Revue québécoise de droit international
Quebec Journal of International Law
Revista quebequense de derecho internacional

Données personnelles et surveillance massive : quelle protection face aux ingérences des autorités publiques?

Roberto Angrisani

Numéro hors-série, décembre 2020

70 ans de la *Convention européenne des droits de l'homme* : L'Europe et les droits de la personne

URI : https://id.erudit.org/iderudit/1078532ar
DOI : https://doi.org/10.7202/1078532ar

Aller au sommaire du numéro

Éditeur(s)

Société québécoise de droit international

ISSN

0828-9999 (imprimé)
2561-6994 (numérique)

Découvrir la revue

Citer cet article

Angrisani, R. (2020). Données personnelles et surveillance massive : quelle protection face aux ingérences des autorités publiques? *Revue québécoise de droit international / Quebec Journal of International Law / Revista quebequense de derecho internacional*, 107–134. https://doi.org/10.7202/1078532ar

Résumé de l'article

Les données à caractère personnel représentent aujourd'hui l'un de bien le plus important faisant l'objet d'échanges tant dans le secteur privé et commercial que dans le secteur public, entre services répressifs ou de renseignement. Le Conseil de l'Europe s'est très rapidement préoccupé des risques et des enjeux liés au respect des droits de l'homme lors du traitement de données à caractère personnel, appuyé grandement par l'activité interprétative de la Cour européenne des droits de l'homme qui a su élargir la portée de l'article 8 de la *Convention européenne des droits de l'homme (CEDH)*, au point d'y inclure la protection de toute donnée à caractère personnel. Les autorités publiques font une utilisation grandissante des données personnelles de citoyens et ressortissants de pays tiers et les révélations en matière de surveillance massive en sont une preuve éloquente. Cet article, mettant en exergue le fait que la jurisprudence de la Cour européenne des droits de l'homme a - au fil des décennies - permis de mitiger les violations des droits fondamentaux des personnes dans ce domaine, vise à souligner qu'il est aujourd'hui plus que jamais légitime de s'interroger sur le fait de savoir si la protection offerte par la *CEDH* est encore adaptée aux défis contemporains liés à la protection des données à caractère personnelles.

DONNÉES PERSONNELLES ET SURVEILLANCE MASSIVE : QUELLE PROTECTION FACE AUX INGÉRENCES DES AUTORITÉS PUBLIQUES?

Roberto Angrisani[*]

Les données à caractère personnel représentent aujourd'hui l'un de bien le plus important faisant l'objet d'échanges tant dans le secteur privé et commercial que dans le secteur public, entre services répressifs ou de renseignement. Le Conseil de l'Europe s'est très rapidement préoccupé des risques et des enjeux liés au respect des droits de l'homme lors du traitement de données à caractère personnel, appuyé grandement par l'activité interprétative de la Cour européenne des droits de l'homme qui a su élargir la portée de l'article 8 de la *Convention européenne des droits de l'homme* (*CEDH*), au point d'y inclure la protection de toute donnée à caractère personnel. Les autorités publiques font une utilisation grandissante des données personnelles de citoyens et ressortissants de pays tiers et les révélations en matière de surveillance massive en sont une preuve éloquente. Cet article, mettant en exergue le fait que la jurisprudence de la Cour européenne des droits de l'homme a - au fil des décennies - permis de mitiger les violations des droits fondamentaux des personnes dans ce domaine, vise à souligner qu'il est aujourd'hui plus que jamais légitime de s'interroger sur le fait de savoir si la protection offerte par la *CEDH* est encore adaptée aux défis contemporains liés à la protection des données à caractère personnelles.

Personal data are today one of the most important commodities exchanged both in the private and in the public sector, between law enforcement or intelligence services. The Council of Europe has very quickly become concerned about the risks and vulnerabilities related to the respect of human rights when processing personal data, greatly supported by the interpretative activity of the European Court of Human Rights, which has been able to broaden the scope of Article 8 *European Convention on Human Rights* (*ECHR*) to include the protection of all personal data. Public authorities are making increasing use of personal data of citizens and third-country nationals and the revelations in the field of mass surveillance are eloquent proofs of this. This article, highlighting the fact that the case-law of the European Court of Human Rights has - over the decades - mitigated violations of fundamental rights of individuals in this area, aims to underline that it is now more legitimate than ever to question whether the protection offered by the ECHR is still adequate to the contemporary challenges of personal data protection.

Los datos personales representan hoy en día uno de los bienes más importantes que se intercambian tanto en el sector privado y comercial como en el sector público, entre los servicios de represión o de inteligencia. El Consejo de Europa se ha preocupado muy rápidamente por los riesgos y desafíos relacionados con el respeto de los derechos humanos en el tratamiento de los datos personales, apoyado en gran medida por la actividad interpretativa del Tribunal Europeo de Derechos Humanos, que ha podido ampliar el alcance del artículo 8 del *Convenio Europeo de Derechos Humanos* para incluir la protección de todos los datos personales. Las autoridades públicas utilizan cada vez más los datos personales de los ciudadanos y de los nacionales de terceros países y las revelaciones en el ámbito de la vigilancia de masas son una prueba elocuente de ello. Este artículo, en el que se destaca el hecho de que la jurisprudencia del Tribunal ha atenuado -a lo largo de los decenios- las violaciones de los derechos fundamentales de las personas en esta esfera, tiene por objeto subrayar que ahora es más legítimo que nunca cuestionar si la protección que ofrece el *Convenio* sigue siendo adecuada a los desafíos contemporáneos de la protección de los datos personales

[*] Chargé de cours en droit de l'Union européenne et chercheur à la Chaire Jean Monnet en intégration européenne de l'Université Laval.

Depuis le début des temps, l'humanité a connu une multitude d'étapes et de phases différentes, chacune caractérisée par des découvertes ou des éléments qui ont changé le quotidien et sont devenus, au fil des années, le centre d'intérêt principal de la majorité de la population. À partir de la pierre, à travers le feu, en passant par la soie, nous pouvons dire, avec une certaine assurance, que l'ère que nous vivons présentement est « l'ère des données ». L'utilisation et l'exploitation des informations à caractère personnel revêtent une importance capitale dans la société contemporaine et en perspective, ce phénomène est destiné à augmenter dans le futur. « Tout en saluant les progrès historiques des technologies de l'information et de la communication (TIC) et les effets positifs qui en découlent pour les individus »[1], les institutions européennes n'ont pas manqué de manifester leur inquiétude envers « des possibilités jusqu'alors impensables d'identifier les individus grâce à leurs données »[2]. Possibilité que les technologies offrent à un nombre toujours croissant d'acteurs privés et d'instances publiques[3].

Dans ce cadre, la *Convention de sauvegarde des droits de l'homme et des libertés fondamentales* (*CEDH*)[4] assure la protection des données à caractère personnel, par le biais de son article 8. La jurisprudence de la Cour européenne des droits de l'Homme (CourEDH ou Cour) a élargi la portée de l'article 8, qui était initialement voué au respect de la vie privée et familiale en sens large, au point d'y inclure la protection des données à caractère personnel[5].

Ainsi, ce droit fondamental à la protection des données, tel qu'interprété par la CourEDH, a été une grande source d'inspiration dans le panorama juridique international, et il est maintenant inscrit aussi dans la *Charte des droits fondamentaux de l'Union européenne*[6] (*CDFUE*) et dans de nombreuses constitutions nationales[7] des États parties au Conseil de l'Europe. De surcroît, d'autres instruments internationaux de protection des droits fondamentaux, adoptés notamment sous l'égide des Nations Unies, font mention de la protection des données en tant

---

1 Conseil de l'Europe, AP, 2011 4e sess, *La protection de la vie privée et des données à caractère personnel sur l'internet et les médias en ligne*, Doc 12695 (2011) [*Protection de la vie privée*].

2 *Ibid*.

3 *Ibid*.

4 *Convention de sauvegarde des droits de l'homme et des libertés fondamentales*, 4 novembre 1950, 213 RTNU 221 (entrée en vigueur : 3 septembre 1953) [*Convention européenne des droits de l'homme*].

5 *Protection de la vie privée*, *supra* note 1 au para 16.

6 CE, *Charte des droits fondamentaux de l'Union européenne*, [2012] JO, C 326/02 [*Charte des droits fondamentaux*]; la *Convention* est également le texte de référence de nombreux textes internationaux et nationaux, en commençant par la directive 95/46/CE de l'Union européenne (CE, *Directive 95/46/CE du Parlement Européen et du Conseil*, [1995] JO, L 281), laquelle constitue un développement des principes de la *Convention*. À cet égard, dans son préambule, elle précise et amplifie les principes de la *Convention*; Les mêmes principes, développés et complétés, sont présents dans le règlement (UE) 2016/679 (CE, *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données)*, [2016] JO, L 119/1 [*Règlement général sur la protection des données*]).

7 Par exemple l'Allemagne en 1971, la Suède en 1973 et la France en 1978.

qu'extension du droit au respect de la vie privée[8]. Dans ce domaine, le Conseil de l'Europe adopte de plus en plus de conventions et de protocoles ouverts à la signature de pays qui ne sont pas parties à la *CEDH*.

Dans cette quête d'universalité, l'action du Conseil de l'Europe produit des effets même à l'extérieur du système régional, en poussant la promotion des droits fondamentaux à l'échelle mondiale. C'est pour cette raison que tout au long de ce travail nous ferons parfois référence aux autres textes internationaux de protection des droits de l'homme.

Néanmoins, avant d'entrer dans le vif de l'analyse, il nous semble opportun de souligner la divergence d'approche existante en matière de « définition » des garanties offertes par l'article 8. Si d'une part la doctrine traditionnelle[9] utilise toujours la formule « protection des données à caractère personnel » pour indiquer une portion plus large du droit à la protection à la vie privée couverte par l'article 8§1 de la *CEDH*, une autre partie minoritaire[10] du panorama scientifique préfère rester fidèle à la nomenclature de la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* (*Convention STE 108*)[11]. Ce document, dès son intitulé, met au centre la personne et ses droits. Compte tenu de la marchandisation progressive des données à caractère personnel, cette deuxième approche est à notre avis souhaitable, notamment lorsque l'intention est celle de remettre l'individu et son intégrité physique et morale au centre du discours juridique.

La question posée se rattache à la problématique de la protection des données que la CourEDH offre par le biais de l'article 8 *CEDH*[12]. Cela nous permet de mettre

---

8 Voir l'article 12 de la *Déclaration universelle des droits de l'Homme* relativement au droit au respect de la vie privée, Rés AG 217A (III), Doc off AG NU, 3e sess, supp n°13, Doc NU A/810 (1948) 71, et l'article 17 du *Pacte international relatif aux droits civils et politiques*, 19 décembre 1966, 999 RTNU 171 (entrée en vigueur : 23 mars 1976) qui protège le droit à la protection de la vie privée, de la famille, du domicile et de la correspondance.

9 Fréderic Sudre, Droit européen et international des droits de l'homme, 10e éd, Paris, Presses Universitaires de France, 2011 [Sudre, « Droit européen »]; Andrea Manzella et al, *Riscrivre i diritti in Europa*, Bologne, il Mulino, 2001; Agence des droits fondamentaux de l'Union européenne, Manuel de droit européen en matière de protection des données, Luxembourg, Office des publications de l'Union européenne, 2014 [Manuel de droit européen]; Fréderic Sudre et al, Les grands arrêts de la Cour européenne des droits de l'homme, 6e éd, Paris, Thémis, 2011 [Sudre, « Les grands arrêts »].

10 Michel Gentot, « La protection des données personnelles à la croisée des chemins » dans Pierre Tabatoni, dir, *La protection de la vie privée dans la société de l'information*, Tome 3, Paris, Presses Universitaires de France, 2000.

11 *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, 28 janvier 1981, 1496 RTNU 65 (entrée en vigueur : 1er octobre 1985) [*Convention STE 108*]; telle que modifiée par le Conseil de l'Europe, Comité des ministres, *Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel*, 10 janvier 2018, STCE 223 [*Protocole d'amendement*]; voir l'article 1, chapitre 1 : « Le but de la présente *Convention* est de protéger toute personne physique, quelle que soit sa nationalité ou sa résidence, à l'égard du traitement des données à caractère personnel, contribuant ainsi au respect de ses droits de l'homme et de ses libertés fondamentales et notamment du droit à la vie privée ».

12 *Convention européenne des droits de l'homme*, *supra* note 4, art 8 : « 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

rapidement en relief les passages fondamentaux de l'évolution de cette norme et de son interprétation par la Cour dans le cadre du Conseil de l'Europe.

En regardant l'évolution juridique des institutions régionales européennes, nous constatons que le Conseil de l'Europe s'est très rapidement préoccupé des risques et des enjeux liés au respect des droits de l'homme lors du traitement de données à caractère personnel. Il a par ailleurs adopté, au début des années 1970, deux résolutions à cet effet[13]. Par souci d'harmonisation, le 28 janvier 1981, l'Assemblée parlementaire du Conseil de l'Europe a ainsi jugé opportun de synthétiser ces résolutions en une seule convention, la *Convention STE 108*[14] - ouverte à la signature des États non parties à la *CEDH*[15] -, et récemment amendée par le *Protocole*[16] adopté par le Comité des ministres lors de sa 128e session à Elseneur, le 18 mai 2018[17].

Sur le plan terminologique, la portée de la notion de « vie privée » n'a toujours pas tout à fait été délimitée. Elle a entre-temps été considérablement révisée dans une série d'arrêts[18], notamment dans l'*affaire S. et Marper c. Royaume-Uni* du

---

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 ».

13 Conseil de l'Europe, Comité des ministres, 28e sess, *Rapport explicatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, 1981 art 4(3) en ligne : *COE* <rm.coe.int/09000016800ca471>; voir la Résolution (73) 22 de 1973 (Conseil de l'Europe, Comité des ministres, *Résolution (73) 22 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé* (1973)) qui énonçait les principes de la protection des données pour le secteur privé et la Résolution (74) 29 de 1974 (Conseil de l'Europe, Comité des ministres, *Résolution (74) 29 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur public* (1974)) qui a fait la même chose pour le secteur public.

14 Gentot, *supra* note 10; Jean-Philippe Walter, allocution, Groupe de rapporteurs sur la coopération juridique (GR-J), présenté au Conseil de l'Europe, 7 octobre 2014 [non publiée], en ligne : *COE* <rm.coe.int/09000016806b2950> [Walter] : « Aujourd'hui ce texte a été ratifié par 45 États sur 47 États membres et l'Uruguay est devenu en août 2013 le premier État non-membre du Conseil de l'Europe à y adhérer ».

15 *Convention européenne des droits de l'homme*, *supra* note 4; cette convention est entrée en vigueur le 1er octobre 1985. Elle a, à l'heure actuelle, été ratifiée par tous les États membres exception faite de la République de St. Marin et la Turquie; le 10 avril 2013, l'Uruguay est devenu le premier pays non-membre partie de la *Convention*.

16 *Protocole d'amendement*, *supra* note 11.

17 Gentot, *supra* note 10; pour l'évolution des travaux législatifs, voir aussi Conseil de l'Europe, CAHDATA, 3e réunion, *Document de travail : Convention 108 avec son Protocole additionnel et propositions de modernisation* 9 avril 2014 [non publié], en ligne : *COE* <rm.coe.int/0900001680591224>.

18 Voir *Klass et autres c Allemagne* (1978), 28 CEDH (Sér A) [*Klass c Allemagne*]; *Malone c Royaume-Uni* (1984), 95 CEDH (Sér A); *Leander c Suède* (1987), 116 CEDH (Sér A); *Gaskin c Royaume-Uni* (1989), 160 CEDH (Sér A); *Halford c Royaume-Uni* (1997), 1997-III CEDH; *Amann c Suisse* [GC], n°27798/95, [2000] II CEDH 201; et *Rotaru c Roumanie* [GC], n°28341/95, [2000] V CEDH 61; notamment dans l'*arrêt Niemietz c Allemagne* (1992), 251-B CEDH (Sér A), on retrouve un passage édifiant : « Il sera toutefois trop restrictif de la limiter à un "cercle intime" où chacun peut mener sa vie personnelle à sa guise et d'en écarter entièrement le monde extérieur à ce cercle. Le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l'individu de nouer et développer des relations avec ses semblables ».

4 décembre 2008[19], où « la Cour rappelle que la notion de vie privée est une notion large, non susceptible d'une définition exhaustive, qui recouvre l'intégrité physique et morale de la personne »[20]. En se référant à l'article 8 il est donc possible, par la Cour, d'englober de multiples aspects de la vie d'un individu, à partir de la protection de son domicile ou de la vie familiale, en passant par la protection du droit à la correspondance jusqu'aux questions qui ont trait à la liberté sexuelle.

En considérant l'étendue de la matière et l'impossibilité de traiter de façon satisfaisante tous les aspects liés aux traitements de données à caractère personnel, nous allons concentrer notre analyse sur l'utilisation faite par l'autorité publique des données personnelles, notamment dans le cadre des ingérences justifiées (ou que l'on présume être justifiées) par des nécessitées liées 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 »[21]. Les objets de notre étude seront ainsi l'utilisation des données à caractère personnel faite par les autorités de police et la justice pénale, avec une attention particulière envers la jurisprudence récente en matière de surveillance massive[22].

À cet effet, nous puiserons dans les principes dégagés par la jurisprudence de la Cour EDH et dans les sources de droit qu'elle applique, afin de trouver des éléments de réponse à la question suivante : dans quelle mesure la protection offerte par la *CEDH* s'adapte au contexte changeant qui pousse les autorités publiques à une utilisation grandissante de données à caractère personnel?

À partir de la lecture combinée faite par la Cour de l'article 8 et de différentes conventions qui lient les États parties du Conseil de l'Europe à ce sujet, il semble y avoir une interprétation plutôt dynamique[23], voir évolutive (I) du droit à la protection des données à caractère personnel. Toutefois, la jurisprudence récente en matière d'utilisation par les autorités publiques des données à caractère personnel, montre que l'action de la Cour EDH, tout en ayant un impact remarquable, rencontre des limites notamment face aux phénomènes de surveillance massive (II).

---

19 *S et Marper c Royaume-Uni* [GC], n°30562/04, [2008] V CEDH 213.

20 Sudre, « Les grands arrêts », *supra* note 9.

21 *Convention européenne des droits de l'homme*, *supra* note 4, art 8.

22 L'expression « surveillance massive » a été pour la première fois utilisée au sein du Conseil de l'Europe par la Commission des questions juridiques et des droits de l'homme (Conseil de l'Europe, AP, 2015 sess parlementaire (2e partie), Textes adoptés, Rec 2067), qui, le 6 novembre 2013, a nommé Pieter Omtzigt Rapporteur sur « les opérations massives de surveillance » (Conseil de l'Europe, AP, 2013 sess ordinaire (4e partie), proposition de résolution, *Les opérations massives de surveillance en Europe*, Doc 13288); voir également Conseil de l'Europe, AP, 2013 sess ordinaire (4e partie), proposition de recommandation, *Protocole additionnel à la Convention européenne des droits de l'homme sur la protection des donneurs d'alerte qui révèlent des agissements des pouvoirs publics constituant une violation du droit international et des droits fondamentaux,* Doc 13278.

23 Sudre, « Les grands arrêts », *supra* note 9 à la p 495.

I. L'action de la CourEDH : pierre angulaire de la protection « classique » du droit à la protection des données à caractère personnel

Le paragraphe 1 de l'article 8 *CEDH* nous dit que « [t]oute personne a droit au respect de sa vie privée ». Les destinataires de cette norme sont, au même titre, les citoyens et les gouvernements des quarante-sept pays membres ayant ratifié la *Convention*. Forte d'une expérience de plusieurs décennies d'activité juridictionnelle, la CourEDH a vite montré que cette norme toute seule n'était pas suffisante à couvrir la complexité des questions à trancher dans un domaine en évolution continue tel que les données personnelles.

En effet, la protection des données à caractère personnel présente une nature à la fois « horizontale »[24] et « transversale »[25], du fait qu'il s'agit d'un aspect qui touche désormais à tous les domaines de notre quotidien. Au fil des années, la CourEDH a tracé le chemin pour une protection toujours plus large et englobante des données à caractère personnel, par le biais d'une interprétation évolutive de l'article 8. De surcroit, le « *model* » de protection créé par les juges de Strasbourg a été pris en exemple par d'autres juridictions internationales – notamment la Cour de justice de l'Union européenne – jusqu'au point d'être considéré le modèle « classique » de protection de ce droit.

A. Les influences de la jurisprudence de la CourEDH sur un droit en évolution

Avec le développement des technologies et la mondialisation des échanges et des traitements de données personnelles,

> le droit à la protection des données est devenu incontournable non seulement pour garantir le respect des droits et des libertés fondamentales lors du traitement de données personnelles, mais aussi pour garantir l'État de droit et le fonctionnement de la démocratie[26].

Sur le plan international, la CourEDH agit en tant que chef de file dans la promotion et la défense de ce droit. Ce leadership se justifie par des arrêts courageux et avant-gardistes qui ont généré des avancées importantes vers le progrès au niveau législatif. L'*affaire Klass et autres c. Allemagne*[27] représente probablement le premier arrêt prononcé par la Cour sur une question de protection de données personnelles, destiné à faire école. À la base de cette affaire, il y avait le recours présenté en 1971 par un juge et des avocats allemands soulevant des doutes sur la compatibilité d'une réforme – introduite en 1968 – de l'article 10 de la *Loi fondamentale pour la République fédérale d'Allemagne*[28] avec la *CEDH*.

---

24 *Droit européen*, *supra* note 9 à la p 326.
25 Walter, *supra* note 1414.
26 *Ibid*.
27 *Klass c Allemagne*, *supra* note 18 aux para 49–50.
28 All, *Loi fondamentale pour la République fédérale d'Allemagne* (*RFA*), 1949, art 10.

En effet, « [l]es requérants contestaient la possibilité même de mesures de surveillance secrètes adoptées sans notification à l'intéressé, ainsi que la substitution à un contrôle par le juge d'un contrôle parlementaire »[29]. Tranchant cette question, dans le contexte difficile de post-occupation de l'Allemagne, « [l]a cour dans cette affaire a fait preuve d'un réalisme salutaire car il était impératif d'admettre des restrictions afin de lutter efficacement contre le terrorisme »[30] :

> Les sociétés démocratiques se trouvent menacées de nos jours par des formes très complexes d'espionnage et par le terrorisme, de sorte que l'Éta[t] doit être capable, pour combattre efficacement ces menaces, de surveiller en secret les éléments subversifs opérant sur son territoire. La Cour doit donc admettre que l'existence de dispositions législatives accordant des pouvoirs de surveillance secrète de la correspondance, des envois postaux et des télécommunications est, devant une situation exceptionnelle, nécessaire dans une société démocratique à la sécurité nationale et/ou à la défense de l'ordre et à la prévention des infractions pénales[31].

Cependant, elle met en relief l'impératif de balancement des instances sécuritaires collectives avec la protection des droits de l'individu. Il ne faut pas alors perdre de vue que ces restrictions doivent toujours se faire dans le respect des droits fondamentaux.

> La Cour souligne néanmoins que les États contractants ne disposent pas pour autant d'une latitude illimitée pour assujettir à des mesures de surveillance secrète les personnes soumises à leur juridiction. Consciente du danger, inhérent à pareille loi, de saper, voire de détruire, la démocratie au motif de la défendre, elle affirme qu'ils ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure jugée par eux appropriée[32].

Ces mots sont incroyablement d'actualité après bientôt quarante ans, mais le juge de Strasbourg à l'époque de l'*arrêt Klass et autres c. Allemagne*, ne disposait d'aucun instrument normatif supplémentaire. Le regard sur la question a ainsi uniquement été posé à travers l'article 8 de la *Convention*, qui comme avec un prisme a décomposé le concept traditionnel de protection de la vie privée et a pu montrer la présence indissoluble du droit à la protection des données à caractère personnel dans l'éventail des garanties offertes par cet article.

À partir de là, la communauté internationale s'est penchée sur la question, poussant l'émergence d'une série – pas toujours harmonisée – d'accords, de protocoles et lois nationales, qui ont composé de manière progressive le corpus normatif existant aujourd'hui en matière de protection des données à caractère personnel.

La lumière jaillissante de l'article 8, grâce à l'interprétation de la CourEDH, a eu un grand impact à la fois au niveau national et international. L'Allemagne, la Suède

---

29 Sydney Adoua, *La lutte contre le terrorisme et le respect des droits de l'homme*, Mémoire Master 2, Université d'Orléans, 2004 à la p 7.

30 *Ibid.*

31 *Klass c Allemagne*, *supra* note 18 au para 48.

32 *Ibid* au para 49.

et la France ont été les premières nations à se doter d'une loi pour la protection des données.

Les impacts les plus évidents de l'action de la CourEDH n'ont pas tardés à se manifester même dans d'autres systèmes régionaux. L'Union européenne, dont tous les Pays membres sont aussi parties à la *CEDH*, a d'abord émis la *Directive 46/95/CE* du 24 octobre 1995[33] qui qualifie de « données à caractère personnel » :

> toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité [...][34].

La *CDFUE*[35] a ensuite perfectionné cette tutelle confiant à travers deux articles distincts le « respect de la vie privée familiale »[36] et la « protection des données à caractère personnel »[37]. Avec l'entrée en vigueur du *Traité de Lisbonne*[38], la *CDFUE* est enfin rentrée en tant que telle dans le droit primaire de l'Union par le biais de l'article 6 du TFUE[39]. Toutefois, le vrai phare de ces progrès a toujours été le Conseil de l'Europe dans la mesure où il a su adapter son activité législative aux enseignements découlant de la jurisprudence de la CourEDH. L'adoption en 2016 du *Règlement général pour la protection des données*[40], montre à quel point cette influence a été marquante aussi dans le droit de l'UE.

Dans les prochains paragraphes, nous verrons en détail les actes qui ont été produits et dans quelle mesure l'activité prétorienne de la *Cour* a été déterminante pour atteindre les hauts niveaux de protection des données à caractère personnel en vigueur aujourd'hui.

---

33 CE, *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, [1995] JO, L281/31.

34 *Ibid* art 2 a); dans *Règlement général sur la protection des données*, *supra* note 6, la même définition est reportée comme suit à l'article 4(1) : « "données à caractère personnel", toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée"); est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

35 *Charte des droits fondamentaux*, *supra* note 6.

36 *Ibid*, art 7.

37 *Ibid*, art 8; selon l'article 8 : « 1. Toute personne a droit à la protection des données à caractère personnel la concernant; 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification; 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».

38 *Traité de Lisbonne modifiant le Traité sur l'Union européenne et le Traité instituant la Communauté européenne*, 13 décembre 2007, 2702 RTNU 1 (entrée en vigueur : 1er décembre 2009).

39 CE, *Traité sur le fonctionnement de l'Union européenne,* [2012] JO, C 326/47.

40 *Règlement général sur la protection des données*, *supra* note 6.

1. La protection limitée offerte par la Cour à partir de l'article 8 jusqu'à l'adoption de la *Convention STE 108* par le Conseil de l'Europe

Au sein du Conseil de l'Europe, la reconnaissance explicite du droit fondamental à la protection des données à caractère personnel figure, pour la première fois, dans la *Convention STE 108*[41]. Ce texte

> impose l'obligation aux États parties de garantir, sur leur territoire, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant (« protection des données »)[42].

La CourEDH définit un certain nombre de principes notamment concernant l'importance de la qualité des données, qui elles doivent

> être adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées (principe de proportionnalité); à leur exactitude; à la confidentialité des données sensibles; à l'information de la personne concernée et à son droit à l'accès et à la rectification des données[43].

L'*affaire Mc Veigh, O' Neill et Evans c. Royaume-Uni*[44] de 1981 figure parmi les premières requêtes à voir appliquer les critères et les garanties de la nouvelle *Convention* à certaines violations présumées du droit à la protection des données que les requérants disent avoir subies durant une période de détention. L'un des arrêts les plus intéressants, du fait de la portée novatrice de son contenu, est aussi *Leander c. Suède*[45], introduit en 1985 et tranché définitivement par la *Cour* en 1987. Il s'agissait d'un ancien charpentier qui, à la suite d'un « contrôle personnel »[46] réunissant sur son compte des informations secrètes, avait été jugé trop peu fiable pour être gardien d'un musée dont plusieurs entrepôts se trouvaient dans une zone militaire. L'objet principal de la question était donc la légitimité du fichier secret de la police, utilisé en cas de candidature d'une personne à un emploi important pour la sécurité nationale. En l'espèce la Cour a statué sur un aspect essentiel de l'article 8 :

> [...] la compilation, la conservation, l'utilisation et la communication par l'État de données à caractère personnel, par exemple dans un fichier de police, emportent ingérence dans le droit au respect de la vie privée de chacun, tel que garanti par l'article 8§1 de la Convention[47].

---

41 Gentot, *supra* note 10.

42 Agence des droits fondamentaux de l'Union européenne, *La protection des données à caractère personnel dans l'Union européenne: le rôle des autorités nationales chargées de la protection des données. Renforcement de l'architecture des droits fondamentaux au sein de l'UE II*, Luxembourg, Office des publications de l'Union européenne, 2012 à la p 12.

43 *Ibid*.

44 *McVeigh, O'Neill et Evans* (1982), Comm Eur DH DR, n°8022/77.

45 *Leander c Suède*, *supra* note 18.

46 *Ibid* aux para 9 et 10.

47 Conseil de l'Europe, Division de la recherche de la Cour européenne des droits de l'homme, *Internet : la jurisprudence de la Cour européenne des droits de l'homme* (rapport), 2015, à la p 9, en ligne : *COE* <www.echr.coe.int>.

Ce principe a été successivement à la base de nombreuses décisions dans les années suivantes. Il représente un gros pas en avant dans la direction d'une protection tous azimuts des données à caractère personnel et définit une limite importante aux ingérences de l'autorité publique.

Au fil des années le Conseil de l'Europe a adopté d'autres instruments législatifs afin d'adapter la norme de l'article 8 à l'évolution de la technologie et de la société. De surcroît, parmi les nombreuses recommandations[48], nous retrouvons des textes comme la *Convention sur les droits de l'homme et de la médecine*[49], qui est devenue une véritable référence en matière de traitement de données médicales et sur le terrain de la recherche bio médicale. Dans ce sens, tout en revenant au champ de la protection des données en sens large, une autre recommandation très importante est la *Convention sur la cybercriminalité*[50], qui vise à protéger les données personnelles contre les atteintes portées par les personnes privées. Aussi connue sous le nom de *Convention de Budapest*, ce texte prévoit une série de mesures – incluant du droit pénal matériel –, que les États contractants s'engagent à mettre en œuvre afin de combattre conjointement le crime informatique, notamment en prévenant les « [i]nfractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques »[51] (sujet privé)[52].

La *Convention STE 108* a toujours fait preuve de dynamisme, car pendant longtemps elle a été « le seul instrument international juridiquement contraignant dans le domaine de la protection des données et de par son caractère ouvert, elle a une vocation universelle, susceptible de pallier l'absence de convention mondiale »[53]. Le Conseil a adopté plusieurs protocoles pour la mise à jour du texte et a créé des organismes spécialisés pour la finalisation d'un nouveau protocole capable de répondre le mieux possible aux grands défis de la mondialisation. Qui plus est, avec l'aide du Comité consultatif (TP-D), le Comité des ministres, en vertu de l'article 17 du *Statut*

---

48 Il s'agit des plus importants documents complémentaires à la *Convention STE 108*; voir : Conseil de l'Europe, Comité des ministres, *Recommandation R(95) 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques* (1995); Conseil de l'Europe, Comité des ministres, *Recommandation R(97) 5 relative à la protection des données médicales* (1997); Conseil de l'Europe, Comité des ministres, *Recommandation R(97) 18 concernant la protection des données à caractère personnel collectées et traitées à des fins statistiques* (1997); Conseil de l'Europe, Comité des ministres, *Recommandation R(99) 5 sur la protection de la vie privée sur Internet* (1999); et Conseil de l'Europe, Comité des ministres, *Recommandation R(2002) 9 sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance* (2002).

49 *Convention pour la protection des droits de l'homme et de la dignité de l'être humain à l'égard des applications de la biologie et de la médecine : Convention sur les Droits de l'Homme et la biomédecine*, 4 avril 1997, 2137 RTNU 171, (entrée en vigueur : 1er décembre 1999).

50 *Convention sur la cybercriminalité*, 23 novembre 2001, 2296 RTNU 167, (entrée en vigueur : 1er juillet 2004) [*Convention sur la cybercriminalité*].

51 *Ibid*, titre 1.

52 *Ibid*, art 37; au même titre que la *Convention STE 108* est une convention ouverte à l'adhésion d'États tiers.

53 Walter, *supra* note 14 à la p 2.

du Conseil de l'Europe[54] et selon la *Résolution CM/RES (2011)24*[55] concernant les comités intergouvernementaux et les organes subordonnés, a institué le Comité *ad hoc* sur la protection des données (*CAHDATA*)[56]. Cet organe spécialisé est né avec la mission spécifique de présenter des propositions de modernisation du texte de la *Convention STE 108*. Ces propositions se sont enfin transformées dans le protocole d'amendement[57] adopté en mai 2018 et qui constitue la *Convention STE 108+*.

Le protocole d'amendement répond aux

> objectifs de l'exercice de modernisation, à savoir renforcer la protection des personnes au regard de l'évolution technologique en la matière, notamment de mieux maîtriser l'utilisation faite de leurs données personnelles[58].

« Un autre aspect fondamental de la modernisation est de rendre à la Convention sa crédibilité pleine et entière [...] »[59]. Une attention particulière a été posée sur les mécanismes de vérification de la capacité de chaque candidat à l'adhésion de satisfaire aux conditions requises et sur les États parties afin qu'ils continuent d'honorer leurs engagements[60]. Un autre point crucial a été

> d'assurer la cohérence et la compatibilité avec le cadre juridique de l'Union européenne et finalement de réaffirmer et de promouvoir la vocation universelle et le caractère ouvert de la Convention[61].

Ce dynamisme montre que la protection offerte par l'article 8 est en évolution continue. Aussi, dans la jurisprudence de la *CEDH*, on peut trouver plusieurs exemples de l'élargissement progressif du champ d'application de l'article 8. Par exemple, dans l'*affaire Amann c. Suisse*[62], les autorités avaient intercepté un appel téléphonique effectué par une femme de l'ambassade à Berne, alors Soviétique, pour commander au requérant un appareil dépilatoire. Bien que l'interception concernât un appel téléphonique professionnel, la Cour

> a considéré que la sauvegarde des données relatives à cet appel touchait à la vie privée du requérant. Elle a souligné que le terme « vie privée » ne devait pas être interprété de façon restrictive, en particulier dans la mesure où le respect de la vie privée englobe le droit pour l'individu de nouer et de développer des relations avec ses semblables. De surcroît, aucune raison

---

54 *Statut du Conseil de l'Europe*, 5 mai 1949, STE 001 (entrée en vigueur : 3 août 1949).

55 Conseil de l'Europe, Comité des ministres, *Résolution CM/RES (2011)24 concernant les comités intergouvernementaux et les organes subordonnés, leur mandat et leurs méthodes de travail*, 1125e réunion des Délégués des ministres (2011).

56 Pour le mandat et autre information, voir le site web de la protection des données du Conseil de l'Europe, en ligne : *COE* <www.coe.int/t/dghl/standardsetting/dataprotection/Cahdata_fr.asp>.

57 *Protocole d'amendement*, *supra* note 11.

58 Walter, *supra* note 14 à la p 11.

59 *Ibid* à la p 4.

60 *Ibid*.

61 *Ibid*; il est opportun de rappeler que la *Convention STE 108+* est maintenant ouverte à la signature des organisations internationales (article 27), sous l'exemple de l'UE (article 26).

62 *Amann c Suisse*, *supra* note 18.

> de principe ne permettait d'exclure les activités professionnelles ou commerciales de la notion de « vie privée »[63].

2. LES NOUVELLES GARANTIES NORMATIVES SOUS L'INFLUENCE DE LA JURISPRUDENCE DE LA COUR

La présente section est destinée à mettre en relief les garanties qui ont été affirmées grâce à la *Convention STE 108* et aux avancées contenues dans le *Protocole* d'amendement à la *Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel*, adopté par le Comité des ministres, le 18 mai 2018 (*Convention STE 108+*).

En ce qui concerne les éléments novateurs, la *Convention STE 108+* – déjà dans sa version originelle – introduit des éléments qui permettent un exercice plein et effectif du droit à la protection des données à caractère personnel face à l'utilisation de la part de l'autorité publique ou des instances privées. Entre la version originelle et le protocole d'amendement qui est actuellement à l'étape de ratification, on peut remarquer plusieurs différences. Il s'en suivra une synthèse des avancées les plus importantes sur le plan des garanties.

Parmi les personnes concernées, l'une des figures clé est le « maître du fichier », qui maintenant devient le « responsable du traitement » :

> la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui, seul ou conjointement avec d'autres, dispose du pouvoir de décision à l'égard du traitement de données[64].

L'article 6 prescrit pour le responsable du traitement des garanties spécifiques à respecter lorsqu'il s'agit de données « particulières » (syndicales, génétiques, concernent infractions pénales, l'origine raciale, l'orientation sexuelle, les opinions politiques, etc.).

Le nouvel article 8, intitulé « Transparence du traitement », prévoit que chaque État contractant prévoit rendre disponibles les informations sur l'identité, la résidence du responsable du traitement, la typologie de données traitée et que les moyens de recourir contre sa décision sont dédiés au dit responsable. Il peut ainsi travailler tout seul ou en collaboration avec un « sous-traitant », comme il peut y avoir ou pas un destinataire, à savoir la personne physique ou morale, l'autorité publique, le service, l'agence, à qui les données sont accessibles ou transmises. À ce sujet, la *Convention STE 108+* lui assigne des tâches particulières et des responsabilités spécifiques. L'article 5, complètement renouvelé, dans son paragraphe 2 prévoit notamment que « le traitement de données ne peut être effectué que sur la base du consentement libre, spécifique, éclairé et non équivoque de la personne concernée ».

---

63 Manuel de droit, *supra* note 9 à la p 40.

64 Conseil de l'Europe, Comité des ministres, *Convention modernisée pour la protection des personnes à l'égard du traitement des données à caractère personnel,* art 2 al 1 para b [*Convention STE 108+*].

Le texte ne prévoit pas une définition du terme « consentement », mais une lecture systémique des différents articles permet de comprendre très bien que les clés pour une interprétation adaptée sont la clarté, la transparence et son caractère non équivoque. Ces éléments doivent caractériser les informations concernant le processus de traitement afin que la personne concernée puisse correctement fournir son consentement.

La nouvelle *Convention STE 108+* amendée prévoit enfin une « Autorité » indépendante, nationale, chargée de veiller au respect de ses dispositions, avec le « pouvoir d'ester en justice ou de porter à la connaissance de l'autorité judiciaire compétente des violations des dispositions de la présente *Convention* »[65], et renforce aussi les pouvoirs du « Comité conventionnel » qui n'a plus seulement un rôle « consultatif », mais se voit également conférer des pouvoirs d'évaluation et de surveillance[66].

Afin de revenir aux origines de ces propositions, nous allons maintenant poser notre regard sur les principes dégagés par la jurisprudence de la *CEDH*. Dans l'*affaire Turek c. Slovaquie*[67] du 14 février 2006, le requérant dénonçait à la fois le fait que l'ancien service de sécurité de l'ex-Tchécoslovaquie communiste conservait un dossier dans lequel il était inscrit sur la liste des agents de ce service, et le refus des autorités de lui délivrer un « certificat de sécurité » indispensable pour son avancement de carrière. M. Turek a à plusieurs reprises essayé d'avoir accès à son propre dossier afin de faire rectifier les informations sur son compte, car elles étaient infondées, à son avis. Le juge slovaque, en revanche, avait considéré que la charge de la preuve du fait que l'ingérence litigieuse était contraire aux règles applicables à l'époque revenait au requérant, sans tenir en compte que ces informations étaient secrètes et donc inaccessibles à tous hormis aux autorités étatiques, c'est-à-dire le *Slovenská informačná služba* (SIS), soit le service de renseignements du gouvernement slovaque.

La Cour a donc estimé que « pareille exigence lui imposait [au requérant] en pratique une charge irréaliste, et était contraire au principe d'égalité. [...] elle était excessive. » Il y a donc eu violation de l'article 8 à raison de « l'absence d'une procédure par laquelle le requérant aurait pu obtenir la protection effective de son droit au respect de sa vie privée [...] »[68].

L'article 8 de la *Convention STE 108*, en vigueur à l'époque[69], dédié aux « garanties complémentaires pour la personne concernée » prévoyait déjà la possibilité de « connaitre l'existence d'un fichier »[70] contenant des données personnelles à son

---

65 *Ibid*, art 12(2)d); voir également *Convention STE 108+*, *supra* note 64, art 15(2)d).

66 Selon l'article 23 de la *Convention STE 108+*, le Comité conventionnel formulera un avis sur le niveau de protection des données assuré par un État ou une organisation internationale préalablement à leur adhésion à la *Convention*; Il peut aussi évaluer si le droit interne de la Partie concernée est conforme aux dispositions de la *Convention* et déterminer si les mesures prises ont été suivies d'effet (existence d'une autorité de contrôle, responsabilités, existence de voies de recours en vigueur).

67 *Turek c Slovaquie*, nº 57986/00, [2006] II CEDH 69.

68 *Ibid* au para 116.

69 *Convention STE 108*, *supra* note 11; aujourd'hui substitué par l'article 9 de la *Convention STE 108+*; *Convention STE 108+*, *supra* note 64.

70 *Convention STE 108*, *supra* note 11, art 8 a).

nom et de demander « sans délai ou frais excessifs la confirmation de l'existence »[71] du dossier. Le texte du *Protocole* de 2018[72] semble directement prendre inspiration de cet arrêt, car de nouveaux droits sont octroyés aux personnes concernées pour qu'elles puissent davantage contrôler leurs données à l'ère numérique. Selon l'article 9[73], en effet, la personne qui voit ses données traitées par une autorité publique, peut non seulement « obtenir, à sa demande, sans frais et sans délai excessifs, la rectification de ces données ou, le cas échéant, leur effacement »[74], mais aussi elle peut demander à prendre « connaissance du raisonnement qui sous-tend le traitement »[75]. À tout cela se rajoute une garantie très importante, dans le sens de la prise en compte de la personne à qui les données traitées appartiennent :

> Toute personne a le droit : a. de ne pas être soumise à une décision l'affectant de manière significative, qui serait prise uniquement sur le fondement d'un traitement automatisé de données, sans que son point de vue soit pris en compte[76].

L'analyse combinée des normes internationales et de l'action de la Cour européenne des droits de l'homme confirme donc le dynamisme et la vocation novatrice de sa jurisprudence en matière de protection des données à caractère personnel.

B. Le rôle de la jurisprudence de la Cour dans l'encadrement des pouvoirs de l'autorité publique sur le traitement de données à caractère personnel

Dans l'*affaire Turek c. Slovaquie*[77], le juge de Strasbourg souligne aussi un autre aspect très important pour comprendre l'étendu de la protection offerte par l'article 8 face à l'utilisation par l'autorité publique des données à caractère personnel. Le fait que le requérant n'ait pas pu accéder à son dossier et donc rectifier les fausses informations ne relève pas de sa responsabilité, lorsque l'État n'a pas adopté toutes les mesures pour un exercice effectif du droit à la protection des données, y compris le respect des garanties déjà énumérées, prévues dans la *Convention STE 108*[78]. En effet, en cas de traitement présumé illicite de données à caractère personnel par une autorité publique, le contrôle de la *CEDH* se concentre en trois phases différentes. Tout d'abord, il faut vérifier que la requête tombe dans le champ des droits protégés par l'article 8§1[79]. Ensuite il faut vérifier si l'État assume une obligation positive concernant les droits garantis, et enfin, s'assurer qu'il s'en est acquitté.

---

71 *Ibid* art 8 b).
72 *Convention STE 108+*, *supra* note 11.
73 *Ibid*.
74 *Ibid*, art 9 au para 1e).
75 *Ibid*, art 9 au para 1c).
76 *Ibid*, art 9 au para 1a).
77 *Turek c Slovaquie*, s*upra* note 67.
78 *Ibid* au para 116.
79 Les problématiques concernant cette phase ont été brièvement traitées dans les passages précédents, notamment quant à la place du droit à la protection des données dans le champ d'application de l'article 8§1.

En effet, du point de vue méthodologique, il semble opportun de soutenir la thèse qui encadre la vérification des obligations positives dans le contrôle primaire fait par le juge sur le droit de l'article 8§1[80]. Tout au long de la prochaine section, nous allons démontrer comment cette partie de l'analyse rentre dans la notion de « respect »[81] du droit garanti par la norme. Le troisième passage concerne l'évaluation de l'ingérence de l'État dans la sphère du droit à la protection des données à caractère personnel. Il faudra alors vérifier si elle a eu lieu, et le cas échéant, si elle est prévue par la loi, justifiée par un but légitime ou si elle est nécessaire dans une société démocratique. Encore une fois le parallèle avec la jurisprudence sera crucial pour la compréhension des enjeux de la question. Nous commencerons premièrement par traiter des obligations positives.

1. LES OBLIGATIONS POSITIVES DE L'ÉTAT POUR UNE PROTECTION EFFECTIVE DES DONNÉES PERSONNELLES

> Si l'objet essentiel de l'article 8 est de « prémunir l'individu contre des ingérences arbitraires des pouvoirs publics », la Cour estime que cette disposition peut engendrer, de surcroît, des obligations positives inhérentes à un respect effectif des valeurs qu'elle protège. Ainsi, de même qu'il a l'obligation négative de s'abstenir d'interférer arbitrairement dans la vie familiale et privée, [...], l'État peut également être amené à agir concrètement pour assurer le respect de toute une série d'intérêts personnels énoncés par cette disposition[82].

Ces obligations peuvent impliquer l'adoption par l'État de mesures visant au respect de la vie privée jusque dans les relations des individus entre eux, par exemple un internaute et les personnes donnant accès à un site internet particulier[83]. En d'autres termes, il pèse sur l'État une obligation positive de prendre des mesures visant à la prévention effective des actes portant gravement atteinte aux données concernant une personne, parfois par le biais de dispositions pénales efficaces[84].

> La base de cette interprétation de l'article 8 repose sur la référence au droit de l'individu au respect de sa vie privée et familiale etc., ce qui a permis aux juges de Strasbourg d'étendre les obligations de l'État au-delà de la simple non-ingérence[85].

---

80 Ursula Kilkelly, « Le droit au respect de la vie privée et familiale : un guide sur la mise œuvre de l'article 8 de la *Convention européenne des Droits de l'Homme* » dans *Précis sur les droits de l'homme*, Strasbourg, Allemagne, 2003 à la p 8.

81 Colombine Madeleine, « La technique des obligations positives en droit de la Convention européenne des droits de l'homme », thèse de droit de la *Convention européenne des droits de l'homme,* vol 133, Paris, Dalloz, 2014 à la p 29.

82 Kilkelly, *supra* note 80 à la p 21.

83 *X et Y c Pays-Bas* (1985), 91 CEDH (Sér A) aux para 23–24 et 27.

84 *Ibid*; *August c Royaume-Uni*, nº 36505/02, (21 janvier 2003); *MC c Bulgarie*, nº39272/98, [2003] XII CEDH 45 au para 150.

85 Kilkelly, supra note 80 à la p 21.

Afin que le respect soit plein, l'État doit remplir les obligations qui permettent un exercice effectif du droit protégé par l'article 8. Dans l'*arrêt X et Y c. Pays-Bas*[86] concernant une requête dirigée contre le Royaume des Pays-Bas, un père se plaint du fait que la législation néerlandaise n'avait pas permis une protection adéquate contre les abus sexuels commis par un agresseur sur sa fille Y. Elle, une personne handicapée mentale, âgée de seize ans à l'époque des faits, n'avait pas pu saisir les tribunaux, car mineure de dix-huit ans. Les requérants ont donc allégué la violation de l'article 8 de la *Convention STE 108*, dénonçant un manquement de la part de l'autorité publique. En l'espèce la *Cour* a ainsi déclaré :

> [L'article 8] ne se contente pas de commander à l'État de s'abstenir de pareilles ingérences : à cet engagement plutôt négatif s'ajouter des obligations positives inhérentes à un respect effectif de la vie privée ou familiale [...]. Elles peuvent impliquer l'adoption de mesures visant au respect de la vie privée jusque dans les relations des individus entre eux[87].

Avec l'*arrêt X et Y c. Pays-Bas*, la *Cour* bouscule pour la première fois la conviction traditionnelle selon laquelle la *CEDH* ne prévoit que des obligations négatives, car le passage précité équivaut à dire que dans certaines circonstances, la *Convention* exige de l'État qu'il prenne des mesures actives pour permettre aux individus d'exercer les droits qui leur sont conférés par l'article 8[88]. Empruntant les mots de Frédéric Sudre l'on pourrait affirmer que, grâce aux obligations positives, il est possible de « dépasser l'ancien clivage artificiel » entre « obligation de » et « obligation à »[89]. La CourEDH dans sa jurisprudence a souvent eu recours aux obligations positives[90], pour pousser les États à adopter des mesures de droit substantiel, par exemple dans le domaine pénal, mais aussi pour inciter les parlements à changer ou rajouter des normes sur le plan procédural. L'un des meilleurs exemples jurisprudentiels de la CourEDH à ce sujet est l'*affaire Gaskin c. Royaume-Uni*[91]. Il s'agit d'un jeune délinquant qui prétendait surmonter ses difficultés grâce à une meilleure connaissance de son passé tumultueux. Comme la municipalité de Liverpool avait interdit l'accès au contenu des dossiers dument conservés dans ses archives, il choisit de saisir le Juge de Strasbourg pour se plaindre d'une violation du droit au respect de sa vie privée. En l'espèce la Cour, après avoir estimé que l'accès à des informations concernant l'enfance et les années de formation relève de la « vie privée et familiale », a explicitement affirmé que l'obligation positive de permettre à l'individu l'accès aux dossiers le concernant pesait sur l'État[92]. En l'occurrence, la violation de l'article 8, vérifiée par la CourEDH, ne concernait pas une ingérence *strictu sensu* de l'autorité publique dans le droit du requérant, il s'agissait plutôt d'un défaut,

---

86 *X et Y c Pays-Bas*, *supra* note 83.

87 *Ibid* au para 23.

88 Kilkelly, *supra* note 80 à la p 22 : « Cette obligation positive peut parfois inclure la protection des intéressés contre les actions d'autres particuliers les privant de la jouissance effective de leurs droits. »

89 Sudre, « Droit européen », *supra* note 9 à la p 252.

90 *Ibid* à la p 257 : « *Guincho c./Portugal*, 10 juillet 1984, droit à un procès équitable *Mathieu-Mohin et Clerfaty c./Belgique*, 2 mars 1987, A. 113, §50, droit à des élections libres; *Gustaffson c./Suede*, 26 avril 1997, droit à la liberté syndicale Fuentes Bobo c./ Espagne 29 février 200, droit de propriété, etc. ».

91 *Gaskin c Royaume-Uni*, *supra* note 18.

92 *Ibid* aux para 36, 37, 41, 47 et 49.

dans le système britannique, de constituer des organes indépendants chargés de prendre la décision finale sur l'accès.

La décision *Gaskin* a aussi permis à la Cour d'affirmer dix ans plus tard l'importance de l'accès aux données médicales. Dans l'*arrêt McGinley et Egan c. Royaume-Uni*[93] du 9 juin 1998, relatif à la santé des militaires ayant participé à des essais nucléaires, le juge de Strasbourg a clairement affirmé que l'accès à des données médicales pressentait un lien suffisamment étroit avec leur vie privée pour dénoncer une violation de l'article 8.

En effet, la distinction entre obligations positives procédurales et substantielles[94] est déjà connue en doctrine, de même que l'objection concernant la légitimité pour un juge de s'octroyer le pouvoir de créer des normes dans un système romano-germanique comme ceux de la plupart des États européens. Dans le cas de juridictions nationales, ce problème n'est pas facile à résoudre, toutefois dans le cas de la CourEDH plusieurs facteurs peuvent contribuer à légitimer une pratique de la sorte.

La signature même d'une convention internationale pour la sauvegarde de droits fondamentaux par volonté expresse des États et l'institution conséquente d'un juge chargé de la mettre en pratique, sanctionnant toute action des États divergeant du modèle démocratique et libéral, confère au juge de Strasbourg une légitimité fondatrice et le place comme « gardien des valeurs démocratiques et de la paix en Europe »[95]. Ainsi, comme l'affirme Colombine Madeleine[96] dans sa brillante thèse de doctorat, récemment soutenue à Paris : « la technique juridique des obligations positives est un outil d'adaptation de la norme juridique conventionnelle à l'évolution des États démocratiques et libéraux européens ». Ce que renforce la conviction à l'égard du dynamisme de la Cour. « Il est difficile d'identifier les circonstances dans lesquelles le respect de l'article 8 [de la *Convention européenne des droits de l'homme*] impose une action positive »[97] de la part de l'État. En ce sens, les autorités nationales bénéficient d'une large marge d'appréciation[98].

> Selon les Juges de Strasbourg, l'État, afin de déterminer l'éventuelle existence d'une obligation positive, doit se demander si un juste équilibre a pu être établi entre l'intérêt général de la collectivité et les intérêts de l'individu[99].

---

93 *McGinley et Egan c Royaume-Uni* (1998), III CEDH.

94 Françoise Tulkens, « Le droit à la vie et le champ des obligations des États dans la jurisprudence récente de la Cour européenne des droits de l'homme » dans *Libertés, justice, tolérance. Mélanges en* hommage *du* D*oyen Gérard Cohen-Jonathan*, Bruxelles, Bruylant, 2004 à la p 1626; Sudre, « Droit européen », *supra* note 9 à la p 258; Madeleine, *supra* note 81 à la p 61.

95 Madeleine, *ibid*.

96 *Ibid*.

97 Kilkelly, *supra* note 80 à la p 21.

98 *Ibid*.

99 Kilkelly, *supra* note 80 à la p 21; voir par exemple *Gaskin c Royaume-Uni*, supra note 18; à la lecture de cet arrêt est possible de constater que souvent, le choix de la *CourEDH* entre l'adoption de l'approche reposant sur des obligations positives et l'analyse ordinaire de l'instance à l'aune de l'article 8§2 ressorts dans l'exposé des motifs, mais pas dans les conclusions.

2. LES EFFORTS DE LA COUR POUR UN ÉQUILIBRE ENTRE PROTECTION DE L'INTÉRÊT DE L'INDIVIDU ET DÉFENSE DES INTÉRÊTS DE LA COLLECTIVITÉ

Pourrait-on affirmer qu'il existe une décision judiciaire dépourvue de la recherche de proportionnalité entre l'intérêt individuel et celles de la collectivité? La vie en société requiert toujours une mise en balance de ces différentes instances. Cette recherche d'équilibre est aussi au cœur de l'action de la CourEDH lorsqu'il s'agit d'identifier une ingérence dans le droit à la protection de données personnel. La deuxième partie de l'article 8[100] prévoit une liste fermée de limites à la protection du droit à la vie privée et familiale, au domicile et à la correspondance. Une fois l'ingérence vérifiée, la Cour procède à l'analyse de trois facteurs distincts afin d'appliquer l'exception au cas concret. Le premier est un critère de légalité, il faut donc se demander si l'ingérence est prévue par la loi. « Si la mesure contestée ne remplit pas ce critère de légalité, elle est assimilée à une violation sans qu'il soit nécessaire d'examiner davantage l'affaire au fond »[101]. Dans l'*affaire Malone c. Royaume-Uni*[102], concernant l'interception des conversations téléphoniques, la Cour a eu l'occasion de préciser la portée de l'expression « prévue par la loi ». En l'espèce

> [l]es Juges de Strasbourg déclarèrent que le droit applicable n'indiquait pas avec assez de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans le domaine considéré : l'écoute secrète des conversations téléphoniques reposant sur une pratique administrative, ses modalités pouvaient être modifiées à tout moment et elle constituait par conséquent une violation de l'article 8[103].

Dans les années quatre-vingt-dix, dans l'*affaire Kahn c. Royaume-Uni*[104], toujours concernant des écoutes téléphoniques, la Cour est allée encore plus loin quant à l'importance des modalités d'utilisation du matériel recueilli. Se référant à sa jurisprudence précédente, elle a souligné l'importance de la prévisibilité comme composante indissoluble du principe de légalité :

> Les mots « prévues par la loi » [...] exigent l'accessibilité de celle-ci aux personnes concernées et une formulation assez précise pour leur permettre – en s'entourant, au besoin, de conseils éclairés – de prévoir, à un degré raisonnable dans les circonstances de la cause, les conséquences pouvant résulter d'un acte déterminé[105].

« Dès lors qu'il est établi qu'une ingérence est prévue par la loi, la Cour poursuit son examen en se demandant si elle poursuit un but légitime au sens de

---

100 *Convention STE 108+*, *supra* note 11.

101 Kilkelly, *supra* note 80 à la p 25; voir aussi Ivana Roagna, *La protection du droit au respect de la vie privée et familiale par la Convention européenne des droits de l'homme,* 1ère éd dans *Série des précis sur les droits de l'homme du Conseil de l'Europe,* Strasbourg, Conseil de l'Europe, 2012 à la p 39.

102 *Malone c Royaume-Uni*, *supra* note 18.

103 Kilkelly, *supra note* 80 à la p 26.

104 *Kahn c Royaume-Uni*, n°35394/97, [2000] V CEDH 303.

105 *Margareta et Roger Andersson c Suède* (1992), 226 CEDH (Sér A) au para 75.

l'article 8(2) »[106]. La norme laisse aux États une large marge d'appréciation. Ainsi, le fichage ou l'interception de communication et correspondance à caractère personnel peuvent rentrer dans la « nécessité » de défendre la « sécurité nationale » ou « l'ordre » et « la prévention des infractions pénales »; « le retrait d'enfants d'un foyer violent ou le refus d'accorder la garde »[107] peuvent se justifier par la « protection de la santé ou de la morale » ou « des droits et libertés d'autrui »[108]; ou encore l'expulsion ou la déportation d'une personne peut être « nécessaire au bien-être économique du pays »[109].

> Ainsi, dans la plupart des affaires, la Cour accepte l'idée que l'État agissait dans un but licite et rejette rarement le ou les buts légitimes identifiés, même lorsqu'ils sont contestés par le requérant[110].

« La phase finale de l'examen [de la Cour] porte sur la détermination du caractère "nécessaire" de l'ingérence dans une "société démocratique" »[111]. D'après les juges dans l'*affaire Dudgeon c Royaume-Uni*[112], « la *Convention* est conçue pour sauvegarder et promouvoir les idéaux et valeurs d'une société démocratique »[113]. En ce sens, dans l'*arrêt Olsson c. Suède,* elle affirme que : « la notion de nécessité implique une ingérence fondée sur un besoin social impérieux et notamment proportionné au but légitime recherché [...] »[114].

À la suite des déclarations et aux arrêts jusqu'ici cités, l'on remarque que le centre de l'action de la Cour a toujours été la recherche de l'équilibre qui permette d'apprécier l'exercice des droits d'un individu par rapport à l'intérêt public plus large. En ce sens, déjà en 1989, dans l'ancienne affaire *Soering c. Royaume-Uni,* le juge de Strasbourg écrivait :

> [...] le souci d'assurer un juste équilibre entre les exigences de l'intérêt général de la communauté et les impératifs de la sauvegarde des droits fondamentaux de l'individu est inhérent à l'ensemble de la Convention[115].

Ce grand effort, qui représente un phare pour toute application de droits fondamentaux, devient d'importance capitale lorsqu'on parle d'utilisation de données personnelles par l'autorité publique.

---

106 Kilkelly, *supra* note 80 à la p 30.
107 *Ibid* à la p 31.
108 *Ibid*.
109 *Ibid*.
110 *Ibid*.
111 *Ibid*.
112 *Dudgeon c Royaume-Uni* (1981), 45 CEDH (Sér A).
113 Kilkelly, *supra* note 80 à la p 32.
114 *Olsson c Suède* (1988), 130 CEDH (Sér A) au para 67; Kilkelly, *ibid* à la p 31 : Déjà dans l'arrêt *Handyside c Royaume-Uni* (1976), 24 CEDH (Sér A), la *Cour* avait donné une première définition du terme « nécessaire », précisant que « n'est pas synonyme d'indispensable, mais n'a pas non plus la souplesse de termes tels qu'"admissible", "normal", "utile", "raisonnable", ou "opportun" ».
115 *Soering c Royaume-Uni* (1989), 161 CEDH (Sér A) au para 89.

II. L'utilisation par les autorités publiques des données à caractère personnel et les limites de l'action de la CourEDH face aux nouveaux défis de la surveillance massive

Dans l'ensemble des affaires liées à la protection des données pour lesquels le juge de Strasbourg est saisi, un grand nombre de cas concernent les secteurs des enquêtes judiciaires en matière pénale et des interceptions de communications dans le cadre des opérations secrètes de surveillance massive. Bien que les moyens employés dans les deux cas soient presque les mêmes (interception d'appels téléphoniques et communications électroniques, fichage, etc.) la grande différence est dans la « base légale », plus précisément, dans le fait que ces opérations soient ou pas « prévues par la loi ». Autre élément de distinction est la dimension territoriale, car d'habitude, les enquêtes de police se déroulent, de surcroit, sur le territoire national, lorsque les activités de surveillance impliquent la collaboration d'acteurs internationaux. Dans cette deuxième partie nous verrons quelle protection assure la CourEDH en force de l'article 8 de la *Convention européenne des droits de l'homme*, mais aussi quelles sont les limites trahies par les affaires plus récentes et dans quelle mesure ces arrêts vont dans la direction de renforcer les relations de confiance mutuelle entre États parties.

A. La protection des données personnelles dans le cadre des enquêtes policières et de la justice pénale : une protection « classique » jusqu'ici très efficace

Si c'est vrai que « l'efficacité d'un système de protection des droits de la personne s'évalue par le traitement qu'il réserve aux prisonniers et aux étrangers »[116], il devrait en principe y avoir encore plus de soins pour les personnes qui font l'objet d'une enquête. Voici l'une des raisons pour lesquelles le respect du droit à la protection des données personnelles dans le cadre des enquêtes de police occupe une place de choix dans cette étude. L'attention de la Cour pour la modalité de traitement des données et la prévention du risque de stigmatisation est toujours présente :

> Enfin, il appartient à la Cour d'être particulièrement attentive au risque de stigmatisation de personnes qui, à l'instar du requérant, n'ont été reconnues coupables d'aucune infraction et sont en droit de bénéficier de la présomption d'innocence. Si, de ce point de vue, la conservation de données privées n'équivaut pas à l'expression des soupçons, encore faut-il que les conditions de cette conservation ne leur donnent pas l'impression de ne pas être considérés comme innocents[117].

---

[116] Olivier Delas, « Le renvoi des étrangers vers un risque de mauvais traitement : l'arrêt N. c. Royaume-Uni ou la Cour européenne des droits de l'homme en terrain glissant? » dans Olivier Delas et Michaela Leuprecht, dir, *Liber Amicorum Peter Leuprecht.* Bruxelles, Bruylant, 2012 à la p 321; l'auteur en ce passage reporte une conversation privée avec l'ancien Représentant spécial du Secrétaire général des Nations Unies pour les droits de l'Homme au Cambodge, professeur et ami, Peter Leuprecht.

[117] *Brunet c France*, n°21010/10 (18 septembre 2014) au para 37; *S et Marper c Royaume-Uni*, *supra* note 19 au para 122; *MK c France*, n°19522/09 (18 avril 2013) au para 36.

Le passage cité se trouve au point 37 de l'*arrêt Brunet c France*[118] et c'est l'une des plus claires affirmations de ce principe de la part de la Cour. Le cas en question concerne une vive altercation d'un couple dont la conjointe dépose une plainte auprès du procureur compétent, ce qui justifie le placement en garde à vue de son compagnon. Le jour suivant, les deux se réconcilient et écrivent au procureur pour retirer les plaintes réciproques. Ladite procédure fut ainsi placée sans suite. Après quelques mois, l'homme demanda que soient effacées ses données personnelles collectées dans le système de traitement des infractions constatées (STIC)[119], mais la réponse des autorités fut négative et puisque son dossier avait été classé sans suite, il était dans l'impossibilité de présenter un recours contre cette décision.

Avant de dévoiler ce que la Cour a décidé, ouvrons une petite parenthèse sur le contexte normatif. En matière pénale, aux dispositions de la *Convention STE 108* – en vigueur à l'époque –, se rajoutent celles d'une importante recommandation (*R87*)[120], qui spécifie la façon dont les autorités de police doivent donner effet aux principes dans le contexte du traitement de données à caractère personnel. La recommandation ne prévoit pas de collecte ouverte et aveugle de données par les autorités de police. Elle limite la collecte de données à caractère personnel par les autorités de police aux données nécessaires pour la prévention d'un réel danger ou la suppression d'une infraction pénale spécifique.

La CourEDH a systématiquement reconnu que l'enregistrement et la conservation de données à caractère personnel par des autorités de police ou de sécurité nationale constituaient une atteinte à l'article 8(1) de la *CEDH*. De nombreux arrêts de la CourEDH portent sur la justification de telles atteintes[121]. Par exemple dans l'*affaire Vetter c. France*[122], la police judiciaire, qui soupçonnait une personne d'homicide, mis sous écoute l'appartement d'une personne chez qui celui-ci se rendait régulièrement. Le requérant prétendait inutilisables les écoutes, d'ailleurs déterminantes pour son arrestation, car recueillie en violation de l'article 8. En effet, dans le cas d'espèce, la Cour conclut à la violation de la *Convention*, car la loi française n'était pas suffisamment claire quant à la pose de micros et aux modalités d'exercice du pouvoir d'appréciation des autorités[123].

Revenons maintenant à l'*affaire Brunet c. France*. L'importance de cette affaire qui aboutit à une vérification d'infraction de l'article 8 par les autorités françaises, relève de deux aspects. Dans un premier temps, la Cour fait une précision importante :

> [...] si les informations répertoriées au STIC ne comportent ni les empreintes digitales […] ni le profil ADN des personnes, elles présentent néanmoins un caractère intrusif non négligeable, en ce qu'elles font apparaître des éléments

---

118 *Brunet c France*, *ibid.*

119 *Ibid* au para 7.

120 Conseil de l'Europe, Comité des ministres, *Recommandation R (87) 15 du Comité des ministres aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police*, (1987).

121 Voir par ex *Leander c Suède*, *supra* note 18; *MM c Royaume-Uni*, n°24029/07 (13 novembre 2012); *MK c France*, *supra* note 117.

122 *Vetter c France*, n°59842/00 (31 mai 2005).

123 *Ibid* au para 28; voir aussi *PG et JH c Royaume Uni*, n°44787/98, [2001] IX CEDH 233, concernant l'utilisation par la police d'un dispositif d'écoute caché dans l'appartement d'un des requérants, qui n'était pas prévu par la loi.

> détaillés d'identité et de personnalité en lien avec des infractions constatées, dans un fichier destiné à la recherche des infractions[124].

Successivement, elle balaye les classifications françaises (non-lieu à procéder, sans suite, etc.) rapportant tout à la nette distinction entre condamné et innocent[125]. Pour toute personne innocente il n'y a donc aucune raison « légitime » ou « nécessaire dans une société démocratique » pour collecter et garder des données à caractère personnel[126].

Toujours sous l'angle de la nécessité des mesures dans une société démocratique et de la légitimité des ingérences prévues par la loi, la *CourEDH* a opéré une distinction encore plus poussée entre les typologies d'ingérence possibles selon l'article 8 de la *Convention européenne des droits de l'homme*. Dans l'*affaire Ben Faiza c. France*[127] du 8 février 2018, le juge de Strasbourg a montré à quel point la « base légale »[128] destinée à justifier les hypothèses de géolocalisation en temps réel d'un suspect était trop générique et n'offrait pas les conditions de « prévisibilité » nécessaire pour offrir le degré minimal de protection voulu par l'article 8[129]. Il a pourtant conclu à une violation de l'article 8, en prenant toutefois acte que la France en 2014 s'était dotée d'une loi beaucoup plus précise et conforme aux prescriptions de l'article 8[130]. La Cour a jugé, d'autre part, que la réquisition judiciaire adressée à l'opérateur téléphonique constituait une ingérence dans la vie privée de M. Ben Faiza, mais que celle-ci était prévue par la loi et qu'elle poursuivait un but légitime (la défense de l'ordre, la prévention des infractions pénales, etc.). La Cour estime aussi que cette mesure était nécessaire dans une société démocratique, car elle visait à démanteler un trafic de stupéfiants de grande ampleur[131].

Cette distinction opérée par la *Cour* montre l'importance d'encadrer les ingérences selon les critères de l'article 8 et produit un impact sur « plusieurs affaires relatives à la captation massive de données et à des systèmes de surveillance d'une ampleur inégalée »[132]. Elle confirme et spécifie encore plus en détail la protection « classique » offerte par la *Convention européenne des droits de l'homme* en matière de protection de données à caractère personnel. Dans la partie subséquente, nous nous pencherons sur l'efficacité de cette action de la Cour face à la surveillance de masse.

---

124 *Brunet c France*, *supra* note 117 au para 39.

125 *Ibid* aux para 40-41.

126 Même typologie de discours pour les infractions commises via internet, réglées par la *Convention sur la cybercriminalité*, *supra* note 50; cette convention est ouverte à l'adhésion de pays non-membres du Conseil de l'Europe et, mi-2013, quatre États hors Conseil de l'Europe (l'Australie, la République dominicaine, le Japon et les États-Unis) étaient partis à la *Convention* et 12 autres non-membres l'avaient signée ou avaient été invités à y adhérer.

127 *Ben Faiza c France*, n°31446/12 (8 février 2018).

128 Art 81 C proc pén; la Cour avait d'ailleurs déjà jugé, dans le cadre d'affaires relatives à des écoutes téléphoniques, que l'article 81 du *CPP*, même lu en combinaison avec d'autres dispositions du *CPP*, n'offrait pas la « prévisibilité » exigée par l'article 8 de la *Convention*.

129 *Ben Faiza c France*, *supra* note 127 aux para 58–60.

130 *Ibid* aux para 41 et 61.

131 *Ibid* aux para 77-80.

132 Nicolas Hervieu, « Le fichage policier sous les fourches caudines européennes : Droit au respect de la vie privée (Art. 8 CEDH) » dans *La Revue des droits de l'homme*, au para 50, en ligne : *OPJ* <journals.openedition.org/revdh/879>.

B. La surveillance massive à l'épreuve de l'*affaire Big Brother Watch c Royaume-Uni* du 4 septembre 2013 : *Stress test* pour la *CEDH*

Que ce soit un nouveau modèle de voiture, une centrale nucléaire de dernière génération, ou un avion, souvent nous entendons parler de « *stress test* ». Dans le système bancaire, il s'agit d'un

> exercice consistant à simuler des conditions économiques et financières extrêmes, mais plausibles afin d'en étudier les conséquences sur les banques et de mesurer leur capacité de résistance à de telles situations[133].

Personne n'a jamais avancé l'hypothèse d'en effectuer un sur un système international de protection des droits fondamentaux. Toutefois, le grand nombre d'affaires conclues et pendantes devant la CourEDH, ne sont pas une simulation, mais un vrai examen pour la tenue d'un système basé sur la *Convention européenne des droits de l'homme*. Les révélations faites par l'ancien analyste de l'agence de sécurité nationale des États-Unis (*NSA*), Edward Snowden, aux journalistes en juin 2013, ont démontré l'existence de pratiques de surveillance massive et d'intrusion à large échelle jusqu'ici inconnues du grand public et de la plupart des décideurs politiques.

Dans ce contexte, trois organismes non gouvernementaux[134] qui se battent pour la protection internationale de la liberté d'expression, et une experte de surveillance qui travaille à l'Université des Sciences appliquées de Berlin, ont saisi la CourEDH en dénonçant des violations de l'article 8 commises par les services de renseignement du Royaume-Uni. Dans l'*affaire Big Brother Watch et autres c. Royaume Uni*[135], les requérants allèguent avoir été l'objet d'une surveillance généralisée[136] par les services de renseignement anglais, qui avec une utilisation illicite des programmes *PRISM*[137] et *UPSTREAM*[138], mis en place par la *NSA*, auraient intercepté leurs appels téléphoniques et communications électroniques. Ils ont demandé à la Cour de juger si les ingérences dénoncées sont « prévues par la loi » et « nécessaires dans une société démocratique ».

Le travail de la Cour a été assez long et complexe vu l'importance des enjeux. Dans son analyse, elle a examiné la conventionnalité de trois types de surveillance : l'interception massive de communications; l'obtention de données de communications auprès de fournisseurs de télécommunications; et le partage de renseignements avec les services secrets étrangers.

---

133 « Stress test (test de résistance bancaire) » 25 juin 2019, en ligne : *La finance pour tous* <www.lafinancepourtous.com/decryptages/crises-economiques/mecanique-des-crises/stress-test-test-de-resistance-bancaire/>; pour une définition plus détaillée, voir : Banque centrale européenne, Comprehensive assessment stress test manual, Frankfurt, 2014.

134 *Big Brother Watch*, basé à Londres; *English Pen*, basé à Londres avec 145 centres affiliés en plus de 100 pays; et *Open Right Group*, basé à Londres.

135 *Big Brother Watch et autres c Royaume-Uni*, n°58170/13 (13 septembre 2018) [*Big Brother Watch c Royaume-Uni*].

136 Le terme utilisé dans la version officielle en anglais de la requête est « *generic surveillance* ».

137 Programme pour l'accès officiel à neuf sociétés internet, dont Google, Microsoft et Yahoo.

138 Programme pour l'interception de données directement à partir des câbles à fibre optique sous-marins câbles et des infrastructures de propriété des États-Unis : ce programme permet l'accès, la recherche et la collecte de données à caractère personnel grâce à l'utilisation de mots clés.

Pour ce faire, le juge de Strasbourg s'est aussi appuyé sur les principes dégagés par sa propre jurisprudence en la matière[139], en rappelant entre autres les critères minimaux qui doivent être établis par la loi afin d'éviter tout abus de pouvoir, mentionnés dans l'*arrêt Weber and Saravia*[140] :

> [...] [a)] la nature des infractions susceptibles de donner lieu à un mandat d'interception, [b)] la définition des catégories de personne susceptibles d'être mises sur écoute, [c)] la fixation d'une limite à la durée de l'exécution de la mesure, [d)] la procédure à suivre pour l'examen, [e] l'utilisation et la conservation des données recueillies, [f)] les précautions à prendre pour la communication des données à d'autres parties, et [g)] les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements[141].

L'objet de l'examen de compatibilité avec les exigences de la *Convention* était la *Loi RIP* ou *RIPA* (*Regulation of Investigatory Powers Act*, *2000*)[142] qui réglementait le système d'interception massive et le système d'obtention de données de communication auprès de fournisseurs de services de communication anglais depuis l'année 2000[143]. À cet égard, la Cour considère que l'utilisation d'un tel système d'interception massive n'emporte pas en lui-même violation de la *Convention*, mais observe néanmoins qu'un tel régime doit respecter les critères qui se trouvent énoncés dans sa jurisprudence. Cependant, les processus de sélection et de recherche, dans le système en cause, ne sont pas soumis à une surveillance indépendante adéquate et les critères de recherche utilisés pour filtrer et sélectionner les communications interceptées à examiner restent génériques[144]. En force de ces arguments, la Cour a conclu à une violation de l'article 8, et a aussi confirmé la violation du même article pour les griefs concernant l'obtention d'informations de la part des fournisseurs de services de communication, du fait qu'elle n'est pas « prévue par la loi ».

Si d'une part cet arrêt a une portée novatrice, en même temps il laisse derrière de grands vides. L'on pourrait presque dire que la plupart des attentes n'ont pas été respectées. Reconnaitre la législation anglaise insuffisante et le système de surveillance mis en place par les services de renseignement comme n'étant « pas prévu par la loi » est un passage important, mais définitivement pas suffisant. Il est assez étonnant de constater la position de la Cour envers un autre élément de l'affaire généré par les révélations de Snowden et dont la portée est peut-être encore plus grave. Il s'agit du partage de renseignement avec les services de renseignement de pays étrangers.

---

139 *Roman Zakharov c Russie* [GC], n°47143/06, [2015] VIII CEDH 309; *Mustafa Sezgin Tanrikulu c Turquie*, n°27473/06 (18 juillet 2017); *Amann c Suisse*, *supra* note 18; *Huvig c France* (1990), 176-B CEDH (Sér A); *Malone c Royaume-Uni*, *supra* note 18; *Leander c Suède*, *supra* note 18.

140 *Weber et Saravia c Allemagne*, n°54934/00, [2006] XI CEDH 351.

141 *Ibid* au para 95.

142 *Regulation of Investigatory Powers Act 2000* (R-U).

143 Entretemps, le Royaume-Uni s'est doté en 2016 d'une loi plus respectueuse des droits fondamentaux et conforme aux exigences imposées par l'article 8 de la Convention, cette dernière loi n'a pas été prise en compte par la Cour puisque à l'époque des faits elle n'était pas encore en vigueur.

144 *Big Brother Watch c Royaume-Uni*, *supra* note 135, notamment au para 493.

Dans l'analyse des limites à l'exercice du droit à la protection des données personnelles, prévues à l'article 8§2[145], nous avons approfondi les principes de « légitimité », « nécessité » ou « légalité », auxquels les États doivent s'attendre pour justifier leurs ingérences. Dans le cas d'espèce, le dossier Snowden montre que la *NSA* et ses partenaires étrangers, notamment au sein de l'alliance « *Five Eyes* » (États-Unis, Royaume-Uni, Canada, Australie et Nouvelle-Zélande), contournent les restrictions nationales en échangeant les données relatives aux ressortissants de leurs partenaires respectifs. Grâce aux programmes comme *PRISM*, *TEMPORA*[146], *PREFER*[147], et *UPSTREAM*, ces agences de renseignement arrivent à surveiller plus de 600 millions de conversations par jour et jusqu'à 5 milliards de métadonnées[148]. Il est impossible de vérifier ou tout simplement d'assumer que de telles ingérences soient motivées par des soupçons fiables sur chacune des personnes concernées, il s'agit plutôt de la collecte et de l'analyse indistincte de données à caractère personnel[149].

Or, ces opérations ont aussi été possibles grâce à la collaboration de plusieurs pays membres de la *CEDH*, notamment l'Allemagne, le Danemark, la France et la Norvège. Sur ce, malgré l'*arrêt Big Brother Watch* qui montre clairement, au paragraphe 423, que l'une des finalités du partage d'information entre services de renseignement de différents pays est de contourner les lois nationales plus rigides et les critères fixés par la *Convention*, la Cour conclus que le Royaume-Uni n'a pas violé l'article 8, ni l'article 10 par son dispositif de partage de renseignements avec des États étrangers.

Pourtant, l'Assemblée parlementaire du Conseil d'Europe, dans plusieurs rapports, s'était déjà montrée assez sensible sur la question et avait à tel propos parlé de « collusion visant à se soustraire aux restrictions », invitant ainsi le Comité des ministres à ouvrir une négociation pour l'adoption d'un « Code du renseignement », et à dresser une recommandation aux États membres pour la protection de la vie privée à l'ère du numérique. En effet, ces orientations ont été consacrées par la nouvelle *Convention STE 108+*, qui à son article 14 (flux transfrontières de données à caractère personnel) établit que chaque Partie ne doit pas s'opposer à produire une autorisation pour le transfert de données vers un autre État partie, il existe néanmoins une exception « lorsqu'il existe un risque réel et sérieux que le transfert à une autre Partie [...] conduise à contourner les dispositions de la *Convention* »[150].

---

145 *Convention européenne des droits de l'homme*, *supra* note 4; Voir la partie I-B-2, ci-dessus.

146 Programme pour la surveillance du réseau câblé de fibre optique transocéanique.

147 Programme pour la collecte des données des appels manqués et message texto (SMS).

148 Les métadonnées sont les informations complémentaires liées à toute communication électronique, notamment concernant la date, l'heure et la position exactes dont la communication est partie.

149 À tel propos Didier Bigo, professeur de sciences politique à Paris et expert de réputation internationale, durant la conférence « Sécurité, renseignement, surveillance et obéissance après Snowden » organisée par le Centre de Hautes Études internationales à l'Université Laval, le 8 octobre 2014 [non publié], soulignait comment après le 11 septembre 2001 la logique mondiale de la protection des données dans les opérations de renseignements a changé : « Avant les agences de renseignent observaient 10 % de la population pour protéger les 90 % qui restait, aujourd'hui grâce aux progrès technologiques elles sont capables de surveiller 90 % de la population mondiale pour détecter 10 % des terroristes et criminels ».

150 *Convention Ste 108+*, *supra* note 11, art 14(1).

L'un des enjeux majeurs dans l'*affaire Big Brother Watch* est que la Cour s'est retrouvée *de facto* à juger des violations faites par des États membres en « collusion » avec des États non-membres, au détriment du droit à la protection des données de citoyens européens. Cette dynamique, telle que montrée par les révélations de Snowden, a inévitablement généré un écroulement vertigineux de la confiance réciproque entre les membres du Conseil de l'Europe[151].

Dans ce sens, il est possible de parler de « limites » à l'action de la CourEDH, dans la mesure où ces récents arrêts n'ont pas (ou n'ont plus) la force de restaurer une confiance brisée au sein du Conseil de l'Europe, dû à la dimension transnationale des phénomènes de surveillance de masse.

Dans un autre cadre, si l'on considère l'évolution globale de la jurisprudence européenne (au sens large) l'on remarque « [qu'à] priori, les exigences de la [Cour de justice de l'Union européenne] au regard de la *Charte des droits fondamentaux de l'UE* apparaissent plus strictes sur ce point »[152]. Si l'on regarde les principes dégagés par le juge de Luxembourg pour l'obtention de données de communications auprès de fournisseurs de télécommunication, « l'accès aux données par les autorités doit être soumis à l'autorisation préalable d'une instance judiciaire ou administrative indépendante »[153]. L'Avocat général Sánchez-Bordona, dans ses conclusions du 15 janvier 2020, reprend ces principes affirmant l'incompatibilité de « [l]a conservation générale et indifférenciée de toutes les données susceptibles d'être recueillies par les fournisseurs de services de communication électronique [...] »[154] avec le droit de l'UE[155]. En plus, il remarque l'importance d'encadrer les mesures de contrôle massives non seulement « en termes d'*efficacité pratique,* mais en termes d'*efficacité juridique* et dans le contexte d'un État de droit »[156].

Cela étant, la Cour de justice de l'Union européenne n'a pas encore tranché définitivement la question à savoir si un tel contrôle indépendant *ex ante* est également indispensable pour accéder aux données obtenues par l'interception

---

151 Sur l'importance de la confiance mutuelle en matière de lutte à la surveillance massive, voir Conseil de l'Europe, *Surveillance de masse - Quel contrôle démocratique?* Strasbourg, Édition du Conseil de l'Europe, 2016 [*Surveillance de masse*].

152 Emilie Jacot-Guillarmod, « La surveillance des télécommunications par les services secrets (CourEDH) (I/III) », commentaire de *Big Brother Watch et autres c Royaume-Uni* à la p 3, en ligne : LawInside <www.lawinside.ch/702/>.

153 *Ibid*; *v*oir en ce sens *Tele2 Sverige AB c Post-och telestyrelsen* [GC], C-203/15, 21 décembre 2016, en ligne : CJUE <curia.europa.eu/jcms/jcms/P_106311/fr/>.

154 Manuel Campos Sánchez-Bordona, « Conclusions de l'Avocat général M. Manuel Campos Sánchez-Bordona », commentaire de *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs Igwan.net c Premier ministre, Garde des Sceaux, ministre de la justice, Ministre de l'Intérieur, Ministre des Armées*, 15 janvier 2020 au para 135 [non publié], en ligne : *CJUE* <//curia.europa.eu/juris/document/document.jsf?text=&docid=222263&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=18262171>.

155 CE, *Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communication électroniques)*, [2002] JO, L 201/37.

156 Sánchez-Bordona, *supra* note 154 para 137.

massive. Cette question fait l'objet de plusieurs questions préjudicielles actuellement pendantes devant la Cour de justice de l'Union européenne[157].

***

La CourEDH a toujours eu un rôle de pionnier dans la défense des droits fondamentaux et est le premier tribunal à connaitre une affaire de ce genre. Comme nous l'avons montré dans la première partie de ce travail, arrêt après arrêt, elle a su bâtir une véritable protection jurisprudentielle en matière de protection des données à caractère personnel. L'analyse de la jurisprudence nous a montré que l'article 8, grâce à l'interprétation « cinétique » faite par la CourEDH, s'est montré un instrument efficace et capable de s'adapter au panorama changeant des dernières années. Cependant, les affaires concernant la surveillance massive ont lancé de nouveaux défis.

L'*affaire Big Brother Watch* présente plusieurs difficultés, notamment le fait que la Cour met en exergue un écroulement vertigineux de la confiance réciproque entre les pays parties à la *Convention de sauvegarde des droits de l'homme et des libertés fondamentales*. L'attention et les attentes de millions de personnes étaient également dirigées vers la Cour sur ce point, car sa réponse a eu un impact sur la crédibilité même du système de protection des droits de l'homme au sein du Conseil de l'Europe. Il ne faut guère minimiser ou oublier les énormes difficultés qui ont caractérisé le travail de la Cour sur ce sujet si sensible, dans un contexte où les attaques terroristes n'ont jamais cessé de frapper sur l'Europe. Cela force à constater que le texte de cet arrêt représente un savant exercice de « diplomatie judiciaire », car tout en étant efficace et tranchant nettement certaines questions juridiques, il n'impacte pas de façon incisive sur la dimension politique qui sous-tend les rapports et la coopération entre États Parties à la *Convention* en matière de renseignement. Aux juges de Strasbourg va aussi le mérite de ne pas avoir cédé aux pressions de ceux qui prônent la sécurité à tout prix, ni à la tentation d'avancer avec une interprétation toujours plus extensive de la *Convention*.

La balle est donc dans le champ du législateur. L'Assemblée du Conseil de l'Europe ayant fait le premier pas en approuvant la *Convention STE 108+*, reste d'actualité le véritable objectif d'un « code de renseignement », pour lequel est fondamentale une volonté de collaboration proactive des gouvernements des États parties. Les « limites » que nous reprochons à l'action récente de la CourEDH sont

---

157 *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs Igwan.net c Premier ministre, Garde des Sceaux, ministre de la justice, Ministre de l'Intérieur, Ministre des Armées*, n°C-511/18 [en délibéré]; *Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX c Conseil des ministres*, n°C-520/18 [en délibéré]; *Privacy International c Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service*, n°C-623/17 [en délibéré].

d'ailleurs plus que compréhensibles dans un système international dans lequel l'équilibre des pouvoirs laisse toujours le dernier mot aux parlements nationaux des États souverains. Il est néanmoins dans les souhaits des citoyens des quarante-sept pays du Conseil de l'Europe que les leçons apprises par des affaires telles que *Big Brother Watch et autre c. Royaume-Uni* ouvrent la voie à des réformes importantes implantées au nom de la sauvegarde des libertés et des droits des Européens, tout en sachant que « [n]otre liberté repose sur ce que les autres ignorent de notre existence »[158].

[158] Alexandre Soljenitsyne, tel que cité par Pieter Ometzigt dans « Surveillance de masse », *supra* note 151 à la p 3.