France*, 2004 (§§ 22-57), quant à l'interruption provisoire de la diffusion d'un livre contenant des données couvertes par le secret médical au sujet d'un chef d'État décédé.
- *Mitov et autres c. Bulgarie* (déc.), 2023 (§§ 30-41), concernant les règles d'anonymisation édictées par le président de la Cour administrative suprême et la législation portant création d'une règle imposant la publication différée de certaines décisions rendues dans des affaires pénales, à la suite de quoi les requérants, journalistes d'investigation, n'avaient pas pu consulter librement sur Internet l'ensemble des éléments scannés du dossier qui se trouvaient dans la base de données de la juridiction concernée.
- *Ramadan c. France* (déc.), 2024 (§§ 28-46), où le requérant, qui était accusé d'agressions sexuelles pour lesquelles il était visé par une procédure pénale qui était pendante, avait diffusé dans un ouvrage ainsi que dans deux autres médias des informations concernant l'identité de la victime alléguée, sans avoir recueilli son accord, alors que l'identité de l'intéressée avait déjà été divulguée par des tiers dans un média.

350. Au sujet de la diffusion d'images personnelles dans la presse écrite ou à travers les moyens d'information audio-visuels, ou de l'injonction de ne pas diffuser de telles données personnelles, la Cour est parvenue à un constat de violation de l'article 10 dans plusieurs affaires parmi lesquelles : *Pinto Coelho c. Portugal (n° 2)*, 2016 (§§ 31-56), sur la condamnation d'une journaliste pour avoir diffusé l'enregistrement d'une audience sans autorisation ; *Haldimann et autres c. Suisse*, 2015 (§§ 63-68), sur la condamnation de quatre journalistes pour avoir enregistré et diffusé, dans un but d'intérêt public, un entretien avec un courtier en assurances réalisé par caméra cachée ; *Krone Verlag GmbH & Co. KG c. Autriche*, 2002, (§§ 21-39), au sujet d'une injonction de ne pas publier la photographie d'un certain homme politique; *News Verlags GmbH & Co.KG c. Autriche*, 2000

(§§ 37-60), sur l'interdiction faite à un journal de publier la photographie d'un suspect dans le cadre d'une procédure pénale dirigée contre ce dernier.

351. La diffusion de telles images ou l'injonction de ne pas les diffuser n'ont en revanche pas emporté un constat de violation de l'article 10 dans les affaires : *Société de Conception de Presse et d'Édition c. France*, 2016 (§§ 32-54), s'agissant d'une injonction judiciaire d'occulter, dans un magazine en vente, la photographie d'une personne séquestrée et torturée ; *Axel Springer SE et RTL Television GmbH c. Allemagne*, 2017 (§§ 43-59), s'agissant de la décision d'interdire la publication d'images qui auraient permis de reconnaître une personne jugée pour meurtre ; *Egeland et Hanseid c. Norvège*, 2009 (§§ 56-65), concernant la condamnation de rédacteurs-en-chef de journaux pour avoir publié des photographies d'une personne sur le point d'être conduite en prison pour purger une longue peine qu'elle venait de se voir infliger. Voir aussi les paragraphes 17 et 65 ci-avant concernant l'affaire *Vučina c. Croatie* (déc.) 2019. Dans l'affaire *Standard Verlagsgesellschaft mbH c. Autriche (n° 3)*, des décisions de justice injustifiées ayant ordonné à un media de divulguer les données relatives aux auteurs de commentaires injurieux mis en ligne sur son portail d'actualités dans le cadre d'un débat politique ont emporté un constat de violation de l'article 10 de la Convention.

352. Dans l'affaire *Alpha Doryforiki Tileorasi Anonymi Etairia c. Grèce*, 2018 (§§ 59-69, 77-78), la diffusion à des fins journalistiques de plusieurs vidéos issues d'une surveillance secrète avec une caméra cachée d'une personnalité publique a entraîné un constat de violation et un autre de non-violation de l'article 10 selon que l'enregistrement avait été effectué dans un espace public ou dans un espace privé.

353. S'agissant d'une diffusion sur Internet, par des particuliers, d'images d'autres individus captées en secret, sans le consentement du sujet des données, dans l'affaire *Khadija Ismayilova c. Azerbaïdjan*, 2019 (§§ 158-166), la Cour a condamné l'État défendeur pour ses défaillances de protéger la requérante, journaliste de profession, qui avait été filmée par des personnes inconnues à travers des caméras cachées installées dans son appartement. La divulgation injustifiée, de la part des autorités, dans un communiqué de presse qui prétendait fournir un rapport d'avancement sur une enquête pénale, des données personnelles comme le nom de l'intéressée et l'adresse de ses proches et de ses collègues de travail n'a fait qu'aggraver la situation, en contradiction avec l'esprit d'un environnement protecteur à l'égard du journalisme (*ibidem*, § 165).

354. Dans une affaire qui mettait en cause la protection de la liberté d'expression d'un lanceur d'alerte et la divulgation des données confidentielles touchant à la sureté de l'État, la Cour a conclu à la violation de l'article 10 au sujet de la condamnation pénale du requérant pour avoir rendu publiques des irrégularités dans la collecte des données à caractère personnel par le service de renseignements qu'il avait constatée dans le cadre de ses attributions professionnelles (*Bucur et Toma c. Romanie*, 2013, §§ 95-120). Dans une autre affaire concernant un lanceur d'alerte, le médecin-chef adjoint d'un hôpital public avait été licencié après avoir signalé qu'il soupçonnait son supérieur hiérarchique de pratiquer l'euthanasie – soupçon qui s'était révélé infondé. La Cour a conclu à la non-violation de l'article 10, car les soupçons du requérant reposaient sur des informations disponibles dans les dossiers médicaux électroniques, or le requérant savait que ces dossiers ne renfermaient pas toutes les informations relatives à la santé des patients, contrairement aux dossiers papier. Ainsi, même s'il avait agi de bonne foi, il n'avait pas dûment vérifié l'exactitude et la fiabilité des informations qu'il divulguait (*Gawlik c. Liechtenstein*, 2021, §§ 74-78).

355. La question de la protection des données personnelles des journalistes ou des données en possession des journalistes pouvant entraîner la découverte de l'identité de leurs sources a été examinée par la Cour dans plusieurs affaires, parmi lesquelles :

- *Sedletska c. Ukraine*, 2021 (§§ 59-60 et 64-73), où les autorités d'enquête avaient obtenu du juge l'autorisation de recueillir les données de communications d'une journaliste – dates, heures et bornage de son téléphone mobile près de certaines rues et certains

emplacements sur une période de seize mois – auprès de son opérateur de téléphonie mobile, et où la Cour a conclu à la violation de l'article 10 au motif que la mesure litigieuse n'était pas justifiée par un « impératif prépondérant d'intérêt public » et ne présentait pas de garanties procédurales suffisantes ;

- *Jecker c. Suisse*, 2020 (§§ 37-43), où une injonction faite à une journaliste de divulguer l'identité d'une source afin d'aider les autorités pénales à identifier un vendeur de stupéfiants a été jugée par la Cour contraire à l'article 10, en l'absence d'une pesée *in concreto* des différents intérêts en jeu ;
- *Telegraaf Media Nederland Landelijke Media B.V. et autres c. Pays-Bas*, 2012 (§ 102), où la mise sous surveillance de journalistes autorisée sans contrôle préalable d'un organe indépendant et l'ordre de communiquer des documents pouvant entraîner l'identification de leurs sources a emporté une violation des articles 8 et 10 combinés. Un contrôle postérieur n'aurait pas suffi, car, une fois anéantie, la confidentialité des sources journalistiques ne peut être rétablie (*ibidem*, §§ 100-101) ;
- *Financial Times Ltd et autres c. Royaume-Uni*, 2009 (§ 63), où la Cour a précisé que la conduite de la source ne peut jamais être décisive pour déterminer l'opportunité de prendre une injonction de divulgation et ne doit représenter qu'un facteur, certes important, à prendre en compte dans l'exercice requis de mise en balance ;
- *Weber et Saravia c. Allemagne* (déc.), 2006 (§§ 143-153), où la Cour a déclaré manifestement mal fondé un grief tiré de l'atteinte à la liberté d'expression résultant des dispositions d'une loi autorisant la surveillance à but stratégique des télécommunications, et empêchant les journalistes de garantir que les informations qu'ils recevaient dans le cadre de leurs activités demeuraient confidentielles ;
- *Ernst et autres c. Belgique*, 2003 (§§ 94-105), où des perquisitions et les saisies massives dans les locaux professionnels des requérants, journalistes, visant à identifier leurs sources ont constitué une violation de l'article 10. (Voir aussi les affaires *Roemen et Schmit c. Luxembourg*, 2003, §§ 47-60, au sujet des perquisitions chez un journaliste visant à identifier ses sources ; *Tillack c. Belgique*, 2007, §§ 56-68, concernant les perquisitions et saisies au domicile et au bureau d'un journaliste soupçonné de corruption d'un fonctionnaire européen pour obtenir des informations confidentielles relatives aux enquêtes en cours au sein des institutions européennes, afin d'identifier l'auteur de ces divulgations ; *Sanoma Uitgevers B.V. c. Pays-Bas* [GC], 2010, §§ 64-100, ayant traité de la saisie par la police de pièces qui auraient pu permettre l'identification de sources journalistiques ; *Nagla c. Lettonie*, 2013, §§ 78-102, relativement aux recherches urgentes au domicile d'une journaliste impliquant la saisie d'appareils de stockage de données contenant ses sources d'informations ; *Sérvulo & Associados - Sociedade de Advogados, RL, et autres c. Portugal*, 2015, §§ 101-120, au sujet de la saisie de grande ampleur de documents informatiques et messages électroniques d'un cabinet d'avocats ; et *Görmüş et autres c. Turquie*, 2016, §§ 32-77, concernant la protection des sources journalistiques qui étaient des fonctionnaires ayant constaté et signalé des comportements ou des pratiques qu'ils estimaient contestables sur leur lieu de travail dans le contexte de la confidentialité des affaires militaires), et
- *Big Brother Watch et autres c. Royaume-Uni* [GC], 2021, §§ 442-458, s'agissant d'un régime d'interception en masse des communications permettant aux services de renseignement d'accéder à des éléments journalistiques confidentiels de manière fortuite, en prenant accidentellement de tels éléments dans les « filets » d'une interception en masse, pouvant ainsi aboutir à la collecte de très nombreux éléments journalistiques confidentiels. La Cour a abouti à un constat de violation de l'article 10 de la Convention.

3. Protection des données et interdiction de la discrimination (article 14 de la Convention)

356. Dans l'affaire *Sheffield et Horsham c. Royaume-Uni* [GC], 1998 (§§ 51-61, 76-77), qui portait sur la question de savoir s'il pesait sur l'État défendeur une obligation de reconnaître sur le plan juridique la nouvelle identité sexuelle des requérantes, deux transsexuelles opérées du sexe masculin au sexe féminin, la Cour a conclu à la non-violation de l'article 8, seul ou combiné avec l'article 14. Aux yeux de la Cour, les situations dans lesquelles les requérantes pouvaient avoir à divulguer leurs données personnelles ne se produisaient pas avec une fréquence telle que l'on pouvait estimer qu'elles portaient une atteinte disproportionnée aux droits au respect de leur vie privée. La Cour a également observé que l'État défendeur s'était efforcé, dans une certaine mesure, de minimiser les risques pour les transsexuels de se voir poser des questions embarrassantes concernant leur sexe en leur permettant d'obtenir des permis de conduire, des passeports et d'autres types de documents officiels établis sous leurs nouveaux prénoms et sexe, et que l'utilisation des certificats de naissance comme moyen d'identification était officiellement découragée (*ibidem*, § 59 ; *Cossey c. Royaume-Uni*, 1990, §§ 36-42).

357. Dans quelques affaires où la Cour a examiné des questions étroitement liées à la protection des données personnelles sous l'angle des articles 8 ou 9, la Cour a estimé qu'aucune question distincte ne se posait au regard de l'article 14 (*Sinan Işık c. Turquie,* 2010, § 57, sur la question de la mention, obligatoire ou facultative, de la confession du requérant sur sa carte d'identité ; *Avilkina et autres c. Russie,* 2013, § 61, sur la divulgation de dossiers médicaux relatifs à plusieurs témoins de Jéhovah qui ont refusé de subir des transfusions sanguines ; *Christine Goodwin c. Royaume-Uni* [GC], 2002, §§ 92-93, 108 et *I. c. Royaume-Uni* [GC], 2006, §§ 72-73, 88, sur la question de la reconnaissance juridique de la conversion sexuelle d'un individu).

4. Protection des données et droit au respect des biens (article 1 du Protocole n° 1)

358. La Cour a traité de la protection des données à caractère personnel et du droit au respect des biens lors de perquisitions et saisies.

359. Dans l'affaire *Smirnov c. Russie*, 2007 (§§ 53-59), la Cour a jugé que les autorités nationales n'avaient pas ménagé un « juste équilibre » entre les impératifs de l'intérêt général et les exigences de la protection du droit du requérant au respect de ses biens et qu'il y avait donc eu violation de l'article 1 du Protocole n° 1 en raison de la perquisition du domicile du requérant, avocat de profession, suivie de la saisie entre autres de l'unité centrale de son ordinateur contenant les disques durs avec ses données personnelles. Si la rétention de preuves matérielles pouvait être nécessaire dans l'intérêt d'une bonne administration de la justice, l'ordinateur en lui-même n'était ni l'objet, ni l'instrument, ni le produit d'une infraction pénale. Puisque les informations qui se trouvaient enregistrées sur le disque dur, pouvant être utiles et déterminantes pour l'enquête avaient été examinées par l'enquêteur, imprimées et versées au dossier, il n'y avait aucune raison justifiant la poursuite de la rétention de l'unité centrale qui, de surcroît, était l'instrument de travail du requérant, utilisé par ailleurs pour conserver les données de ses clients.

360. Dans l'affaire *Kruglov et autres c. Russie*, 2020 (§§ 145-146), la perquisition et la saisie par la police aux domiciles et bureaux des requérants, avocats de profession, ou de leurs clients, des ordinateurs et des disques durs renfermant des informations personnelles et des documents couverts par le secret professionnel, et n'étant pas en eux-mêmes un objet, un instrument ou un produit d'une infraction criminelle, ont emporté la violation de l'article 1 du Protocole n° 1.

361. Dans l'affaire *Pendov c. Bulgarie*, 2020 (§§ 43-51), la Cour a jugé que la rétention inutilement prolongée du serveur informatique du requérant dans le cadre d'une procédure pénale contre des tiers a emporté une violation de l'article 1 du Protocole n° 1. Le fait que le serveur informatique du

requérant n'ait jamais été examiné aux fins de l'enquête pénale, visant uniquement des tiers, la possibilité pour les autorités de copier les informations nécessaires, l'importance du serveur pour l'activité professionnelle du requérant et que le parquet soit en partie resté inactif ont fait de la rétention du serveur du requérant pendant sept mois et demi une mesure disproportionnée (*ibidem*, § 51).

5. Protection des données et liberté de circulation (article 2 du Protocole n° 4)

362. La Cour a eu à connaître quelques affaires où la liberté de circulation d'un individu s'est trouvée limitée en raison de ses données personnelles mémorisées par les autorités. Elle les a généralement traitées sous l'angle de l'article 8.

363. Ainsi, dans l'affaire *Dalea c. France* (déc.), 2010, la mémorisation par la police, dans le fichier du système d'information Schengen, de données dont l'exactitude était contestée par l'intéressé, empêchait le requérant de voyager librement dans l'espace Schengen. Le requérant se trouvait dans l'impossibilité d'accéder et de faire rectifier les données personnelles figurant dans ce fichier. La Cour a réitéré que l'article 8 ne garantissait pas, comme tel, un droit d'entrer ou de résider dans un État dont on n'était pas ressortissant. En l'occurrence, l'atteinte portée à la vie privée du requérant en raison de son inscription par les autorités françaises dans le fichier Schengen était prévue par la loi, poursuivait le but légitime de protection de la sécurité nationale, était proportionnée au but poursuivi et nécessaire dans une société démocratique. Le requérant n'avait pas invoqué l'article 2 du Protocole n° 4.

364. Dans l'affaire *Shimovolos c. Russie*, 2011 (§§ 64-71), des informations sur les déplacements du requérant en train et avion avaient été enregistrées dans la « base de données des surveillances » en raison de son appartenance à une organisation de défense des droits de l'homme. À chaque fois qu'une personne dont le nom figurait sur cette liste achetait un billet de train ou d'avion, le Département intérieur des transports en était automatiquement informé. C'est ainsi que, lorsque le requérant prit le train pour se rendre à Samara à l'occasion d'un sommet Union européenne-Russie et d'un défilé de protestation organisé dans cette ville, trois policiers contrôlèrent ses papiers d'identité et lui demandèrent le motif de son déplacement. La Cour a estimé qu'en recueillant et en conservant des données sur les déplacements du requérant en vertu d'un arrêté ministériel qui n'avait été ni publié ni rendu accessible au public d'une quelconque manière, les autorités avaient porté atteinte à sa vie privée de façon incompatible avec le droit garanti par l'article 8. Elle a en outre estimé qu'aucune question distincte ne se posait sous l'angle de l'article 2 du Protocole n° 4 (*ibidem*, § 73).

365. Dans l'affaire *Beghal c. Royaume-Uni*, 2019 (§§ 89-109), qui soulevait la question de l'importance de surveiller les déplacements de terroristes au niveau international, la Cour a estimé, avant de conclure à la violation de l'article 8, que le pouvoir conféré en vertu de la législation anti-terrorisme aux agents des services de police et d'immigration ainsi qu'aux agents des douanes désignés à cet effet d'interpeller, d'interroger et de fouiller les passagers dans les ports, les aéroports et les terminaux ferroviaires internationaux n'était ni suffisamment délimité ni entouré de garanties juridiques adéquates contre les abus. En particulier, aucune autorisation préalable n'était nécessaire et le pouvoir d'interpeller et d'interroger pouvait être exercé même en l'absence de soupçon de participation à des activités terroristes.

366. Dans l'affaire *Willems c. Pays-Bas* (déc.), 2021, s'agissant de l'obligation, en vertu de la loi sur les passeports, de faire relever les empreintes digitales lors de la demande de passeport ainsi que de la conservation de ces empreintes sur une puce électronique suite à l'incorporation dans le droit national (sans aucune marge de manœuvre pour les autorités nationales) du règlement de l'UE sur les éléments de sécurité et la biométrie dans les documents de voyage, la Cour a rejeté comme

manifestement mal fondés les griefs du requérant tirés de l'article 8 et 2 du Protocole n° 4, eu égard à la « présomption de protection équivalente » en vertu du droit de l'UE, (*ibidem*, §§ 26-36).

B. Protection des données et droits procéduraux

Article 6 de la Convention

> « 1. Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable, par un tribunal indépendant et impartial, établi par la loi, qui décidera, soit des contestations sur ses droits et obligations de caractère civil, soit du bien-fondé de toute accusation en matière pénale dirigée contre elle. Le jugement doit être rendu publiquement, mais l'accès de la salle d'audience peut être interdit à la presse et au public pendant la totalité ou une partie du procès dans l'intérêt de la moralité, de l'ordre public ou de la sécurité nationale dans une société démocratique, lorsque les intérêts des mineurs ou la protection de la vie privée des parties au procès l'exigent, ou dans la mesure jugée strictement nécessaire par le tribunal, lorsque dans des circonstances spéciales la publicité serait de nature à porter atteinte aux intérêts de la justice.10 11
>
> 2. Toute personne accusée d'une infraction est présumée innocente jusqu'à ce que sa culpabilité ait été légalement établie.
>
> 3. Tout accusé a droit notamment à :
>
> a) être informé, dans le plus court délai, dans une langue qu'il comprend et d'une manière détaillée, de la nature et de la cause de l'accusation portée contre lui ;
>
> b) disposer du temps et des facilités nécessaires à la préparation de sa défense ;
>
> c) se défendre lui-même ou avoir l'assistance d'un défenseur de son choix et, s'il n'a pas les moyens de rémunérer un défenseur, pouvoir être assisté gratuitement par un avocat d'office, lorsque les intérêts de la justice l'exigent ;
>
> d) interroger ou faire interroger les témoins à charge et obtenir la convocation et l'interrogation des témoins à décharge dans les mêmes conditions que les témoins à charge ;
>
> e) se faire assister gratuitement d'un interprète, s'il ne comprend pas ou ne parle pas la langue employée à l'audience.

Article 13 de la Convention

> « Toute personne dont les droits et libertés reconnus dans la présente Convention ont été violés, a droit à l'octroi d'un recours effectif devant une instance nationale, alors même que la violation aurait été commise par des personnes agissant dans l'exercice de leurs fonctions officielles. »

1. Droit à un procès équitable (article 6 de la Convention)[12]

367. Tout individu dont les données à caractère personnel font l'objet d'un traitement automatisé dans le cadre d'une procédure judiciaire doit bénéficier des garanties prévues par l'article 6, quelle que soit sa position dans la procédure, demandeur, défendeur, témoin, accusé ou simple tiers.

[12] Ce chapitre doit être lu à la lumière et combiné avec les Guides sur l'article 6 en matière *civile* (pp 60-91) et *pénale* (pp 32-100)

a. Garanties générales (article 6 § 1 de la Convention)

368. Dans plusieurs affaires, la Cour a examiné, sur le terrain de l'article 6 § 1, la nécessité de protéger des données à caractère personnel des parties ou des tierces parties lors de l'examen des différentes garanties générales pour assurer l'équité de procédures judiciaires, à savoir, notamment, l'égalité des armes et le respect du contradictoire, la publicité des débats et du prononcé, l'administration d'éléments de preuve, le caractère raisonnable de la durée de la procédure et l'exigence de motivation des décisions de justice.

i. Égalité des armes et respect du contradictoire lors d'une procédure impliquant des données sensibles ou confidentielles

369. Dans l'affaire *Eternit c. France* (déc.), 2012 (§§ 35-42), une procédure entamée par l'employeur contestant la décision d'une caisse d'assurance maladie de reconnaître le caractère professionnel de la maladie de l'un de ses employés, procédure lors de laquelle l'employeur ne s'était pas vu communiquer les observations médicales du médecin conseil de la caisse n'a pas été jugée contraire à l'article 6 § 1. La non-communication à l'employeur des données médicales de son salarié pouvait s'expliquer par l'exigence de protéger la confidentialité de ses données médicales, dont les tribunaux devaient tenir compte au même titre que du droit de la société requérante à une procédure contradictoire, de manière à ce qu'aucun de ces droits ne soit atteint dans sa substance même. Cet équilibre était réalisé dès lors que l'employeur pouvait solliciter du juge la désignation d'un médecin expert indépendant, à qui seraient remises les pièces composant le dossier médical du salarié et dont le rapport, établi dans le respect du secret médical, aurait pour objet d'éclairer la juridiction et les parties (*ibidem*, § 37). Le fait qu'une expertise n'ait pas été ordonnée dans tous les cas où un employeur la demandait, mais seulement dans le cas où la juridiction s'estimait insuffisamment informée, n'était pas contraire à l'article 6 § 1 en matière de procès équitable (*ibidem*, §§ 35-39).

370. Dans l'affaire *Kennedy c. Royaume-Uni*, 2010 (§§ 184-191), des restrictions au principe de l'égalité des armes et du contradictoire devant la Commission des pouvoirs d'enquête, un organe indépendant chargé d'examiner toute plainte formulée par les individus qui estimaient avoir fait l'objet d'une interception illégale de leurs communications par les autorités, n'ont pas été jugées incompatibles avec l'article 6 § 1. Les intérêts de la sécurité nationale ou la nécessité de garder secrètes certaines méthodes d'enquête en matière pénale devaient être mis en balance avec le droit à une procédure contradictoire. Aux yeux de la Cour, il était nécessaire de dissimuler des informations sensibles et confidentielles, dont la divulgation aurait empêché la réalisation de l'objectif poursuivi (*ibidem*, §§ 186-187).

371. De façon plus générale, la Cour a souligné que le droit à un procès pénal contradictoire impliquait, pour l'accusation comme pour la défense, la faculté de prendre connaissance des observations ou éléments de preuve produits par l'autre partie, ainsi que de les commenter, par exemple un enregistrement vidéo d'un accusé retenu comme élément de preuve à charge (*Murtazaliyeva c. Russie*, [GC], 2018, §§ 90-95).

ii. Motivation des décisions de justice et protection des données

372. Dans l'affaire *Surikov c. Ukraine*, 2017 (§§ 102-103), la Cour a conclu à la violation de l'article 6 § 1 au motif que les juridictions nationales ne s'étaient pas penchées sur certains points pertinents et importants soulevés. L'intéressait alléguait que son employeur avait de façon arbitraire recueilli et conservé des données sensibles et obsolètes concernant sa santé mentale, puis utilisé celles-ci lors de l'examen de sa demande de promotion, et les avait illégalement divulgués à ses collègues et devant le tribunal. La Cour a réaffirmé que l'article 6 obligeait les tribunaux à indiquer les motifs de leurs jugements. Bien que cette obligation ne puisse être comprise comme exigeant une réponse détaillée à tous les arguments, si les tribunaux nationaux ignoraient un point spécifique, pertinent et

important formulé par un requérant cela serait contraire au principe d'équité (*ibidem*, § 101 et les exemples de jurisprudence qui y sont cités).

373. Dans l'affaire *Samoylova c. Russie*, 2021 (§§ 50-52), qui portait sur la diffusion dans un reportage télévisé de l'adresse de résidence exacte de la requérante, de son numéro d'identification de contribuable et des images de l'intérieur de sa maison de campagne, la Cour a jugé que les juridictions internes avaient omis de fournir une réponse spécifique et explicite aux arguments qui auraient été décisifs pour l'issue de la procédure entamée par l'intéressée, en méconnaissance du droit à un procès équitable garanti par l'article 6 § 1 de la Convention.

374. Dans l'affaire *Kennedy c. Royaume-Uni*, 2010 (§§ 185-191), la politique des autorités consistant à « ne pas confirmer et ne pas démentir », qu'une opération d'interception de communications avait eu lieu n'a pas été jugée incompatible avec l'article 6 § 1. Ainsi la Commission des pouvoirs d'enquête, chargée d'examiner les plaintes des individus estimant avoir fait l'objet d'une interception illégale de leurs communications, pouvait se borner à informer les requérants qu'aucune décision n'a été rendue en leur faveur, car, si un recours devant cette commission pouvait conduire à dévoiler aux plaignants la mise en œuvre d'une opération d'interception, la politique gouvernementale de « non-confirmation et de non-dénégation » serait remise en cause (*ibidem*, § 189).

iii. Administration comme éléments de preuve des données à caractère personnel recueillies illégalement ou contrairement à l'article 8

375. La question de l'utilisation à titre d'éléments de preuve matériels, dans le cadre d'une procédure judiciaire, des données à caractère personnel recueillies de façon contraire aux exigences du droit interne ou à celles de l'article 8 a été à ce jour abordée par la Cour dans plusieurs affaires, dans le cadre de procédures administratives (*Vukota-Bojic c. Suisse*, 2016, § 77, sur l'utilisation dans un litige avec un assuré des informations secrètement collectées par une compagnie d'assurance dans le cadre des pouvoirs que lui conférait le régime d'assurance public), civiles (*Bărbulescu c. Roumanie* [GC], 2017, §§ 140-141, sur l'utilisation des données collectées par un employeur quant à l'usage de l'Internet par un employé sur son lieu de travail pour justifier son renvoi ; *Florindo de Almeida Vasconcelos Gramaxo c. Portugal*, 2022, §§ 130-140, sur l'utilisation de données kilométriques enregistrées par le système GPS du véhicule de fonction d'un délégué médical pour motiver le licenciement de l'intéressé), ou pénales (*Bykov c. Russie* [GC], 2009, §§ 80-83, relative à l'interception d'une conversation dans le cadre d'une opération secrète de police et à l'utilisation des éléments ainsi recueillis pour fonder une condamnation).

376. La Cour a considéré que l'admission et l'utilisation, dans une procédure judiciaire, des preuves de cette nature ne conduisent pas automatiquement à un constat d'iniquité de la procédure si, dans son ensemble, celle-ci a été conduite de manière équitable (*Bykov c. Russie* [GC], 2009, §§ 89-91 ; *Vukota-Bojic c. Suisse*, 2016, §§ 91-100).

377. La Cour a conclu à la violation de l'article 6 § 1 au sujet des informations recueillies grâce à l'intervention d'un informateur de la police, par un dispositif d'enregistrement secret des conversations dans la cellule du requérant qui n'était pas « prévu par la loi » (*Allan c. Royaume-Uni*, 2002, §§ 45-53). Les aveux faits par le requérant n'étaient pas spontanés mais avaient été provoqués par les questions continuelles de l'informateur, qui, à la demande de la police, avait orienté leurs conversations dans des conditions pouvant être considérées comme constituant l'équivalent d'un interrogatoire, mais sans les garanties devant l'accompagner. Bien qu'il n'existât aucune relation particulière entre le requérant et l'informateur et qu'il n'avait pas été noté de contrainte directe, le requérant a subi des pressions psychologiques portant atteinte au caractère volontaire de ses aveux. Dans ces conditions, les informations recueillies pouvaient passer pour avoir été obtenues contre la volonté du requérant, et leur utilisation au procès pour avoir porté atteinte à son droit de garder le silence et de ne pas s'accuser lui-même.

iv. Publicité des débats et du prononcé et confidentialité des données[13]

378. Dans l'affaire *P. et B. c. Royaume-Uni*, 2001 (§§ 38-41, 46-49), l'absence de publicité des débats et le prononcé, à huit clos, d'un jugement rendu dans une affaire concernant la garde d'enfants n'ont pas été jugés contraires à l'article 6 § 1. Aux yeux de la Cour, les procédures de garde d'enfants représentent des exemples types d'une situation dans laquelle il peut se justifier d'interdire l'accès de la salle d'audience à la presse et au public, en vue de protéger les données personnelles de l'enfant concerné et des parties et d'éviter de porter atteinte aux intérêts de la justice (*ibidem*, § 38). Le fait que toute personne pouvant justifier d'un intérêt était en droit de consulter ou d'obtenir une copie du texte intégral des ordonnances et jugements et que les décisions des tribunaux étaient automatiquement publiées sans les noms des intéressés permettait suffisamment de pallier l'absence d'un prononcé public (*ibidem*, § 47).

379. Dans l'affaire *Kennedy c. Royaume-Uni*, 2010 (§ 188), la Cour a rappelé qu'en vertu de l'article 6 § 1, la sécurité nationale pouvait justifier que le public soit écarté d'une procédure et a jugé que la nature des questions soulevées devant la Commission des pouvoirs d'enquête, qui portait sur l'illégalité de l'interception des communications, légitimait l'absence d'une audience publique.

380. La Cour est parvenue à un double constat de violation de l'article 6 dans l'affaire *Vasil Vasilev c. Bulgarie*, 2021, qui mettrait en cause absence totale de publicité (l'exclusion du public de toutes les audiences et l'absence de prononcé public du jugement) lors d'une procédure en dommages et intérêts intentée par le requérant suite à l'interception, l'enregistrement et la transcription d'une conversation téléphonique entre lui et l'un de ses clients surveillé secrètement dans le cadre d'une affaire pénale. L'exclusion du public de toutes les audiences et l'absence de prononcé public du jugement étaient fondée uniquement sur la présence au dossier d'informations classifiées (les éléments de preuve résultant de l'interception secrète de la conversation téléphonique du requérant). Pour la Cour, l'absence totale de publicité ne saurait être justifiée par la nécessité de protéger les informations classifiées sur lesquelles portait l'affaire. La nature des questions soulevées au cours de la procédure, qui concernait la responsabilité d'autorités étatiques pour une prétendue violation des droits garantis par l'article 8, n'avait pas un caractère hautement technique et le requérant n'a pas renoncé à son droit à une audience publique (*ibidem*, §§ 107-111). Lorsqu'une affaire concerne une violation alléguée d'un droit fondamental par les autorités de l'État, l'examen public de la procédure est essentiel pour maintenir la confiance dans l'État de droit. La présence d'informations classifiées dans le dossier de l'affaire ne saurait en elle-même constituer un motif pour refuser au public l'intégralité du jugement. Si une affaire implique des informations classifiées, des techniques existent pour permettre un certain degré d'accès public aux décisions qui y sont rendues tout en maintenant la confidentialité des informations sensibles (*ibidem*, §§ 116-118)

v. Durée des procédures judiciaires statuant sur la question de la protection des données

381. Dans l'affaire *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande* [GC], 2017 (§ 215), la Cour a jugé que la durée totale, six ans et six mois pour deux degrés de juridiction, d'une procédure qui portait sur la légalité, au regard de la législation interne et celle de l'Union européenne, de la publication à grande échelle des données à caractère personnel de nature fiscale par les sociétés requérantes ne répondait pas à l'exigence du délai raisonnable garanti par l'article 6 § 1. La procédure devant la Cour de Justice de l'Union européenne, saisie d'une question préjudicielle, ne saurait être prise en considération dans l'appréciation de la durée imputable aux autorités internes (*ibidem*, § 208).

[13] Voir aussi la partie ci-dessus du présent guide sur la « Divulgation des données dans le contexte des procédures judiciaires » sous l'angle de l'article 8 de la Convention.

382. En revanche, dans l'affaire *Surikov c. Ukraine*, 2017 (§§ 104-106), la Cour a déclaré manifestement mal fondé un grief tiré de la durée d'une procédure visant la conservation, par un employeur, des données sensibles et obsolètes concernant la santé mentale d'un employé et leur utilisation lors de l'examen de sa demande de promotion. La Cour a estimé qu'une durée inférieure à six ans pour trois degrés de juridiction ne saurait poser un problème au regard de l'exigence d'une durée raisonnable prévue par l'article 6 § 1 (*ibidem*, § 101).

b. Garanties spéciales (article 6 §§ 2 et 3 de la Convention)

383. En matière pénale, tout individu dont les données à caractère personnel ont fondé une accusation à son encontre doit bénéficier de certaines garanties spéciales.

i. Protection des données et respect de la présomption d'innocence (article 6 § 2 de la Convention)

384. Dans l'affaire *Batiashvili c. Géorgie*, 2019 (§§ 87-97), la Cour a reconnu l'article 6 § 2 applicable dans une situation où les autorités avaient manipulé avant l'arrestation d'un individu, puis diffusé à une chaîne de télévision, un enregistrement audio de ses conversations téléphoniques. Selon la Cour, l'implication des autorités a contribué à faire passer pour coupable un individu alors que sa culpabilité n'avait pas été établie par un tribunal, emportant une violation de cette disposition. À ses yeux, l'enchaînement de faits, considéré dans son ensemble, indiquait que les autorités d'enquête s'étaient conduites d'une manière qui avait eu une incidence substantielle sur la situation du requérant (*ibidem*, § 94). Même si l'accusation de non-dénonciation d'une infraction a été abandonnée au cours de la procédure de première instance, l'acte d'inculpation transmis au tribunal près de quatre mois après que l'enregistrement eut été rendu public la mentionnait encore, alors que les autorités de poursuite devaient avoir parfaitement connaissance de la fausseté des preuves sur laquelle elle reposait (*ibidem*, § 95).

385. Dans l'affaire *Y.B. et autres c. Turquie*, 2004 (§§ 43-51), les déclarations à la presse par la police au sujet de suspects, photographiés par les journalistes lors d'une conférence de presse organisée dans ses locaux, ont emporté une violation de l'article 6 § 2. La publication, lors d'une procédure pénale, de photographies représentant des suspects ne saurait par elle-même constituer une méconnaissance de leur droit à la présomption d'innocence. Les autorités nationales peuvent renseigner le public sur des enquêtes pénales en cours sous réserve de le faire avec toute la discrétion et toute la réserve requises. Lorsqu'elles rendent publics des éléments objectifs tirés d'une procédure pénale, ces éléments doivent néanmoins être exempts de toute appréciation ou préjugé de culpabilité (*ibidem*, §§ 47-48). En l'occurrence, l'attitude des autorités policières, dans la mesure où elle reflétait une appréciation préalable des charges pouvant être retenues contre les requérants et fournissait à la presse des moyens matériels permettant facilement de les identifier, ne se conciliait pas avec le respect de leur droit à la présomption d'innocence (*ibidem*, § 50).

386. Dans l'affaire *Panteleyenko c. Ukraine,* 2006 (§ 68-71), le libellé des décisions judiciaires ayant mis fin aux poursuites pénales contre le requérant, qui, pour la Cour, ne laissait aucun doute sur le fait que les juges étaient d'avis qu'il avait commis l'infraction dont il était accusé, a emporté un constat de violation de l'article 6 § 2. La décision de non-lieu pour des « motifs exonératoire » a été prise sur la base d'éléments contenant des données personnelles du requérant, notaire de profession, recueillis à la suite d'une perquisition à son bureau menée sans le respect de l'obligation prévue par la loi de notification préalable du mandat de perquisition à l'occupant des lieux et

contrairement à l'interdiction, en droit interne, de saisir des documents et des objets sans rapport direct avec l'enquête (*ibidem*, § 70)[14].

ii. Protection des données et droits de la défense (article 6 § 3 b) de la Convention)

387. Dans l'affaire *Rook c. Allemagne*, 2019 (§ 69), un délai de trois mois et demi pour analyser une masse volumineuse de données et de fichiers électroniques du requérant issus de la surveillance de ses télécommunications, représentait, aux yeux de la Cour, un délai suffisant, au regard de l'article 6 § 3 b), pour permettre à son avocat de préparer sa défense. Compte tenu de la complexité de la procédure pénale en cause, il n'était pas nécessaire de donner à l'avocat du requérant la possibilité de lire et d'écouter chaque élément des données issues de la surveillance, qui avait permis de recueillir au cours de l'enquête 45 000 appels téléphoniques et 34 000 séries d'autres données générées à partir de télécommunications ainsi que 14 million de fichiers électroniques que la police avait confisqué dans l'appartement du requérant et dans d'autres locaux (*ibidem*, §§ 7-8, 67-71).

388. De façon plus générale, la Cour a souligné que les moyens d'investigation actuels pouvaient générer d'énormes quantités de données, dont l'intégration dans une procédure pénale ne devait pas causer de retards inutiles. Le droit du requérant à la communication de la masse brute des données ne doit pas être confondu avec le droit pour lui d'avoir accès à toutes les pièces déjà jugées pertinentes par les autorités, qui d'une manière générale, exige que l'intéressé puisse en comprendre toute la teneur (*ibidem*, § 67). Le simple fait que la procédure judiciaire avait déjà été entamée lorsque l'avocat se vit remettre une copie intégrale du dossier ne peut faire conclure qu'il n'a pas bénéficié d'un temps de préparation suffisant. L'article 6 § 3 b) n'exige pas que la préparation d'un procès d'une certaine durée puisse être terminée avant la tenue de la première audience (*ibidem*, § 72)[15].

389. Dans l'affaire *Sigurður Einarsson et autres c. Islande*, 2019 (§§ 88-93), la Cour a conclu à l'absence de violation de l'article 6 §§ 1 et 3 b) concernant la tenue à l'écart de la défense d'une masse de données collectées de façon non sélective par le parquet et non versées au dossier de l'enquête, et de son tri électronique par le parquet en vue de sélectionner les informations pertinentes pour l'enquête. Concernant la « compilation entière », le parquet ignorait quelle était la teneur de la masse des données et, à ce titre, n'avait bénéficié d'aucun avantage par rapport à la défense. Concernant les données qui avaient été « balisées », en principe, il eût été approprié de donner à la défense la possibilité de réaliser des recherches destinées à trouver des éléments potentiellement à décharge. Cependant, les requérants n'avaient jamais formellement sollicité de décision de justice dans ce sens et ils n'avaient fourni aucune précision sur le type d'éléments qu'ils recherchaient.

2. Droit à un recours effectif (article 13 de la Convention)[16]

390. En matière de divulgation de données médicales, dans l'affaire *Anne-Marie Anderson c. Suède*, 1997 (§§ 41-42), la Cour a conclu à la non-violation de l'article 13 combiné avec l'article 8 relativement à l'absence de recours avant la communication de données médicales personnelles et confidentielles par l'autorité médicale à un service social. Entre autres, la mesure avait été notifiée à l'intéressée et était de portée limitée, les informations dont il s'agissait n'ayant pas été rendues publiques mais bénéficiant du même degré de confidentialité que les dossiers psychiatriques.

---

[14] Voir aussi le *Guide sur l'article 6 de la Convention* (Droit à un procès équitable (volet pénal) sur la motivation des décisions de justice (paragraphes 168-176).

[15] Voir aussi le *Guide sur l'article 6 de la Convention* (Droit à un procès équitable (volet pénal) sur les facilités nécessaires à l'accusé dans la préparation de sa défense.

[16] Ce chapitre doit être lu à la lumière et combiné avec le *Guide sur l'article 13 de la Convention* (Voir notamment les pages 49-51).

391. Dans l'affaire *Mik et Jovanović c. Serbie* (déc.), les requérants se plaignaient, sur le terrain de l'article 8 pris seul et combiné avec l'article 13, du manquement continu de l'État à leur fournir des informations crédibles sur le sort de leurs fils, dont on leur disait qu'ils étaient morts peu après la naissance et dont on ne leur avait jamais montré les corps. La Cour a constaté qu'une loi récemment adoptée avait établi un mécanisme (y compris une base de données ADN) permettant de répondre à la situation à laquelle les requérants et d'autres personnes étaient confrontés. Elle a observé en particulier que le nouveau cadre juridique prévoyait à la fois des procédures judiciaires et des procédures extrajudiciaires de recherche de la situation réelle des nouveau-nés supposément enlevés dans les maternités publiques, permettant aux parents concernés d'obtenir réparation. Elle a noté en outre que certaines mesures importantes avaient été prises pour mettre en œuvre ce nouveau cadre, dont une formation complète des juges et la nomination, pour la procédure extrajudiciaire, de membres (surtout des représentants d'associations de parents établies) d'une commission dotée de larges pouvoirs d'enquête, de recueil de données et d'établissement de rapports. Constatant que les requérants eux-mêmes avaient choisi d'avoir recours à ce nouveau mécanisme, elle a conclu qu'il ne se justifiait plus de poursuivre l'examen de la requête, au sens de l'article 37 § 1 c) de la Convention.

392. Dans l'affaire *Panteleyenko c. Ukraine*, 2006 (§§ 82-84), la Cour a conclu à la violation de l'article 13 combiné avec l'article 8 compte tenu de l'absence d'un recours effectif pour permettre au requérant d'alléguer la divulgation d'informations confidentielles sur sa santé mentale lors d'une audience publique. Pour la Cour, les voies de droit existantes se sont avérées inefficaces car elles n'avaient pas conduit à la cessation de la divulgation des données psychiatriques confidentielles figurant au dossier, ni n'avaient abouti à l'octroi à l'intéressé de dommages-intérêts pour le préjudice subi en raison de l'ingérence dans son droit à sa vie privée. La tenue d'une audience à huis clos aurait permis d'éviter la divulgation des informations litigieuses au public, mais n'aurait pas empêché que celles-ci soient portées à la connaissance des parties et versées au dossier de l'affaire.

393. Concernant la publication sur Internet d'une décision judiciaire divulguant les informations relatives à l'adoption des enfants des requérants, la Cour a conclu, dans l'affaire *X et autres c. Russie*, 2020 (§§ 73-79), à la violation de l'article 13 combiné avec l'article 8 en l'absence d'une voie de recours judiciaire propre à offrir un dédommagement pour le préjudice moral causé par le dysfonctionnement du service de la justice.

394. Dans une affaire relative à l'inscription d'un individu comme « délinquant » dans les registres de la police après avoir été interrogé au sujet d'un viol et le maintien de cette mention sans qu'aucun acte d'accusation n'ait été établi par la suite, la Cour est parvenue à un constat de violation de l'article 13 combiné avec l'article 8 après avoir constaté que l'intéressé n'avait disposé à l'époque des faits d'aucun recours pour s'en plaindre (*Dimitrov-Kazakov c. Bulgarie*, 2011, §§ 37-39).

395. L'absence de recours effectif pour demander la radiation du nom du requérant de la liste annexée à l'ordonnance sur les talibans a constitué une violation de l'article 13 combiné avec l'article 8 dans l'affaire *Nada c. Suisse* [GC], 2012 (§§ 209-214). Le requérant avait pu saisir les juridictions internes, mais elles n'avaient pas examiné ses griefs quant au fond.

396. Concernant l'utilisation de données personnelles dans le cadre professionnel, l'absence de recours effectif quant à la violation du droit au respect de la vie privée des requérants concernant des enquêtes indiscrètes sur la vie privée d'homosexuels ayant abouti à leur révocation de l'armée a constitué une violation de l'article 13 combiné avec l'article 8 dans l'affaire *Smith et Grady c. Royaume-Uni*, 1999 (§§ 136-139).

397. Dans l'affaire *Karabeyoğlu c. Turquie*, 2016 (§§ 128-132), l'indisponibilité d'une voie de recours interne pour faire examiner l'utilisation, dans le cadre d'une enquête disciplinaire, de données provenant d'écoutes téléphoniques issues d'une enquête pénale a conduit la Cour à conclure à la violation de l'article 13 au regard de l'article 8.

398. Dans l'affaire *Peck c. Royaume-Uni*, 2003 (§§ 101-114), la Cour a estimé que le requérant n'avait disposé d'aucun recours effectif pour alléguer la transmission aux médias d'une vidéo provenant d'une télévision en circuit fermé le filmant pendant qu'il essayait de se suicider dans un lieu public. En ce qui concerne la possibilité d'un contrôle juridictionnel, puisque la seule question portée devant les juridictions internes était celle de savoir si la politique suivie en matière d'images captées par des caméras dans les lieux publics pouvait passer pour « irrationnelle », tout examen de la question de savoir si l'atteinte portée aux droits du requérant répondait à un besoin social impérieux ou était proportionnée s'en trouvait de fait exclu (*ibidem*, §§ 106-107). Quant aux commissions compétentes dans le domaine des médias, elles n'offraient pas non plus un recours effectif puisqu'elles n'avaient pas le pouvoir d'allouer des dommages-intérêts (*ibidem*, §§ 108-109). Et au sujet de la possibilité d'introduire une action pour abus de confiance, il était peu probable que les tribunaux eussent admis à l'époque que les images avaient la « nécessaire qualité de confidence » ou que l'information avait été « communiquée dans des circonstances appelant un devoir de discrétion » (*ibidem*, § 111).

399. En matière de surveillance secrète, le caractère secret des mesures rend malaisé, voire impossible, pour l'intéressé d'exercer un recours, notamment aussi longtemps que dure la surveillance. Un « recours effectif » selon l'article 13 doit s'entendre d'un recours aussi effectif qu'il peut l'être eu égard à sa portée limitée, inhérente à tout système de surveillance (*Klass et autres c. Allemagne*, 1978, §§ 68-69). Un mécanisme objectif de contrôle peut être suffisant aussi longtemps que les mesures restent secrètes. Ce n'est qu'une fois les mesures divulguées que des voies de recours doivent s'ouvrir à l'individu dans un délai raisonnable (*Rotaru c. Roumanie* [GC], 2000, § 69).

400. Dans le domaine des mesures ciblées de surveillances secrètes, 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 pouvoir judiciaire offre les meilleures garanties d'indépendance, d'impartialité et de procédure régulière. Il est souhaitable d'aviser la personne concernée après la levée des mesures de surveillance dès que la notification peut être donnée sans compromettre le but de la restriction. Pour donner à l'intéressé le moyen de faire contrôler la procédure relative à l'ingérence dans l'exercice de son droit à la vie privée, il est, en principe, nécessaire de lui fournir un minimum d'informations sur la décision qu'il pourrait contester, par exemple sa date d'adoption et la juridiction dont elle émane (*Roman Zakharov c. Russie* [GC], 2015, §§ 233, 287, 294 ; *İrfan Güzel c. Turquie*, 2017, §§ 96, 98-99).

401. Dans l'affaire *Klass et autres c. Allemagne*, 1978 (§§ 65-72), où la loi « G 10 » permettait d'ouvrir et de contrôler la correspondance et les envois postaux, de lire les messages télégraphiques, d'écouter et d'enregistrer les conversations téléphoniques quand il s'agissait de défendre le pays contre des « dangers imminents », la Cour a jugé que l'ensemble des recours prévus par le droit allemand remplissait, dans les circonstances particulières de la cause, les exigences de l'article 13 au regard de l'article 8, du respect de la vie privée et de la correspondance. Même si, d'après cette loi, l'adoption et l'exécution des mesures restrictives n'étaient pas susceptibles de recours aux tribunaux, certains autres recours s'offraient à quiconque se croyait surveillé. Aux termes de l'arrêt de 1970 de la Cour constitutionnelle fédérale, l'autorité compétente devait aviser l'intéressé dès que les mesures de surveillance étaient levées et que la notification pouvait s'opérer sans compromettre le but de la restriction. À partir de cette notification, diverses voies de recours judiciaires s'ouvraient à l'individu : par une action en constatation, faire rechercher par un tribunal administratif si la loi « G 10 » avait été appliquée légitimement à l'individu et si les mesures de surveillance ordonnées étaient conformes à la loi ; introduire devant une juridiction civile une action en réparation s'il avait subi un dommage ; intenter une action en destruction ou, le cas échéant, en restitution de documents ; en dernier lieu, si aucun de ces recours n'aboutissait, se pourvoir devant la Cour constitutionnelle fédérale afin qu'elle statue sur la violation éventuelle de la Loi fondamentale. Voir

aussi, dans le même sens, les affaires *Leander c. Suède*, 1987 (§§ 78-84), concernant un système de contrôle secret des candidats à des postes importants du point de vue de la sécurité nationale, et *Amann c. Suisse* [GC], 2000 (§§ 89-90), concernant l'interception et l'enregistrement d'un appel téléphonique, et la conservation de données personnelles dans des fichiers des services de sécurité.

402. En l'absence de réponse aux doutes émis par un accusé sur la régularité de la décision de le placer sous écoutes téléphoniques, la Cour a conclu à la violation de l'article 13 combiné avec l'article 8 dans l'affaire *İrfan Güzel c. Turquie*, 2017 (§§ 100-109).

403. Dans l'affaire *Allan c. Royaume-Uni*, 2002 (§ 55), la Cour a conclu à la violation de l'article 13 combiné avec l'article 8 au motif qu'il n'existait à l'époque des faits aucune disposition légale réglementant les dispositifs d'enregistrement secrets des conversations dans la cellule du requérant et leur usage par la police.

404. Dans une affaire où le contrôle global d'un système de surveillance secrète relevait uniquement du ministère des Affaires intérieures, qui était directement impliqué dans la demande de mise en œuvre des moyens de surveillance spéciaux pour protéger la sécurité nationale, et non d'organes indépendants, la Cour a conclu à la violation de l'article 13 au regard de l'article 8 en l'absence d'un recours effectif (*Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev c. Bulgarie,* 2007, §§ 98-103).

405. En l'absence de recours pour contester la conservation, par les agents de l'État, de données sur la vie privée d'une personne ou la véracité de ces informations, la Cour a conclu à la violation de l'article 13 combiné avec l'article 8 dans l'affaire *Rotaru c. Roumanie* [GC], 2000 (§§ 68-73). Il en a été de même dans l'affaire *Segerstedt-Wiberg et autres c. Suède*, 2006 (§§ 116-122), en l'absence de recours permettant d'obtenir l'intégralité des informations figurant dans les fichiers de la Sûreté, la destruction des dossiers conservés par la Sûreté, ou la suppression ou la correction des informations à caractère personnel qui y étaient consignées.

3. Droit à la liberté et sûreté (article 5 de la Convention)

406. Dans l'affaire *Akgün c. Turquie*, 2021 (§§ 178-181), où l'utilisation par le requérant de la messagerie cryptée ByLock constituait la seule preuve qui a fondé, au moment de sa mise en détention provisoire, la raison de le soupçonner, au sens de l'article 5 § 1 c), d'avoir commis l'infraction d'appartenance à une organisation terroriste, la Cour est parvenue à un constat de violation de l'article 5 § 1 c) de la Convention. Les activités répréhensibles reprochées relevaient du crime organisé. Le recours à une preuve électronique attestant qu'un individu fait usage d'une messagerie cryptée qui avait été spécialement conçue et exclusivement utilisée par une organisation criminelle aux fins des communications internes de ladite organisation peut constituer un instrument très important pour la lutte contre la criminalité organisée. Par conséquent, une telle preuve peut valablement fonder, à son début, la détention d'une personne dans la mesure où elle peut fortement indiquer que cet individu appartient à une telle organisation. Cela étant, lorsqu'un tel élément constitue le fondement unique ou exclusif des soupçons pesant sur un suspect, le juge national doit disposer d'informations suffisantes sur cet élément avant de se pencher avec prudence sur son éventuelle valeur probante au regard du droit interne. En l'espèce le Gouvernement n'avait pas pu démontrer qu'à la date de la mise en détention provisoire du requérant, les éléments de preuve à la disposition du juge de paix répondaient au critère de « soupçons plausibles » prévu par l'article 5 § 1 c), et pouvaient ainsi convaincre un observateur objectif que le requérant avait pu commettre l'infraction pour laquelle il avait été détenu. Pour la Cour, le document relatif au constat d'utilisation de ByLock par le requérant, en tant que tel, ne mettait pas en évidence l'activité illégale du requérant dans la mesure où il ne précisait ni les dates de cette activité présumée, ni sa fréquence ou d'autres détails concernant celle-ci. Qui plus est, ni ce document, ni l'ordonnance de mise en détention provisoire n'expliquait en quoi cette activité présumée du requérant indiquerait son appartenance à une organisation terroriste.

IV. Les défis modernes de la protection des données

B. Avancées technologiques, algorithmes et intelligence artificielle[17]

407. Dans les affaires relatives au prélèvement et à la conservation, par des autorités, à des fins de prévention de la criminalité, des empreintes digitales, échantillons biologiques et profils ADN des personnes soupçonnées d'avoir commis des infractions ou condamnées, la Cour a clairement indiqué que l'usage des techniques scientifiques modernes ne pouvait pas être autorisé à n'importe quel prix et sans une mise en balance attentive des avantages pouvant résulter, d'une part, d'un large recours à ces techniques, et des intérêts essentiels s'attachant à la protection de la vie privée, de l'autre (*S. et Marper c. Royaume-Uni* [GC], 2008, § 112 ; *Podchasov c. Russie*, 2024, § 62). Tout État revendiquant un rôle de pionnier dans l'évolution de nouvelles technologies porte la responsabilité particulière de trouver le juste équilibre en la matière (*S. et Marper c. Royaume-Uni* [GC], 2008, § 112). Vu le rythme élevé auquel se succèdent les innovations dans le domaine de la génétique et des technologies de l'information, la possibilité que les aspects de la vie privée se rattachant aux informations génétiques fassent à l'avenir l'objet d'atteintes par des voies nouvelles, que l'on ne peut prévoir aujourd'hui avec précision, ne saurait être écartée (*ibidem*, § 71).

408. Pour la Cour, le développement rapide de techniques de plus en plus sophistiquées, permettant, entre autres, la reconnaissance ou la cartographie faciale à partir de photographies d'individus, rend la captation de leur image, la conservation des données ainsi recueillies et leur éventuelle diffusion problématiques. Les juridictions internes doivent en tenir compte dans l'examen de la nécessité de l'ingérence dans le droit au respect de la vie privée de l'individu concerné (*Gaughran c. Royaume-Uni*, § 70). Dans l'affaire *Gaughran c. Royaume-Uni*, 2020 (§§ 96-98), la Cour a souligné que la technologie utilisée de nos jours était plus complexe et que les juridictions internes n'avaient pas suffisamment envisagé cet aspect dans l'examen de la nécessité de l'ingérence dans le droit au respect de la vie privée de l'individu dont l'image avait été captée par les autorités suite à la réalisation d'une infraction mineure et conservée même après que la condamnation avait été rayée de son casier judiciaire à l'expiration du délai prévu par la loi.

409. Dans l'affaire *Breyer c. Allemagne*, 2020 (§ 88), la Cour a admis que, lorsqu'il s'agit de lutter contre le crime organisé et le terrorisme, les méthodes d'enquête devaient être adaptées aux moyens de communication modernes et aux changements des comportements sociétaux en matière de communication. À ses yeux, l'obligation imposées aux opérateurs de téléphonie mobile de conserver les données et de les tenir à la disposition des autorités constitue, de manière générale, une réponse adéquate à l'évolution des moyens de télécommunication et des comportements en matière de communication. En revanche, dans l'affaire *Podchasov c. Russie*, 2024 (§§ 70-79), le droit interne commandait aux fournisseurs de services de communication sur Internet de conserver et stocker le contenu de toutes les communications sur Internet pendant six mois et les données de communication associées pendant un an, ainsi que de donner aux forces de l'ordre ou aux services de sécurité accès, sur demande, aux données ainsi stockées et aux informations nécessaires pour décrypter les messages électroniques cryptés : la Cour a été frappée par l'étendue extrême de cette obligation de conservation, et elle a considéré qu'une telle ingérence était d'une ampleur et d'une gravité exceptionnelles. Elle a en outre observé que le droit interne n'imposait pas aux forces de l'ordre et aux services de sécurité l'obligation de présenter une autorisation judiciaire au fournisseur de services de communication concerné avant d'obtenir l'accès aux communications d'une personne donnée. En fait, les fournisseurs de services de communication étaient dans l'obligation d'installer

[17] Ce chapitre doit se lire conjointement avec les parties du présent guide sur le Fichage à des fins de lutte contre la criminalité et sur la Collecte de données par les autorités à travers la surveillance secrète.

des équipements qui permettaient aux autorités concernées d'accéder directement aux données stockées. Bien que dans un tel système la nécessité de garanties contre l'arbitraire et les abus soit particulièrement grande, le droit interne n'en prévoyait aucune. En ce qui concerne l'obligation légale de décrypter les communications, elle est parvenue à la conclusion qu'il apparaissait que les mesures litigieuses n'aient pas été limitées à des individus spécifiques, ce qui avait pour effet d'affaiblir le cryptage pour tous les utilisateurs, affectant ainsi tout le monde sans discrimination, y compris les personnes ne représentant aucune menace pour des intérêts légitimes ; elle a donc jugé que de telles mesures ne pouvaient pas être considérées comme proportionnées (§§ 77-79).

410. Dans une affaire relatives à une surveillance massive des communications, *Szabó et Vissy c. Hongrie*, 2016 (§ 68), la Cour a admis que les formes prises par le terrorisme de nos jours avaient pour conséquence naturelle un recours par les gouvernements à des technologies de pointe, notamment à des techniques de surveillance massive des communications, afin d'éviter des incidents imminents. En l'occurrence, la Cour a jugé que la législation autorisant la surveillance de masse ne fournissait pas les garanties nécessaires contre les abus puisque les nouvelles technologies permettaient aux autorités d'intercepter facilement un très grand nombre de données concernant des personnes se trouvant même en dehors de la catégorie initialement visée par l'opération. De plus, pareille mesure pouvait être ordonnée par le pouvoir exécutif sans aucun contrôle, sans faire l'objet d'une appréciation de la question de savoir si elle est strictement nécessaire et en l'absence de toute mesure de recours effectif, judiciaire ou autre (*ibidem*, §§ 73-89).

411. Dans l'affaire *Roman Zakharov c. Russie* [GC], 2015 (§§ 302-305), la Cour a jugé que le risque d'abus inhérent à tout système de surveillance secrète était particulièrement élevé dans un système où les services secrets et la police jouissaient, grâce à des moyens techniques, d'un accès direct à l'ensemble des communications de téléphonie mobile de la population. La Cour a conclu à la violation de l'article 8 jugeant que les dispositions du droit russe qui rendait possible l'interception généralisée des communications ne comportaient pas de garanties adéquates et effectives contre l'arbitraire et le risque d'abus inhérent à tout système de surveillance secrète.

412. Dans l'affaire *Akgün c. Turquie*, 2021 (§§ 178-181), où l'utilisation par le requérant de la messagerie cryptée ByLock constituait la seule preuve qui a fondé, au moment de sa mise en détention provisoire, la raison de le soupçonner, au sens de l'article 5 § 1 c), la Cour a souligné que l'utilisation comme fondement exclusif de tels éléments pour justifier un soupçon pourrait poser un certain nombre de problèmes délicats car, de par leur nature, la procédure et les technologies appliquées à la collecte de ces preuves sont complexes et peuvent dès lors diminuer la capacité des juges nationaux à établir leur authenticité, leur exactitude et leur intégrité (voir paragraphe 373 ci-dessus).

413. Dans les affaires *Centrum för rättvisa c. Suède* [GC], 2021, § 261, et *Big Brother Watch et autres c. Royaume-Uni* [GC], 2021, §§ 322-323, la Cour a expressément admis que le recours à un régime d'interception en masse n'était pas en soi contraire à l'article 8, vu la prolifération des menaces que font aujourd'hui peser sur les États des réseaux d'acteurs internationaux qui utilisent Internet pour communiquer et qui échappent souvent à la détection grâce à l'utilisation de technologies sophistiquées. La Cour a néanmoins souligné qu'au vu de l'évolution constante des technologies de communication modernes, son approche habituelle à l'égard des régimes de surveillance ciblée devait être adaptée aux particularités d'un régime d'interception en masse, à raison à la fois du risque d'abus inhérent à ce type d'interception et du besoin légitime, qui le caractérise, d'opérer dans le secret. En particulier, 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 devraient être appréciées à chaque étape du processus, que les activités d'interception en masse devraient être soumises à l'autorisation d'une autorité indépendante dès le départ et que les opérations devraient faire l'objet d'une supervision et d'un contrôle indépendant opéré *a posteriori*.

414. Dans l'affaire *Glukhin c. Russie*, 2023, la Cour a examiné pour la première fois la question de l'utilisation par la police d'une technologie de reconnaissance faciale. Cette technologie avait été utilisée, tout d'abord, pour identifier le requérant à partir de photographies et vidéos publiées sur une chaîne publique sur Telegram, puis pour le repérer et l'interpeller alors qu'il se déplaçait en métro. La Cour a relevé la nature très intrusive de ces mesures, soulignant qu'un niveau élevé de justification était par conséquent requis pour qu'elles puissent être considérées comme « nécessaires dans une société démocratique », le niveau de justification le plus élevé étant requis pour l'utilisation de la technologie de reconnaissance faciale en temps réel (*ibidem*, § 86). À cet égard, elle a observé que le requérant était poursuivi pour une infraction mineure, à savoir pour s'être livré à une manifestation en solo sans déclaration préalable, qu'il n'avait jamais été accusé d'avoir commis un acte répréhensible au cours de sa manifestation (blocage de la circulation, dommages aux biens ou actes de violence), et qu'il n'avait pas non plus été allégué que ses actions avaient représenté un risque pour l'ordre public ou la sécurité des transports. Au vu de ces circonstances, la Cour a considéré que l'utilisation d'une technologie de reconnaissance faciale pour identifier le requérant et, *a fortiori*, l'utilisation d'une telle technologie en temps réel pour le repérer et l'interpeller ne répondaient à aucun « besoin social impérieux » et ne pouvaient ainsi être considérées comme « nécessaires dans une société démocratique » (*ibidem*, §§ 88-90).

B. Internet et moteurs de recherche

415. 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 (*Węgrzynowski et Smolczewski c. Pologne*, 2013, § 58 ; *M.L. et W.W. c. Allemagne*, 2018, § 91 ; *Hurbain c. Belgique* [GC], 2023, §236). 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 (*Times Newspapers Ltd c. Royaume-Uni (nos 1 et 2)*, 2009, § 27).

416. Les communications en ligne et leur contenu risquent bien plus que la presse de porter atteinte à l'exercice et à la jouissance des droits et libertés fondamentaux, en particulier du droit au respect de la vie privée, et ce notamment en raison du rôle important que jouent les moteurs de recherche (*Hurbain c. Belgique* [GC], 2023, §236 ; *M.L. et W.W. c. Allemagne*, 2018, § 91 et les références qui y sont citées).

417. Les informations contenant des données à caractère personnel tenues à la disposition des moteurs de recherche par les médias peuvent facilement être repérées par les internautes. En raison de l'effet amplificateur concernant le degré de diffusion des informations et de la nature de l'activité dans laquelle s'inscrit la publication de l'information, les obligations des moteurs de recherche à l'égard de la personne concernée par l'information peuvent être différentes de celles de l'éditeur à l'origine de l'information (*Hurbain c. Belgique* [GC], 2023, § 207; *M.L. et W.W. c. Allemagne*, 2018, § 97). Au vu de la distinction qui existe entre les activités et obligations des exploitants de moteurs de recherches et celles des éditeurs de presse, les personnes concernées qui cherchent à obtenir la protection des données à caractère personnel les concernant dans ce contexte ne sont pas tenues de s'adresser, préalablement ou simultanément, au site Internet d'origine pour exercer leurs droits vis-à-vis des moteurs de recherche, dès lors qu'il s'agit ici de deux formes de traitement différentes, chacune ayant sa propre légitimité et des incidences spécifiques sur les droits et intérêts des personnes. L'on ne saurait pas non plus conditionner l'examen d'une action contre l'éditeur d'un site Internet de presse à une demande de déréférencement préalable (*Hurbain c. Belgique* [GC], 2023, § 208). Voir aussi les paragraphes ci-dessus du présent guide pour plus d'informations sur le « Droit à l'oubli ».

418. Pour la Cour, la mise à disposition d'archives sur Internet contribue à la préservation et à l'accessibilité de l'actualité et des informations (*Times Newspapers Ltd c. Royaume-Uni (nos 1 et 2)*,

2009, § 45). De telles archives constituent une source précieuse pour l'enseignement et les recherches historiques, notamment en ce qu'elles sont immédiatement accessibles au public et généralement gratuites (*Hurbain c. Belgique* [GC], 2023, § 180).Les États bénéficient d'une latitude plus large pour établir un équilibre entre les intérêts concurrents lorsque les informations sont archivées et portent sur des événements passés que lorsqu'elles ont pour objet des événements actuels (*Times Newspapers Ltd c. Royaume-Uni (nos 1 et 2)*, § 45). Le devoir de la presse de se conformer aux principes d'un journalisme responsable en vérifiant l'exactitude des informations publiées est plus rigoureux en ce qui concerne les informations qui ont trait au passé, et dont la diffusion ne revêt aucun caractère d'urgence, qu'en ce qui concerne l'actualité, par nature périssable (*ibidem*, § 45).

419. Dans l'affaire *Hurbain c. Belgique* [GC], 2023 (§§ 180-185) la Cour a noté l'émergence en Europe d'un consensus quant à l'importance des archives, précisant que celles-ci doivent, en règle générale, rester authentiques, fiables et intègres de sorte que la presse puisse s'acquitter de sa mission. Elle en a déduit que l'intégrité des archives de presse devait être le fil conducteur de tout examen d'une demande tendant à la suppression ou à la modification de tout ou partie d'un article archivé, et cela d'autant plus s'il s'agit d'un article dont la licéité n'a jamais été mise en cause. Elle a ajouté que pareilles demandes appelaient une vigilance particulière et un examen approfondi de la part des autorités nationales.

C. Transferts et flux de données

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

421. L'affaire *Big Brother Watch et autres c. Royaume-Uni* [GC], 2021 soulevait, entre autres, la question de la compatibilité avec l'article 8 de la Convention d'un partage de renseignements interceptés par de services de renseignement étrangers, en l'occurrence de l'Office national de sécurité américain (« la NSA »). La Cour a indiqué que l'échange de renseignements devrait 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. Les garanties en question s'appliquent également à la réception, par un État contractant, d'éléments interceptés demandés à un service de renseignement étranger. 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, les mêmes règles doivent s'appliquer à l'ensemble des éléments reçus qui pourraient être le produit d'une interception. 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 (*ibidem*, §§ 498-499).

Liste des affaires citées

La jurisprudence citée dans le présent guide renvoie à des arrêts et décisions rendus par la Cour européenne, ainsi que, le cas échéant, 'à des décisions et rapports de la Commission européenne des droits de l'homme (« la Commission »).

Sauf mention particulière indiquée après le nom de l'affaire, la référence citée est celle d'un arrêt sur le fond rendu par une chambre de la Cour. La mention « (déc.) » renvoie à une décision de la Cour et la mention « [GC] » signifie que l'affaire a été examinée par la Grande Chambre.

Les arrêts de chambre non « définitifs », au sens de l'article 44 de la Convention, à la date de la présente mise à jour sont signalés dans la liste ci-après par un astérisque (*). L'article 44 § 2 de la Convention est ainsi libellé : « L'arrêt d'une chambre devient définitif a) lorsque les parties déclarent qu'elles ne demanderont pas le renvoi de l'affaire devant la Grande Chambre ; ou b) trois mois après la date de l'arrêt, si le renvoi de l'affaire devant la Grande Chambre n'a pas été demandé ; ou c) lorsque le collège de la Grande Chambre rejette la demande de renvoi formulée en application de l'article 43. ». Si le collège de la Grande Chambre accepte la demande de renvoi, l'arrêt de chambre devient alors caduc et la Grande Chambre rendra ultérieurement un arrêt définitif.

Les hyperliens des affaires citées dans la version électronique du guide renvoient vers la base de données HUDOC (<*http://hudoc.echr.coe.int*>) qui donne accès à la jurisprudence de la Cour (arrêts et décisions de Grande Chambre, de chambre et de comité, affaires communiquées, avis consultatifs et résumés juridiques extraits de la Note d'information sur la jurisprudence), ainsi qu'à celle de la Commission (décisions et rapports) et aux résolutions du Comité des Ministres.

La Cour rend ses arrêts et décisions en anglais et/ou en français, ses deux langues officielles. La base de données HUDOC donne également accès à des traductions de certaines des principales affaires de la Cour dans près de trente langues non officielles. En outre, elle comporte des liens vers une centaine de recueils de jurisprudence en ligne produits par des tiers.

—A—

A.B. c. Pays-Bas, n° 37328/97, 29 janvier 2002
A.P., Garçon et Nicot c. France, n°s 79885/12 et 2 autres, CEDH 2017
A.P. c. Arménie, n° 58737/14, 18 juin 2024
Adomaitis c. Lituanie, n° 14833/18, 18 janvier 2022
Akgün c. Turquie, n° 19699/18, 20 juillet 2021
Allan c. Royaume-Uni, n° 48539/99, CEDH 2002-IX
Alexandridis c. Grèce, n° 19516/06, 21 février 2008
Alkaya c. Turquie, n° 42811/06, 9 octobre 2012
Alpha Doryforiki Tileorasi Anonymi Etairia c. Grèce, n° 72562/10, 22 février 2018
Amann c. Suisse [GC], n° 27798/95, CEDH 2000-II
Anchev c. Bulgarie (déc.), n°s 38334/08 et 68242/16, 5 décembre 2017
André et autres c. France, n° 18603/03, 24 juillet 2008
Antoneta Tudor c. Roumanie, n° 23445/04, 24 septembre 2013
Antović et Mirković c. Monténégro, n° 70838/13, 28 novembre 2017
Apostu c. Roumanie, n° 22765/12, 3 février 2015
Armonienė c. Lituanie, n° 36919/02, 25 novembre 2008
Association « 21 Décembre 1989 » et autres c. Roumanie, n°s 33810/07 et 18817/08, 24 mai 2011
Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev c. Bulgarie, n° 62540/00, 28 juin 2007
Avilkina et autres c. Russie, n° 1585/09, 6 juin 2013

Axel Springer AG c. Allemagne [GC], nº 39954/08, 7 février 2012
Axel Springer SE et RTL Television GmbH c. Allemagne, 51405/12, 21 septembre 2017
Aycaguer c. France, nº 8806/12, 22 juin 2017

—B—

B.B. c. France, nº 5335/06, 17 décembre 2009
Batiashvili c. Géorgie, nº 8284/07, 10 octobre 2019
Bărbulescu c. Roumanie [GC], nº 61496/08, 5 septembre 2017 (extraits)
Bédat c. Suisse [GC], 56925/08, CEDH 2016
Beghal c. Royaume-Uni, nº 4755/16, 28 février 2019
Benedik c. Slovénie, nº 62357/14, 24 avril 2018
Ben Faiza c. France, nº 31446/12, 8 février 2018
Bernh Larsen Holding AS et autres c. Norvège, nº 24117/08, 14 mars 2013
Biancardi c. Italie, nº 77419/16, 25 novembre 2021
Big Brother Watch et autres c. Royaume-Uni [GC], nºs 58170/13 et 2 autres, 25 mai 2021
Biriuk c. Lituanie, nº 23373/03, 25 novembre 2008
Bogomolova c. Russie, nº 13812/09, 20 juin 2017
Boljević c. Serbie, nº 47443/14, 16 juin 2020
Borislav Tonchev c. Bulgarie, nº 40519/15, 16 avril 2024
Brunet c. France, nº 21010/10, 18 septembre 2014
Breyer c. Allemagne, nº 50001/12, 30 janvier 2020
Buck c. Allemagne, nº 41604/98, CEDH 2005-IV
Buturugă c. Roumanie, nº 56867/15, 11 février 2020
Bykov c. Russie [GC], nº 4378/02, 10 mars 2009

—C—

C.C. c. Espagne, nº 1425/06, 6 octobre 2009
Cakicisoy et autres c. Chypre (déc.), nº 6523/12, 23 septembre 2014
Canonne c. France (déc.), nº 22037/13, 2 juin 2015
Caruana c. Malte (déc.), nº 41079/16, 15 mai 2018
Casarini c. Italie (déc.), nº 25578/11, 5 novembre 2024
Catt c. Royaume-Uni, nº 43514/15, 24 janvier 2019
Cherrier c. France, nº 18843/20, 30 janvier 2024
Centre pour la démocratie et l'état de droit c. Ukraine, nº 10090/16, 26 mars 2020
Centrum för rättvisa c. Suède [GC], nº 35252/08, 25 mai 2021
Cemalettin Canlı c. Turquie, nº 22427/04, 18 novembre 2008
Cevat Özel c. Turquie, nº 19602/06, 7 juin 2016
Christine Goodwin c. Royaume-Uni [GC], nº 28957/95, CEDH 2002-VI
Ciubotaru c. Moldova, nº 27138/04, 27 avril 2010
Coban c. Espagne (déc.), nº 17060/02, 25 septembre 2006
Comité de rédaction de Pravoye Delo et Shtekel c. Ukraine, nº 33014/05, CEDH 2011 (extraits)
Copland c. Royaume-Uni, nº 62617/00, CEDH 2007-I
Cossey c. Royaume-Uni, 27 septembre 1990, série A nº 184
Craxi c. Italie (nº 2), nº 25337/94, 17 juillet 2003

—D—

D.H. et autres c. Macédoine du Nord, nº 44033/17, 18 juillet 2023
D.L. c. Bulgarie, nº 7472/14, 19 mai 2006
Dalea c. France (déc.), nº 964/072 février 2010
DELTA PEKÁRNY a.s. c. République tchèque, nº 97/11, 2 octobre 2014
Demirtepe c. France, nº 34821/97, CEDH 1999-IX (extraits)
Denysyuk et autres c. Ukraine, nºs 22790/19 et 3 autres, 13 février 2025
Deveci c. Türkiye (déc.), nº 42785/11, 28 juin 2022
Dimitras et autres c. Grèce, nºs 42837/06 et 4 autres, 3 juin 2010
Dimitrov-Kazakov c. Bulgarie, nº 11379/03, 10 février 2011
Doerga c. Pays-Bas, nº 50210/99, 27 avril 2004
Dragan Petrović c. Serbie, nº 75229/10, 14 avril 2020
Dragojević c. Croatie, nº 68955/11, 15 janvier 2015
Drakšas c. Lituanie, nº 36662/04, 31 juillet 2012
Drelon c. France, nºs 3153/16 et 27758/18, 8 septembre 2022
Dudgeon c. Royaume-Uni, 22 octobre 1981, série A nº 45
Dumitru Popescu c. Roumanie (nº 2), nº 71525/01, 26 avril 2007
Dupuis et autres c. France, nº 1914/02, 7 juin 2007

—E—

Éditions Plon c. France, nº 58148/00, CEDH 2004-IV
Egeland et Hanseid c. Norvège, nº 34438/04, 16 avril 2009
Ekimdzhiev et autres c. Bulgarie, nº 70078/12, 11 janvier 2022
Elberte c. Lettonie, nº 61243/08, CEDH 2015
Erdem c. Allemagne, nº 38321/97, CEDH 2001-VII (extraits)
Ernst et autres c. Belgique, nº 33400/96, 15 juillet 2003
Eternit c. France (déc.), nº 20041/10, 27 mars 2012,

—F—

Fédération nationale des associations et syndicats de sportifs (FNASS) et autres c. France, nºs 48151/11 et 77769/13, 18 janvier 2018
Financial Times Ltd et autres c. Royaume-Uni, nº 821/03, 15 décembre 2009
Florindo de Almeida Vasconcelos Gramaxo c. Portugal, nº 26968/16, 13 décembre 2022
Foxley c. Royaume-Uni, nº 33274/96, 20 juin 2000
Frâncu c. Roumanie, nº 69356/13, 13 octobre 2020
Friedl c. Autriche, nº 15225/89, Rapport de la Commission, 19 mai 1994

—G—

G.S.B. c. Suisse, nº 28601/11, 22 décembre 2015
Gafiuc c. Roumanie, nº 59174/13, 13 octobre 2020
Gardel c. France, nº 16428/05, CEDH 2009
Garnaga c. Ukraine, nº 20390/07, 16 mai 2013
Gaskin c. Royaume-Uni, 7 juillet 1989, série A nº 160
Gaughran c. Royaume-Uni, nº 45245/15, 13 février 2020
Gauvin-Fournis et Silliau c. France, nºs 21424/16 et 45728/17, 7 septembre 2023

Gawlik c. Liechtenstein, n° 23922/19, 16 février 2021
Giesbert et autres c. France, n°s 68974/11 et 2 autres, 1er juin 2017
Gillan et Quinton c. Royaume-Uni, n° 4158/05, CEDH 2010 (extraits)
Gîrleanu c. Roumanie, n° 50376/09, 26 juin 2018
Glukhin c. Russie, n° 11519/20, 4 juillet 2023
Godelli c. Italie, n° 33783/09, 25 septembre 2012
Gorlov et autres c. Russie, n°s 27057/06 et 2 autres, 2 juillet 2019
Görmüş et autres c. Turquie, n° 49085/07, 19 janvier 2016
Grande Oriente d'Italia c. Italie, n° 29550/17, 19 décembre 2024
Grant c. Royaume-Uni, n° 32570/03, CEDH 2006-VII
Greuter c. Pays-Bas (déc.), n° 40045/98, 19 mars 2002
Guerra et autres c. Italie, n° 14967/89, *Recueil des arrêts et décisions* 1998-I
Guillot c. France, 24 octobre 1996, *Recueil des arrêts et décisions* 1996-V
Guiorgui Nikolaïchvili c. Géorgie, n° 37048/04, 13 janvier 2009
Güzel Erdagöz c. Turquie, n° 37483/02, 21 octobre 2008

—H—

Haldimann et autres c. Suisse, n° 21830/09, CEDH 2015
Halford c. Royaume-Uni, 25 juin 1997, *Recueil des arrêts et décisions* 1997-III
Hämäläinen c. Finlande [GC], n° 37359/09, CEDH 2014
Haralambie c. Roumanie, n° 21737/03, 27 octobre 2009
Hájovský c. Slovaquie, n° 7796/16, 1er juillet 2021
Haščák c. Slovaquie, n°s 58359/12 et 2 autres, 23 juin 2022
Hassine c. Roumanie, n° 36328/13, 9 mars 2021
Heglas c. République tchèque, n° 5935/02, 1er mars 2007
Henry Kismoun c. France, n° 32265/10, 5 décembre 2013
Hurbain c. Belgique [GC], n° 57292/16, 4 juillet 2023
Huvig c. France, 24 avril 1990, série A n° 176-B

—I—

I. c. Finlande, n° 20511/03, 17 juillet 2008
I. c. Royaume-Uni [GC], n° 25680/94, 11 juillet 2006
Iordachi et autres c. République de Moldova, n° 25198/02, 10 février 2009
İrfan Güzel c. Turquie, n° 35285/08, 7 février 2017
Ivashchenko c. Russie, n° 61064/10, 13 février 2018

—J—

J.L. c. Italie, n° 5671/16, 27 mai 2021
J.P.D. c. France (déc.), n° 55432/10, 16 septembre 2016
J.S. c. Royaume-Uni (déc.), 445/10, 3 mars2015
Jäggi c. Suisse, n° 58757/00, CEDH 2006-X
Jarnea c. Roumanie, n° 41838/05, 19 juillet 2011
Jecker c. Suisse, n° 35449/14, 6 octobre 2020
Joanna Szulc c. Pologne, n° 43932/08, § 13 novembre 2012

—K—

K.H. et autres c. Slovaquie, nº 32881/04, CEDH 2009 (extraits)
K.S. et M.S. c. Allemagne, nº 33696/11, 6 octobre 2016
K.U. c. Finlande, nº 2872/02, CEDH 2008
Kaczmarek c. Pologne, nº 16974/14, 22 février 2024
Kahn c. Allemagne, nº 16313/10, 17 mars 2016
Karabeyoğlu c. Turquie, nº 30083/10, 7 juin 2016
Kennedy c. Royaume-Uni, nº 26839/05, 18 mai 2010
Khadija Ismayilova c. Azerbaïdjan, nºs 65286/13 et 57270/14, 10 janvier 2019
Khan c. Royaume-Uni, nº 35394/97, CEDH 2000-V
Khoujine et autres c. Russie, nº 13470/02, 23 octobre 2008
Khelili c. Suisse, nº 16188/07, 18 octobre 2011
Kinnunen c. Finlande, nº 18291/91, décision de la Commission, 13 octobre 1993
Kinnunen c. Finlande, nº 24950/94, décision de la Commission, 15 mai 1996
Kırdök et autres c. Turquie, nº 14704/12, 3 décembre 2019
Kiyutin c. Russie, nº 2700/10, CEDH 2011
Klass et autres c. Allemagne, 6 septembre 1978, série A nº 28
Khmel c. Russie, nº 20383/04, 12 décembre 2013
Konovalova c. Russie, nº 37873/04, 9 octobre 2014
Köpke c. Allemagne (déc.), nº 420/07, 5 octobre 2010
Kotilainen et autres c. Finlande, nº 62439/12, 17 septembre 2020
Krone Verlag GmbH & Co. KG c. Autriche, nº 34315/96, 26 février 2002
Kruglov et autres c. Russie, nºs 11264/04 et 15 autres, 4 février 2020
Kruslin c. France, 24 avril 1990, série A nº 176-A
Kurier Zeitungsverlag und Druckerei GmbH c. Autriche, nº 3401/07, 17 janvier 2012
Kvasnica c. Slovaquie, nº 72094/01, 9 juin 2009

—L—

L.B. c. Hongrie [GC], nº 36345/16, 9 mars 2023
L.F. c. France (déc.), nºs 3866/20 et 9292/20, 13 février 2024
L.H. c. Lettonie, nº 52019/07, 29 avril 2014
L.L. c. France, nº 7508/02, CEDH 2006-XI
Labita c. Italie [GC], nº 26772/95, CEDH 2000-IV
Lambert c. France, nº 23618/94, *Recueil des arrêts et décisions* 1998-V
Lavents c. Lettonie, nº 58442/00, 28 novembre 2002
Le Marrec c. France (déc.), nº 52319/22, 5 novembre 2024
Leander c. Suède, 26 mars 1987, série A nº 116
Libert c. France, nº 588/13, 22 février 2018
Liberty et autres c. Royaume-Uni, nº 58243/00, 1 juillet 2008
Liblik et autres c. Estonie, nº 173/15 et 5 autres, 28 mai 2019
Liebscher c. Autriche, nº 5434/17, 6 avril 2021
López Ribalda et autres c. Espagne [GC], nºs 1874/13 et 8567/13, 17 octobre 2019
Lüdi c. Suisse, nº 12433/86, série A nº 238
Lupker et autres c. Pays-Bas, 18395/91, décision de la Commission, 7 décembre 1992

—M—

M.B. c. France, nº 22115/06, 17 décembre 2009

M.C. c. Royaume-Uni, nº 51220/13, 30 mars 2021
M.D. et autres c. Espagne, nº 36584/17, 28 juin 2022
M.G. c. Royaume-Uni, nº 39393/98, 24 septembre 2002
M.K. c. France, nº 19522/09, 18 avril 2013
M.L. et W.W. c. Allemagne, nºs 60798/10 et 65599/10, 28 juin 2018
M.M. c. Royaume-Uni, nº 24029/07, 13 novembre 2012
M.N. et autres c. Saint-Marin, nº 28005/12, 7 juillet 2015
M.P. c. Portugal, nº 27516/14, 7 septembre 2021
M.S. c. Suède, 27 août 1997, § 35, *Recueil* 1997-IV
MGN Limited c. Royaume-Uni, nº 39401/04, 18 janvier 2011
Magyar Helsinki Bizottság c. Hongrie [GC], nº 18030/11, CEDH 2016
Malanicheva c. Russie (déc.), nº 50405/06, 31 mai 2016
Malone c. Royaume-Uni, 2 août 1984, série A nº 82
Marchiani c. France (déc.), nº 30392/03, 27 mai 2008
Margari c. Grèce, nº 36705/16, 20 juin 2023
Matheron c. France, nº 57752/00, 29 mars 2005
McGinley et Egan c. Royaume-Uni, 9 juin 1998, *Recueil des arrêts et décisions* 1998-III
McVeigh, O'Neill et Evans c. Royaume-Uni, nºs 8022/77, 8025/77 and 8027/77, Rapport de la Commission, 18 mars 1981
Mediengruppe Österreich GmbH c. Autriche, nº 37718/18, 26 avril 2022
Mehmedovic c. Suisse (déc.), nº 17331/11, 11 décembre 2018
Mentzen c. Lettonie (déc.), nº 71074/01, CEDH 2004-XII
Messina c. Italie (nº 2), nº 25498/94, CEDH 2000-X
Michaud c. France, nº 12323/11, CEDH 2012
Mik et Jovanović c. Serbie (déc.), nºs 9291/14 et 63798/14, 23 mars 2021
Mikulić c. Croatie, nº 53176/99, CEDH 2002-I
Mifsud c. Malte, nº 62257/15, 29 janvier 2019
Mitov et autres c. Bulgarie (déc.), nº 80857/17, 28 février 2023
Mityanin et Leonov c. Russie, nºs 11436/06 et 22912/06, 7 mai 2018
Mockutė c. Lituanie, nº 66490/09, 27 février 2018
Modestou c. Grèce, nº 51693/13, 16 mars 2017
Moldovan c. Ukraine, nº 62020/14, 14 mars 2024
Montera c. Italie (déc.), nº 64713/01, 9 juillet 2002
Moskalev c. Russie, nº 44045/05, 7 novembre 2017
Mosley c. Royaume-Uni, nº 48009/08, 10 mai 2011
Murray c. Royaume-Uni [GC], 28 octobre 1994, série A nº 300-A
Murtazaliyeva c. Russie [GC], nº 36658/05, 18 décembre 2018
Mustafa Sezgin Tanrıkulu c. Turquie, nº 27473/06, 18 juillet 2017

—N—

N.F. et autres c. Russie, nºs 3537/15 et 8 autres, 12 septembre 2023
N. Š. c. Croatie, nº 36908/13, 10 septembre 2020
Nada c. Suisse [GC], nº 10593/08, CEDH 2012
Nagla c. Lettonie, nº 73469/10, 16 juillet 2013
Negru c. République de Moldova, nº 7336/11, 27 juin 2023
News Verlags GmbH & Co.KG c. Autriche, nº 31457/96, CEDH 2000-I
Niedbała c. Pologne, nº 27915/95, 4 juillet 2000
Nuh Uzun c. Turquie, nºs 49341/18 et 13 autres, 29 mars 2022

—O—

Odièvre c. France [GC], nº 42326/98, CEDH 2003-III
Oleynik c. Russie, nº 23559/07, 21 juin 2016

—P—

P.G. et J.H. c. Royaume-Uni, nº 44787/98, CEDH 2001-IX
P.N. c. Allemagne, nº 74440/17, 11 juin 2020
P.T. c. République de Moldova, nº 1122/12, 26 mai 2020
P. et B. c. Royaume-Uni, nº 36337/97 et 35974/97, CEDH 2001-III
P. et S. c. Pologne, nº 57375/08, 30 octobre 2012
Panteleyenko c. Ukraine, nº 11901/02, 29 juin 2006
Peck c. Royaume-Uni, nº 44647/98, CEDH 2003-I
Peers c. Grèce, nº 28524/95, CEDH 2001-III
Pendov c. Bulgarie, nº 44229/11, 26 mars 2020
Peruzzo et Martens c. Allemagne (déc.), nºs 7841/08 et 57900/12, 4 juin 2013
Perry c. Royaume-Uni, nº 63737/00, CEDH 2003-IX (extraits)
Petrova c. Lettonie, nº 4605/05, 24 juin 2014
Pietrzak et Bychawska-Siniarska et autres c. Pologne, nºs 72038/17 et 25237/18, 28 mai 2024
Pinto Coelho c. Portugal (nº 2), nº 48718/11, 22 mars 2016
Podchasov c. Russie, nº 33696/19, 13 février 2024
Polanco Torres et Movilla Polanco c. Espagne, 34147/06, 21 septembre 2010
Prado Bugallo c. Espagne, nº 58496/00, 18 février 2003
Pruteanu c. Roumanie, nº 30181/05, 3 février 2015

—R—

R.E. c. Royaume-Uni, nº 62498/11, 27 octobre 2015
Radio Twist, a.s. c. Slovaquie, nº 62202/00, CEDH 2006-XV
Radu c. République de Moldova, nº 50073/07, 15 avril 2014
Ramadan c. France (déc.), nº 23443/23, 9 janvier 2024
Rees c. Royaume-Uni, nº 9532/81, série A nº 106
Reklos et Davourlis c. Grèce, nº 1234/05, 15 janvier 2009
Reznik c. Ukraine, nº 31175/14, 23 janvier 2025
Ricci c. Italie, nº 30210/06, 8 octobre 2013
Robathin c. Autriche, nº 30457/06, 3 juillet 2012
Roche c. Royaume-Uni [GC], nº 32555/96, CEDH 2005-X
Roemen et Schmit c. Luxembourg, nº 26419/10, CEDH 2003-IV
Roman Zakharov c. Russie [GC], nº 47143/06, CEDH 2015
Rook c. Allemagne, nº 1586/15, 25 juillet 2019
Rotaru c. Roumanie [GC], nº 28341/95, CEDH 2000-V

—S—

S. et Marper c. Royaume-Uni [GC], nºs 30562/04 et 30566/04, CEDH 2008
S.V. c. Italie, nº 55216/08, 11 octobre 2018
Sanoma Uitgevers B.V. c. Pays-Bas [GC], nº 38224/03, 14 septembre 2010
Samoylova c. Russie, nº 49108/11, 14 décembre 2021

Šantare et Labazņikovs c. Lettonie, n° 34148/07, 31 mars 2016
Sârbu c. Roumanie, n° 34467/15, 28 mars 2023
Särgava c. Estonie, n° 698/19, 16 novembre 2021
Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande [GC], n° 931/13, CEDH 2017 (extraits)
Schmidt c. Allemagne (déc.), n° 32352/02, 5 janvier 2006
Sciacca c. Italie, n° 50774/99, CEDH 2005-I
Sedletska c. Ukraine, n° 42634/18, 1er avril 2021
Segerstedt-Wiberg et autres c. Suède, n° 62332/00, CEDH 2006-VII
Sérvulo & Associados - Sociedade de Advogados, RL, et autres c. Portugal, n° 27013/10, 3 septembre 2015
Sheffield et Horsham c. Royaume-Uni, 30 juillet 1998, *Recueil des arrêts et décisions* 1998-V
Sher et autres c. Royaume-Uni, n° 5201/11, CEDH 2015 (extraits)
Shimovolos c. Russie, n° 30194/09, 21 juin 2011
Silver et autres c. Royaume-Uni, 25 mars 1983, série A n° 61
Sinan Işık c. Turquie, n° 21924/05, CEDH 2010
Smirnov c. Russie, n° 71362/01, 7 juin 2007
Smith et Grady c. Royaume-Uni, n° 33985/96 et 33986/96, *Recueil des arrêts et décisions* 1999-VI
Société de Conception de Presse et d'Édition c. France, n° 4683/11, 25 février 2016
Söderman c. Suède [GC], n° 5786/08, CEDH 2013
Sommer c. Allemagne, n° 73607/13, 27 avril 2017
Sõro c. Estonie, n° 22588/08, 3 septembre 2015
Standard Verlagsgesellschaft mbH c. Autriche (n° 3), n° 39378/15, 7 décembre 2021
Stolkosa c. Pologne (déc.), n° 68562/14, 14 septembre 2021
Succession Kresten Filtenborg Mortensen c. Danemark (déc.), n° 1338/03, CEDH 2006-V
Suprunenko c. Russie (déc.) [comité], n° 8630/11, 19 juin 2018
Surikov c. Ukraine, n° 42788/06, 26 janvier 2017
Szabó et Vissy c. Hongrie, n° 37138/14, 12 janvier 2016
Szuluk c. Royaume-Uni, n° 36936/05, CEDH 2009

—T—

Taylor-Sabori c. Royaume-Uni, n° 47114/99, 22 octobre 2002
Telegraaf Media Nederland Landelijke Media B.V. et autres c. Pays-Bas, n° 39315/06, 22 novembre 2012
Tena Arregui c. Espagne, n° 42541/18, 11 janvier 2024
Témoins de Jéhovah c. Finlande, n° 31172/19, 9 mai 2023
Tillack c. Belgique, 20477/05, 27 novembre 2007
Times Newspapers Ltd c. Royaume-Uni (nos 1 et 2), nos 3002/03 et 23676/03, CEDH 2009
Toma c. Roumanie, n° 42716/02, 24 février 2009
Tønsbergs Blad A.S. et Haukom c. Norvège, n° 510/04, 1er mars 2007
Thoma c. Luxembourg, n° 38432/97, CEDH 2001-III
Trabajo Rueda c. Espagne, n° 32600/12, 30 mai 2017
Trajkovski et Chipovski c. Macédoine du Nord, nos 53205/13 et 63320/13, 13 février 2020

—U—

Ungváry et Irodalom Kft. c. Hongrie, n° 64520/10, 3 décembre 2013
Uzun c. Allemagne, n° 35623/05, CEDH 2010 (extraits)

—V—

Valašinas c. Lituanie, n° 44558/98, CEDH 2001-VIII
Valenzuela Contreras c. Espagne, n° 2767/95, *Recueil des arrêts et décisions* 1998-V
Van der Velden c. Pays-Bas (déc.), n° 29514/05, CEDH 2006-XV
Van Vondel c. Pays-Bas, n° 38258/03, 25 octobre 2007
Vasil Vasilev c. Bulgarie, n° 7610/15, 16 novembre 2021
Vasylchuk c. Ukraine, n° 24402/07, 13 juin 2013
Verlagsgruppe Droemer Knaur GmbH & Co. KG c. Allemagne, 35030/13, 19 octobre 2017
Vetter c. France, n° 59842/00, 31 mai 2005
Vicent Del Campo c. Espagne, n° 25527/13, 6 novembre 2018
Vinci Construction et GTM Génie Civil et Services c. France, n°s 63629/10 et 60567/10, 2 avril 2015
Visy c. Slovaquie, n° 70288/13, 16 octobre 2018
Volodina c. Russie (no. 2), n° 40419/19, 14 septembre 2021
Von Hannover c. Allemagne, n° 59320/00, CEDH 2004-VI
Von Hannover c. Allemagne (n° 2) [GC], n°s 40660/08 et 60641/08, CEDH 2012
Vučina c. Croatie (déc.), n° 58955/13, 24 septembre 2019
Vukota-Bojić c. Suisse, n° 61838/10, 18 octobre 2016

—W—

W. c. Pays-Bas (déc.), n° 20689/08, 20 janvier 2009
Weber et Saravia c. Allemagne (déc.), n° 54934/00, CEDH 2006-XI
Węgrzynowski et Smolczewski c. Pologne, n° 33846/07, 16 juillet 2013
Wieser et Bicos Beteiligungen GmbH c. Autriche, n° 74336/01, CEDH 2007-IV
Willems c. Pays-Bas (déc.), n° 57294/16, 9 novembre 2021
Wirtschafts-Trend Zeitschriften-Verlagsgesellschaft mbH c. Autriche (n° 2) (déc.), n° 62746/00, CEDH 2002-X
Wisse c. France, n° 71611/01, 20 décembre 2005

—X—

X et autres c. Russie, n°s 78042/16 et 66158/14, 14 janvier 2020

—Y—

Y. c. Turquie (déc.), n° 648/10, 17 février 2015
Y.B. et autres c. Turquie, n°s 48173/99 et 48319/99, 28 octobre2004
Y.G. c. Russie, n° 8647/12, 30 août 2022
Y.Y. c. Russie, n° 40378/06, 23 février 2016
Yonchev c. Bulgarie, n° 12504/09, 7 décembre 2017
Youth Initiative for Human Rights c. Serbie, n° 48135/06, 25 juin 2013
Yvonne Chave née Jullien c. France, n° 14461/88, décision de la Commission du 9 juillet 1991

—Z—

Z c. Finlande, 25 février 1997, *Recueil des arrêts et décisions* 1997-I
Zoltán Varga c. Slovaquie, n°s 58361/12 et 2 autres, 20 juillet 2021