Consultation sur les règles en vigueur en Belgique en matière de protection de la vie privée eu égard aux moyens autorisant l'interception et l'exploitation à grande échelle de données relatives à des personnes, organisations, entreprises ou instances établies en Belgique ou qui ont un lien avec la Belgique

Annemie Schaus
Professeure ordinaire
Vice-rectrice à la politique académique
Université libre de Bruxelles

I. Bref exposé du contexte connu des interceptions et captures massives de données à caractère personnel[1]

D'énormes quantités de données personnelles ont pu être captées par le programme PRISM, qui collecte des renseignements à une échelle et à un degré sans précédents, et dont l'objectif va bien au-delà de la lutte contre le terrorisme ou de l'espionnage économique.
Si les faits précis et surtout le rôle de certains acteurs demeurent flous, l'ampleur de l'interception, la surveillance et l'exploitation de données personnelles semble reconnue. En effet, après les premières révélations sur le programme PRISM, le directeur de la NSA a confirmé que celle-ci collecte (à la fois aux États-Unis et en dehors de cet État) des métadonnées sur les communications de tous les principaux opérateurs et qu'elle maintient une base de données contenant ces métadonnées pendant cinq ans.[2]
Il est établi également que le GCHQ a procédé à ce même type d'interception et que des grands opérateurs de réseaux de communications ou de réseaux sociaux[3] ont livrés à la NSA d'importantes données à caractère personnel.

II. Législation applicable

Il faut d'emblée rappeler que la compatibilité des services de renseignement avec la Convention européenne des droits de l'homme[4] ne fait pas de doute. Comme la Cour européenne des droits de l'homme l'a souligné, la protection des droits de l'homme peut passer par l'existence de services de renseignement, pour autant que leurs méthodes respectent les principes fondamentaux en matière de protection des droits de l'homme :
« Quel que soit le système de surveillance retenu, la Cour doit se convaincre de l'existence de garanties adéquates et suffisantes contre les abus. Cette appréciation ne revêt qu'un caractère relatif : elle dépend de toutes les circonstances de la cause, par exemple la nature, l'étendue et la

---

1 Voir le rapport de Mathias Vermeulen « De Snowden-revelaties, massale data-captatie en politieke spionage. Open bronnenonderzoek », 25 novembre 2013.

2 « Le programme de surveillance des États-Unis et leurs effets sur les droits fondamentaux des citoyens de l'UE ». Note de la direction générale des politique internes, Département thématique C : Droits des citoyens et affaires constitutionnelles, IPOL-LIBE_NT(2013)474405_FR ; Voir également le rapport de Mathias Vermeulen.

3 E.a. *Facebook, Twitter, Microsoft, Google, Yahoo!, PalTalk, YouTube, Skype, AOL* et *Apple;* voir le rapport de Mathias Vermeulen.

4 Ci-après, CEDH.

durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, exécuter et contrôler, le type de recours fourni par le droit interne ».[5]
La Cour souligne que les États contractants ne disposent pas d'une marge de manœuvre illimitée pour soumettre les personnes relevant de leur juridiction à des mesures de surveillance secrète. Consciente du danger de méconnaitre, voire de détruire, la démocratie au motif de la défendre, la Cour rappelle que les États ne peuvent prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure qu'ils jugent appropriée.
Il faut en la matière respecter le principe de légalité, de finalité et de proportionnalité, dès lors que le but légitime aura été établi.[6] Il s'ensuit que l'arsenal juridique qui protège la vie privée et les données à caractère personnel devra être respecté (A), mais aussi la souveraineté de l'État sur le territoire duquel la récolte, l'interception et le traitement de données à caractère personnel auront été effectués (B). Dans la mesure où les faits qui nous ont été soumis le permettent, nous analyserons l'application des règles aux récoltes massives des données à caractère personnel qui ont été portées à notre connaissance. Enfin, un aperçu des éventuels remèdes juridiques sera exposé (C).

A. Le respect du droit à la vie privée et la protection des données à caractère personnel

Plusieurs dispositions légales protégeant le droit à la vie privée sont susceptibles de trouver à s'appliquer dans l'affaire qui nous préoccupe ; ces dispositions sont complémentaires. Elles seront synthétiquement exposées, de la disposition au champ d'application le plus général à la disposition à vocation plus particulière, à savoir, l'article 17 du Pacte sur les droits civils et politiques (1) ; l'article 8 de la CEDH (2); la Convention n° 108 pour la protection du traitement automatisé des données à caractère personnel (3) et le droit de l'Union européenne : les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne (4), la 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[7] (telle que complétée par la directive 2002/58/CE du 12 juillet 2002 concernant la protection des données personnelles dans le secteur des communications électroniques) (5) et la directive 2006/24/CE sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques[8] (6). Enfin, il faut rappeler que la loi belge du 8 décembre 1992 sur la protection de la vie privée[9] s'applique si les critères de rattachement avec la
Belgique le justifient[10], ce qui n'est pas clairement déterminé. Dans le cadre de cette étude, nous ne pourrons donc pas analyser spécifiquement cette législation. Dans la mesure où elle s'inscrit

---

5 CEDH, *Klass et autres c. Allemagne* du 6 septembre 1978 ; CEDH, *Vereniging weekblad Bluf! c. Pays-Bas* du 9 février 1995.
6 Si la lutte contre le terrorisme peut constituer un but légitime, le profilage économique des individus ne l'est pas forcément.
7 Ci-après, directive 95/46.
8 Ci-après, directive 2006/24.
9 Ci-après, LPVP.
10 La LPVP est applicable au traitement de données à caractère personnel lorsque le traitement est effectué dans le cadre des activités réelles et effectives d'un établissement fixe du responsable du traitement sur le territoire belge comme l'indique son article 3*bis*, 1°.

dans ligne des dispositions de droit international et exécute le droit européen applicable en la matière, les analyses reprises ci-dessous lui sont transposables.
Nous verrons ensuite comment le respect de normes de protection des données à caractère personnel a fait l'objet de l'accord *Safe Harbour* entre l'UE et les États-Unis (7).
En matière de transfert, de surveillance, de contrôle de conservation de données à caractère personnel par de nouvelles technologies, il ne faut pas entendre, comme le soulignent Cécile de Terwangne et Jean-Noël Colin[11], la vie privée de façon classique dans le sens restreint de protection de la sphère privée, intime, familiale ou confidentielle. Elle s'entend, conformément à l'évolution du droit et des technologies, comme la faculté d'autodétermination, d'autonomie et la capacité de l'individu à effectuer des choix existentiels ou informationnels.[12] Comme l'a consacré la Charte des droits fondamentaux de l'Union européenne[13], il s'agit d'autodétermination informationnelle, c'est-à-dire du droit pour l'individu de connaître les données le concernant qui sont détenues, d'en maîtriser les circuits de communication, d'en empêcher les utilisations impropres ou abusives. Dans ce domaine, la vie privée ne se réduit donc pas à une quête d'intimité; c'est la maîtrise par chacun de son image informationnelle.[14] Cela dit, comme le souligne la CEDH, *« la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Conventioná»*.[15] C'est en ce sens qu'elle doit être ici comprise.

1. L'article 17 du Pacte International relatif aux droits civils et politiques[16]

L'article 17 du PIDESC est la seule disposition internationale de portée universelle qui garantit le droit à la vie privée. Tout comme les dispositions sœurs de l'article 17 qui lui sont contemporaines, cet article ne fait aucune référence aux données à caractère personnel comme élément constitutif du droit à la vie privée. Toutefois, la protection de la vie privée telle que garantie par l'article 17, mise à l'épreuve des nouvelles ingérences rendues possibles par les nouvelles technologies, a amené la 35ème Conférence internationale des commissaires à la protection des données et de la vie privée à encourager les États à adopter l'observation générale n°16 du PIDESC de 1988, de manière à renforcer la protection de la vie privée.[17] Celle-ci favorise la mise en place d'un cadre juridique mondial concernant la protection des données à caractère personnel et la protection de

---

11 *Défis pour la vie privée et la protection des données posés par la technologie,* Rapport, Namur FNDP, février 2011.

12 Pour la reconnaissance explicite d'un droit à l'autodétermination ou l'autonomie personnelle contenu dans le droit au respect de la vie privée de l'article 8 CEDH, voir CEDH, *Evans c. Royaume- Uni,* arrêt du 7 mars 2006 (confirmé par la Grande Chambre dans son arrêt du 10 avril 2007); *Tysiac c. Pologne,* arrêt du 20 mars 2007; *Daroczy c Hongrie,* arrêt du 1er juillet 2008.

13 Voir *infra* et la note suivante.

14 Paul De Hert, Katja de Vries et Serge Gutwirth, Note d'observation sur l'arrêt de la Cour constitutionnelle fédérale allemande du 27 février 2008, *Revue du droit des technologies et de l'information,* 2009, 87. Dans cet arrêt, la Cour reconnait, sur la base du droit général à la personnalité, un tout nouveau droit fondamental à la protection de « la confidentialité et l'intégrité des systèmes d'information technologiques ». Ce nouveau droit fondamental en matière de technologie de l'information doit compléter les droits fondamentaux existants là où ils font défaut.

15 CEDH, *S. et Marper c. Royaume-Uni* du 4 décembre 2008.

16 Ci-après, PIDESC.

17 http://www.unhchr.ch/tbs/doc.nsf/0/7dc7e7821c5da97680256523004a423d?Opendocument

la vie privée. Les États-Unis n'ont pas adhéré à cette observation, raison pour laquelle de nombreuses propositions visent à réactualiser l'article 17 du PIDESC lui-même à l'ère du numérique[18] parce que États-Unis en sont signataires. D'autres proposent d'adopter un protocole additionnel sur la base de l'observation générale n°16 adoptée par l'Assemblé générale des Nations Unies en 1996.[19]
Notons que la troisième Commission des Nations Unies vient d'adopter un texte sur le droit à la vie privée à l'ère du numérique.[20] Elle préconise la protection de la vie privée des personnes « hors ligne » autant que celle « en ligne » et invite tous les États *« à respecter et à protéger le droit à la vie privée, notamment dans le contexte de la communication numérique »*.[21] L'interprétation qui peut être donnée de l'article 17 du PIDESC aujourd'hui est que sa protection couvre les données à caractère personnel.

2. L'article 8 de la CEDH

L'article 8 de la CEDH garantit à chacun le droit au respect de la vie privée. La Cour européenne des droits de l'homme a expressément élargi le champ de la vie privée à celui de la protection des données à caractère personnel. Pour la Cour, «la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée consacré par l'article 8.[22] La Cour considère que *« la protection offerte par l'article 8 serait affaiblie de manière inacceptable si l'usage des techniques scientifiques modernes dans le système de la justice pénale était autorisé à n'importe quel prix et sans une mise en balance attentive des avantages pouvant résulter d'un large recours à ces techniques, d'une part, et des intérêts essentiels s'attachant à la protection de la vie privée, d'autre part »*.[23]
Selon la Cour, l'article 8 impose que le droit interne ménage des garanties appropriées pour empêcher toute utilisation impropre et abusive de données à caractère personnel. La législation nationale doit également assurer que les données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles ne sont conservées sous une forme permettant l'identification des personnes que pendant la durée nécessaire aux finalités pour lesquelles elles sont enregistrées.
La Cour rappelle que *« dans ce contexte comme dans celui des écoutes téléphoniques, de la surveillance secrète et de la collecte secrète de renseignements, il est essentiel de fixer des règles claires et détaillées régissant la portée et l'application des mesures et imposant un minimum d'exigences concernant, notamment, la durée, le stockage, l'utilisation, l'accès des tiers, les procédures destinées à préserver l'intégrité et la confidentialité des données et les procédures de*

---

18 http://www.franceonu.org/IMG/pdf/Vie_privee_FR.pdf
19 http://droitdu.net/2013/10/35eme-conference-internationale-des-commissaires-a-la-protection-des-donnees-et-de-la-vie-privee-une-volonte-duniformiser-la-protection-des-donnees-personnelles/
20 http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1&Lang=F
21 Article 4 du texte de la troisième Commission des Nations Unies
22 Voir document « Case law of the European Court of Human Rights concerning the protection of personal data», DP(2013)CASE LAW, 30 janvier 2013 [non disponible en français], http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/DP%202013%20Case%20Law_Eng%20%28final%29.pdf
23 CEDH, *S. et Marper c. Royaume- Uni* du 4 décembre 2008.

destruction de celles-ci, de manière à ce que les justiciables disposent de garanties suffisantes contre les risques d'abus et d'arbitraire [...] ».

La Cour a ainsi jugé que la mémorisation par une autorité publique de données relatives à la vie privée d'un individu constituait une ingérence dans le droit au respect de sa vie privée garanti par l'article 8, paragraphe 1er, de la CEDH, en précisant que l'utilisation qui en est faite importe peu, notamment en ces termes :

« La mémorisation par une autorité publique de données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8. L'utilisation ultérieure des informations mémorisées importe peu ».[24]

La collecte et l'archivage de données doivent donc contenir les garanties nécessaires à la sauvegarde du droit à la vie privée des individus.[25]

Le 1er juillet 2008, dans une affaire dont les faits sont proches de ceux qui nous occupent, la Cour a condamné le Royaume-Uni pour violation de l'article 8, pour l'interception illégale de communications terrestres par l'agence de renseignement GCHQ, de 1990 à 1998. Le GCHQ interceptait toutes les communications terrestres (fax, emails, télex et communications informatiques) entrant et sortant de la République irlandaise via la tour de *Capenhurst,* située dans une centrale nucléaire et fonctionnant 24 heures sur 24. Outre des informations sur le terrorisme, la tour de *Capenhurst* servait à l'espionnage économique ainsi qu'à l'interception des communications diplomatiques de l'Irlande et des communications personnelles de résidents irlandais notables, à l'aide de listes ciblées de numéros de téléphone ou de systèmes de reconnaissance vocale.[26]

La CEDH estime aussi que les États ont l'obligation de mettre en place une procédure effective permettant aux personnes intéressées d'accéder aux documents rassemblés par les services de sécurité à leur sujet.[27]

Le caractère massif et indifférencié de l'interception, la surveillance, l'utilisation, et l'archivage des données personnelles dont question en l'espèce contrevient manifestement en tous points à l'article 8 ; les mesures dénoncées visent des personnes physiques ou morales, privées ou publiques, de manière indéterminée ; les victimes sont pour la plupart non identifiables ; ces mesures ne se fondent sur aucune base légale valable et au contraire méconnaissent le droit applicable aux transferts de données à caractère personnel, elles sont manifestement disproportionnées au but poursuivi qui eux- mêmes ne sont pas définis.

Dès lors que les certains acteurs susceptibles d'avoir participé à ce système pourraient être des personnes privées, il convient de souligner que l'article 8 de la CEDH est susceptible de déployer un effet horizontal.

Dès 1979, la Cour européenne des droits de l'homme soulignait en effet :

« Si l'article 8 a essentiellement pour objet de prémunir l'individu contre les ingérences arbitraires des pouvoirs publics, il ne se contente pas de commander à l'État de s'abstenir de pareilles ingérences : à cet engagement plutôt négatif s'ajoutent des obligations positives inhérentes à un

---

24 CEDH, *Leander c. Suède* du 26 mars 1987 ; *Kopp c. Suisse* du 25 mars 1998 ; *Amann c. Suisse* du 16 février 2000 ; *Association « 21 Décembre 1989 » et autres c. Roumanie* 24 du mai 2011.

25 CEDH, *Rotaru c. Roumanie* du 4 mai 2000.

26 CEDH, *Liberty et d'autres ONG c. le Royaume-Uni* du 1er juillet 2008.

27 CEDH, *Joanna Szulc c. Pologne* du 13 novembre 2012.

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 ».[28]
Dans l'arrêt *Soderman c. Suède* du 12 novembre 2013, la Cour rappelle que lorsqu'un aspect particulièrement important de l'existence ou de l'identité d'un individu se trouve en jeu, ou que les activités en cause concernent un aspect des plus intimes de la vie privée, la marge laissée à l'État pour réglementer l'obligation qui pèse sur les particuliers, est d'autant plus restreinte.[29]
Dans leurs activités susceptibles de porter atteinte aux droits à la vie privée des individus ou des personnes morales, publiques ou privées, le respect de la vie privée incombe clairement aux fournisseurs de réseaux sociaux, aux entreprises commerciales qui œuvrent dans le domaine des nouvelles technologie et autres acteurs responsables du traitement des données à caractère personnel, sous réserve bien entendu de l'étude dans chaque cas particulier du champ d'application territoriale de l'activité de ces fournisseurs.[30]

3. La Convention n°108 pour la protection du traitement automatisé des données à caractère personnel

La Convention n°108 du Conseil de l'Europe pour la protection du traitement automatisé des données à caractère personnel est le seul instrument juridique spécifique contraignant pour tous les États du Conseil de l'Europe dans ce domaine. Ces grands principes sont les suivants :
- principe de loyauté et licéité de la collecte principe de finalité (données enregistrées pour des finalités déterminées et légitimes et pas utilisées de manière incompatible avec ces finalités) ;
- principe de qualité des données (pertinentes, adéquates, à jour, conservées pour une durée limitée) ;
- régime spécifique réservé aux données sensibles ;
- exigence de sécurité ;
- droits d'accès, de rectification et de recours ;
- possibilité de dérogations au nom d'intérêts publics ou privés prépondérants.

En 2001, un Protocole additionnel concernant les autorités de contrôle et les flux transfrontaliers de données a complété la Convention. La Convention 108 constitue l'un des meilleurs instruments juridiques pour protéger les individus contre les risques associés à la surveillance électronique. Ainsi, elle confère des droits étendus, par exemple, un droit d'accès de rectification ou d'effacement, aux données à caractère personnel.
Notons que la Convention est en cours de modernisation[31] afin de combler les lacunes qu'elle présente malheureusement encore face au défi des technologies, notamment quant à son application extra-territoriale.[32]

---

28 *Airey c. Irlande* du 9 octobre 1979.
29 Voir aussi e.a. CEDH, *I.B. c. Grèce* du 3 octobre 2013.
30 Pour la directive 95 /46, voir *infra.*
31 Proposition de modernisation du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 18 décembre 2012, STE n° 108 (T-PD) ; voir projet de recommandation http://www.coe.int/t/dghl/standardsetting/dataprotection/tpd_documents/T-PD%282013%295rev_fr_Projet%20de%20Rec.%20emploi.pdf; Sur la révision de la *Convention n°108* État des travaux en cours :

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

L'article 7 garantit le droit à la vie privée dans la droite ligne des autres instruments protecteurs des droits de l'homme. L'article 8 a une portée plus originale puisqu'il dispose que toute personne a droit à la protection des données à caractère personnel la concernant et que les données doivent être traitées loyalement, à des fins déterminées, sur la base d'un fondement légitime (consentement ou autre fondement prévu par la loi) ; et que toute personne a un droit d'accès et de rectification de ses données. L'article 7 consacre donc un droit autonome à la protection des données à caractère personnel.
Ainsi que le souligne l'avocat général Pedro Cruz Villalon dans ses conclusions du 12 décembre dernier[33], l'article 8 de la Charte consacre le droit à la protection des données personnelles comme un droit distinct du droit au respect de la vie privée. Si la protection des données tend à assurer le respect de la vie privée, elle est surtout soumise à un régime autonome, principalement défini par la directive 95/46, la directive 2002/58, le règlement n° 45/2001 et la directive 2006/24, ainsi que, dans le domaine relevant de la coopération policière et judiciaire en matière pénale, par la décision-cadre 2008/977/JAI.[34]
A l'inverse, la « sphère du privé » constituant le noyau de la «sphère du personnel», il ne saurait être exclu qu'une réglementation restreignant le droit à la protection des données personnelles en conformité avec l'article 8 de la Charte puisse néanmoins être considérée comme portant une atteinte disproportionnée à l'article 7 de la Charte ».[35]
Evidemment, le droit à la protection des données à caractère personnel repose sur le droit fondamental au respect de la vie privée. On peut donc dire, comme la Cour JUE, que *« les articles 7 et 8 de la Charte sont étroitement liés, au point de pouvoir être considérés comme établissant un « droit à la vie privée à l'égard du traitement des données à caractère personnel »*.[36]

5. La directive 95/46/CE du 24 octobre 1995

La directive 95/46 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, entrée en vigueur en octobre 1998, est la norme de base en droit communautaire dérivé. L'objet de la directive 95/46 est d'imposer aux États membres l'obligation de garantir le droit à la vie privée des personnes physiques à l'égard du traitement de leurs données à caractère personnel, en vue de permettre la libre circulation de ces données entre les États membres.
Elle impose dès lors le respect de règles définissant les conditions de licéité des traitements de données à caractère personnel, précisant les droits des personnes dont les données sont

---

www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_fr.asp

32 Rapport sur les lacunes de la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques, Cécile de Terwangne, Jean-Philippe Moiny, Yves Poullet et Jean-Marc Van Gyzeghem, Novembre 2010, Bureau du comité consultatif de la Convention n° 108.

33 Conclusions de l'avocat général M. Pedro Cruz Villalon du 12 décembre 2013 dans les affaires C-293/12 et C-494/12 pendantes devant la CJCU.

34 Voir *infra.*

35 Conclusions de l'avocat général M. Pedro Cruz Villalon, précitées.

36 Arrêt C-92/09 et C-93/09 du 9 novembre 2010.

collectées et traitées (droit à l'information, le droit d'accès et de rectification ou droit d'opposition et le droit de recours, et le droit à la confidentialité et la sécurité des traitement).
Cette directive a été complétée par la directive 2002/58 du 12 juillet 2002 concernant la protection des données personnelles dans le secteur des communications électroniques qui garantit la confidentialité des communications électroniques. L'obligation de garantir cette confidentialité pèse sur les fournisseurs de service de communications électroniques accessibles au public. Elle impose aussi aux États membres de garantir, sauf exception, la confidentialité non seulement des communications, mais également des données relatives au trafic des abonnés et des utilisateurs de services de communications électroniques. Son article 6 prévoit l'obligation pour les fournisseurs des services de communications d'effacer ou d'anonymiser les données relatives au trafic de leurs abonnés et utilisateurs qu'ils traitent et stockent.

- Les principes

La directive 95/46 vise à protéger les droits et les libertés des personnes par rapport au traitement de données à caractère personnel en établissant des principes directeurs déterminant la licéité de ces traitements.
Ces principes[37] portent sur:

- la qualité des données : les données à caractère personnel doivent notamment être traitées loyalement et licitement, et collectées pour des finalités déterminées, explicites et légitimes. Elles doivent en outre être exactes et, si nécessaire, mises à jour;
- la légitimation des traitements de données : le traitement de données à caractère personnel ne peut être effectué que si la personne concernée a indubitablement donné son consentement ou si le traitement est nécessaire :
- à l'exécution d'un contrat auquel la personne concernée est partie ; ou
- au respect d'une obligation légale à laquelle le responsable du traitement est soumis ; ou
- à la sauvegarde de l'intérêt vital de la personne concernée; ou
- à l'exécution d'une mission d'intérêt public ; ou
- à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ;
- les catégories particulières de traitements : doit être interdit le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions publiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle. Cette disposition est assortie de réserves concernant, par exemple, le cas où le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou aux fins de la médecine préventive et des diagnostics médicaux ;
- l'information des personnes concernées par les traitements de données: un certain nombre d'informations (identité du responsable du traitement, finalités du traitement, destinataires des données, etc) doivent être fournies par le responsable du traitement à la personne auprès de laquelle il collecte des données la concernant;
- le droit d'accès de ces personnes aux données: toute personne concernée doit avoir le droit d'obtenir du responsable du traitement :

---

[37] Voir synthèse de la législation sur : http://europa.eu/legislation_summaries/information_society/data_protection/l14012_fr.htm (décembre 2013).

- la confirmation que des données la concernant sont ou ne sont pas traitées et la communication des données faisant l'objet des traitements ;
- la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente directive - notamment en raison du caractère incomplet ou inexact des données - ainsi que la notification de ces modifications aux tiers auxquels les données ont été communiquées ;
- les exceptions et limitations: les principes relatifs à la qualité des données, à l'information de la personne concernée, au droit d'accès et à la publicité des traitements peuvent voir leur portée limitée afin de sauvegarder, entre autres, la sûreté de l'État, la défense, la sécurité publique, la poursuite d'infractions pénales, un intérêt économique ou financier important d'un État membre ou de l'UE ou la protection de la personne concernée;
- le droit d'opposition aux traitements de données : la personne concernée doit avoir le droit de s'opposer, pour des raisons légitimes, à ce que des données la concernant fassent l'objet d'un traitement. Elle doit également pouvoir s'opposer, sur demande et gratuitement, au traitement des données envisagé à des fins de prospection. Elle doit enfin être informée avant que des données ne soient communiquées à des tiers à des fins de prospection et doit se voir offrir le droit de s'opposer à cette communication ;
- la confidentialité et la sécurité des traitements : toute personne agissant sous l'autorité du responsable du traitement ou celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données personnelles, ne peut les traiter que sur instruction du responsable du traitement. Par ailleurs, le responsable du traitement doit mettre en œuvre les mesures appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé ;
- la notification des traitements auprès d'une autorité de contrôle: le responsable du traitement doit adresser une notification à l'autorité de contrôle nationale préalablement à la mise en œuvre d'un traitement. Des examens préalables sur les risques éventuels au regard des droits et libertés des personnes concernées sont effectués par l'autorité de contrôle après réception de la notification. La publicité des traitements doit être assurée et les autorités de contrôle doivent tenir un registre des traitements notifiés.

Toute personne doit disposer d'un recours juridictionnel en cas de violation des droits qui lui sont garantis par les dispositions nationales applicables au traitement en question. En outre, les personnes ayant subi un dommage du fait d'un traitement illicite de leurs données personnelles ont le droit d'obtenir réparation du préjudice subi.

- Le champ d'application territorial

En vertu de cette directive, des obligations incombent aux fournisseurs d'accès internet, aux moteurs de recherches, aux réseaux sociaux et autres fournisseurs de service de communication, étant tous des responsables du traitement de données à caractère personnel. Dans chaque cas particulier, l'étendue de la responsabilité du responsable du traitement de donnée peut être analysée, notamment au regard la question de l'application territoriale de la directive 95/46. En vertu de l'article 4 de la directive, un État doit appliquer sa législation de protection des données à caractère personnel conforme à la directive, si le responsable du traitement a son lieu

d'établissement sur son territoire, ou en fonction du lieu du moyen de traitement des données, c'est-à-dire si les moyens de traitement des données sont situés sur le territoire de cet État.
Le groupe « Article 29 »[38], dans son avis 5/2009 sur la protection des données par les réseaux sociaux en ligne[39], a souligné que *« Les dispositions de la directive relative à la protection des données s'appliquent dans la plupart des cas aux fournisseurs de SRS, même lorsque leur siège est situé en dehors de l'EEE »*.
Pareillement, l'une des principales conclusions de l'avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche est que la directive sur la protection des données s'applique généralement au traitement des données à caractère personnel par les moteurs de recherche, même lorsque le siège de ces derniers se trouve en dehors de l'EEE, et qu'il incombe aux fournisseurs de moteurs de recherche qui se trouvent dans cette situation de clarifier leur rôle dans l'EEE ainsi que l'étendue de leurs responsabilités en vertu de la directive.[40]
Les transferts de données à caractère personnel d'un État membre vers un pays tiers ayant un niveau de protection adéquat sont autorisés. En revanche, ils ne peuvent être effectués vers un pays tiers ne disposant pas d'un tel niveau de protection, sauf dérogations limitativement énumérées.
Il conviendra donc déterminer en fonction de faits précis, la responsabilité de chaque acteur déterminé.

- Exclusions du champ d'application matériel

L'article 3, paragraphe 2, de ladite directive indique une des limites du champ d'application matériel de celle-ci dans la mesure où il dispose que :
« La présente directive ne s'applique pas au traitement de données à caractère personnel :

- *mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal »*.

La protection des données à caractère personnel dans le cadre de la sécurité publique et le droit pénal sont donc régis par différents instruments spécifiques. Il s'agit notamment d'instruments qui instaurent des systèmes d'information communs au niveau européen, tels que la convention d'application de l'Accord de Schengen qui contient des dispositions spécifiques sur la protection des données dans le cadre du système d'information Schengen (SIS); la convention sur la base de l'article K.3 du traité sur l'Union européenne portant création d'un office européen de police; la décision du Conseil créant Eurojust et les dispositions du règlement intérieur d'Eurojust relatives au traitement et à la protection des données à caractère personnel; la convention établie sur la

---

38 Ce groupe de travail a été institué en vertu de l'article 29 de la directive 95/46. C'est un organe consultatif européen. Ses missions sont décrites à l'article 30 de la directive et 15 de la directive 2002/58.
39 Groupe 29, WP 163 « Avis 5/2009 sur les réseaux sociaux en ligne » du 12 juin 2009.
40 Groupe 29, WP 148 « Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche » du 4 avril 2008.

base de l'article K.3 du traité sur l'Union européenne, sur l'emploi de l'informatique dans le domaine des douanes, qui contient des dispositions relatives à la protection des données à caractère personnel applicables au système d'information des douanes, et la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne.[41] Le 27 novembre 2008, le Conseil a adopté une décision-cadre 2008/977/JAI du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale. Cependant, il s'applique seulement aux transferts de données entre États membres (articles 26 et 13).

6. La directive 2006/24/CE sur la Conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques

La directive 2006/24 est importante pour la question qui nous préoccupe parce qu'elle modifie les directives 95/46 et 2002/58 en prévoyant l'établissement par les États membres d'une obligation de collecte et de conservation des données de trafic et de localisation en imposant aux fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, des obligations de conservation des données de trafic et de localisation qu'elle définit, en vue de garantir leur disponibilité *« aux fins de la recherche, de la détection et de la poursuite d'infractions graves telles que définies par chaque État membre dans son droit interne »*. Ce faisant, la directive déroge aux règles dérogatoires établies par l'article 15, paragraphe 1er, de la directive 2002/58 et régissant la faculté pour les États membres de limiter, pour les motifs prévus à l'article 13, paragraphe 1er, de la directive 95/46, la portée du droit à la protection des données personnelles et, plus largement, du droit au respect de la vie privée dans le cadre spécifique de la fourniture de services de communications électroniques ou de réseaux publics de communications.
La directive 2006/24 vise à l'harmonisation des réglementations des États membres concernant la conservation des données de trafic et de localisation afférentes aux communications électroniques et, dès lors, impose aux États membres qui ne disposeraient pas d'une telle réglementation, d'une obligation de collecte et de conservation desdites données.
Cette obligation faites aux États par la directive a été jugée contraire à la Charte des droits fondamentaux par l'avocat général M. Pedro Cruz Villalon le 12 décembre 2013.[42] La Cour JUE doit encore rendre son arrêt.
La motivation de l'avocat général mérite d'être citée[43] :
« 72. Il n'en demeure cependant pas moins que la collecte et, surtout, la conservation, dans de gigantesques bases de données, des multiples données générées ou traitées dans le cadre de la plus grande partie des communications électroniques courantes des citoyens de l'Union constituent une ingérence caractérisée dans leur vie privée, quand bien même elles ne feraient que créer les conditions de possibilité d'un contrôle rétrospectif de leurs activités tant personnelles que professionnelles. La collecte de ces données crée les conditions d'une surveillance qui, pour ne s'exercer que rétrospectivement à l'occasion de leur exploitation, menace néanmoins de manière

---

41 CJUE, arrêts C-317/04 et C-318/04 du 30 mai 2005, Conclusions de l'Avocat général LEGER, point 41.
Conclusions dans les affaires C-293/12 et C-494/12 pendantes devant la CUCJ.
Les références ont été omises pour faciliter la lecture; voir la référence note précédente.

permanente, pendant toute la durée de leur conservation, le droit des citoyens de l'Union au secret de leur vie privée. Le sentiment diffus de surveillance généré pose de manière particulièrement aiguë la question de la durée de conservation des données.
73. Il doit à cet égard être tout d'abord tenu compte du fait que les effets de cette ingérence se trouvent démultipliés par l'importance acquise par les moyens de communications électroniques dans les sociétés modernes, qu'il s'agisse des réseaux mobiles numériques ou d'Internet, et leur utilisation massive et intensive par une fraction très importante des citoyens européens dans tous les champs de leurs activités privées ou professionnelles.
74. Les données en question, il importe également d'insister encore une fois à cet égard, ne sont pas des données personnelles au sens classique du terme, se rapportant à des informations ponctuelles sur l'identité des personnes, mais des données personnelles pour ainsi dire qualifiées, dont l'exploitation peut permettre l'établissement d'une cartographie aussi fidèle qu'exhaustive d'une fraction importante des comportements d'une personne relevant strictement de sa vie privée, voire d'un portrait complet et précis de son identité privée.
75. L'intensité de cette ingérence se trouve accentuée par des éléments aggravant le risque que, nonobstant les obligations imposées par la directive 2006/24 tant aux États membres eux-mêmes qu'aux fournisseurs de services de communications électroniques, les données conservées ne soient utilisées à des fins illicites, potentiellement attentatoires à la vie privée ou, plus largement, frauduleuses, voire malveillantes.
76. En effet, les données ne sont pas conservées par les autorités publiques elles-mêmes, ni même sous leur contrôle direct, mais par les fournisseurs de services de communications électroniques eux-mêmes sur lesquels pèsent l'essentiel des obligations garantissant leur protection et leur sécurité ».
Et plus loin :
« 102. L'ingérence caractérisée dans le droit au respect de la vie privée que, comme conséquence de l'effet constitutif de la directive 2006/24, les États membres sont censés incorporer à leur propre ordre juridique, apparaît ainsi hors de proportion avec la seule nécessité de garantir le fonctionnement du marché intérieur, quand bien même il doit, par ailleurs, être considéré que cette collecte et cette conservation constituent des moyens adéquats et même nécessaires à la réalisation de l'objectif ultime poursuivi par ladite directive et visant à garantir les disponibilités desdites données aux fins de la recherche et de la poursuite d'infractions criminelles graves. En résumé, la directive 2006/24 ne parviendrait pas à surmonter le test de proportionnalité pour les raisons mêmes qui justifiaient sa base juridique. Les motifs de son salut au regard de la base juridique seraient, paradoxalement, les motifs de sa perte au regard de la proportionnalité. »
Avant de conclure :
« 131. En conclusion, la directive 2006/24 est dans son ensemble incompatible avec l'article 52, paragraphe 1, de la Charte, dans la mesure où les limitations à l'exercice des droits fondamentaux qu'elle comporte, du fait de l'obligation de conservation des données qu'elle impose, ne s'accompagnent pas des principes indispensables appelés à régir les garanties nécessaires à l'encadrement de l'accès auxdites données et de leur exploitation ».

7. L'accord du *Safe Harbor* ou « sphère de sécurité » - Décision de la commission du 26 juillet 2000[44]

Les normes de protection de la vie privée en Europe et aux États-Unis sont nettement différentes, et plus particulièrement aux États-Unis, le droit à la vie privée au sens défini ci-dessus ne protège presque pas les personnes ne se trouvant pas sur ce territoire.[45]
Il est dès lors apparu nécessaire de trouver un cadre juridique apte à permettre le transfert de données à des fins commerciales, de l'Espace économique européen[46] vers les États-Unis.
Ce cadre juridique était d'autant plus nécessaire que, comme nous l'avons vu, les règles spécifiques de la directive 95/46 concernant l'échange de données avec des États-tiers, interdit le transfert de données personnelles en dehors des États non membres de l'EEE qui protégeraient les données personnelles à un niveau inférieur à celui de l'EEE.
Or, les États-Unis disposent d'un système de protection des données de leurs concitoyens, qui ne répond pas aux mêmes normes que celles adoptées dans le cadre de l'EEE. Sans le système du *Safe Harbor,* les exigences mises en place par la directive 95/46 auraient pu constituer une barrière aux échanges et transactions transatlantiques, puisque le non-respect des règles européennes relatives aux données personnelles par une entreprise américaine aurait pu ralentir ou suspendre des négociations commerciales ou conduire à des poursuites judiciaires en cas de violation des règles en vigueur.
Le cadre juridique de la « sphère de sécurité », le *Safe Harbor,* établit une passerelle entre les deux approches de respect de la vie privée en établissant un commun dénominateur à respecter par les entreprises et organisations américaines et permettant le transfert de données personnelles dans les respect du droit de l'EEE.
L'accord du *Safe Harbor* a été négocié entre le Département du Commerce des États-Unis *(Federal Trade Commission* ou *FTC)* et la Commission européenne afin de permettre aux entreprises américaines de certifier qu'elles respectent la législation de l'EEE afin d'obtenir l'autorisation de transférer des données à caractère personnel à des fins commerciales de l'EEE vers les États-Unis.
L'annexe I de la décision du 26 juillet 2000 précise que par donnée ou information à caractère personnel : *« il faut entendre toute donnée ou information concernant une personne identifiée ou identifiable qui entre dans le champ d'application de la directive, qui est transférée de l'Union européenne vers une organisation américaine et qui est enregistrée sous quelque forme que ce soit ».*
Si une entreprise américaine déclare par écrit adhérer aux principes de la sphère de sécurité, l'entreprise européenne devrait, en principe pourvoir, exporter des données à caractère personnel vers cette entreprise.

---

44 Décision de la Commission du 26 juillet 2000, conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la «sphère de sécurité» et par les questions souvent posées y afférentes, publiées par le ministère du commerce des États-Unis d'Amérique document C(2000) 2441 (http://eur lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:FR:PDF)

45 Note de la direction générale des politique internes, Département thématique C : Droits des citoyens et affaires constitutionnelles, IPOL-LIBE_NT(2013)474405_FR

46 Ci-après, EEE ; le *Safe Harbor* a été intégré dans l'accord sur l'EEE, par conséquent, l'Islande, le Liechtenstein et la Norvège ne sont pas considérés comme États-tiers dans l'application de cette norme.

- Les principes

Le cadre juridique du *Safe Harbor* repose sur 7 principes qui doivent être respectés par l'entreprise désireuse d'obtenir la certification. Ces principes sont détaillés dans l'Annexe I de la Décision de la Commission du 26 juillet 2000 relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et sont largement inspirés des principes mis en place par la directive 95/46 :

- Notification : l'information des personnes ;
- Choix : la possibilité accordée à la personne concernée de s'opposer à un transfert à des tiers ou à une utilisation des données pour des finalités différentes, le consentement explicite des personnes pour le recueil de données sensibles ;
- Transfert ultérieur : les principes de notification et de choix devraient être applicable au transfert de données à des tiers ;
- Sécurité : mesures de protection des données ;
- Intégrité des données : qualité et pertinence des données ;
- Accès : le droit d'accès, de rectification, de suppression des données ;
- Mise en œuvre : droit de recours, procédures de suivi et sanctions.[47]

Il faut cependant noter que la description des principes utilise un langage flou et ouvert à interprétation, qui de plus, est soumis au droit américain.
Le processus repose sur un système d'auto-certification volontaire par les entreprises américaines et prévoit un renouvellement de la certification tous les douze mois. L'entreprise intéressée par la certification doit faire parvenir à la *Federal Trade Commission,* une déclaration écrite annuelle attestant qu'elle respecte les principes du *Safe Harbor.* La *Federal Trade Commission* a pour mission de gérer le programme de certification et de surveiller sa mise en œuvre. Elle peut lancer des actions en justice contre une entreprise défaillante ou appliquer des amendes administratives aux entreprises qui, malgré leur déclaration, ne respectent pas *de facto* les principes du *Safe Harbor.*
Une fois que l'entreprise américaine est certifiée « *Safe Harbor* », elle rejoint la liste d'entreprises accréditées et tenue par le Département du Commerce des États-Unis. La liste de 3246 entreprises est consultable sur le site internet du Département du Commerce des États-Unis.[48]
Le système du *Safe Harbor* prévoit également que les plaintes de citoyens de l'EEE contre une entreprise ou organisation américaine relative à la protection des données personnelles devront être introduites devant des juridictions américaines (hormis quelques exceptions).
Mais en pratique, comme l'indique la récente étude commissionnée par le Parlement européen sur le *Safe Harbor: « Les négociateurs américains du ministère du commerce ont travaillé en étroite collaboration avec les lobbies commerciaux américains afin d'élaborer une liste de « questions fréquemment posées » permettant aux entreprises américaines d'interpréter l'accord sur la sphère de sécurité de manière à réduire les droits de l'UE en matière de protection de la vie privée,*

[47] Pour le détail des 7 principes, voir Annexe I de la décision de la Commission du 26 juillet 2000 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:FR:PDF).
[48] http://export.gov/safeharbor/ (fin septembre 2013).

indiquant comment contourner les règles liées aux données identifiables, refuser les droits d'accès, et se soustraire à tout devoir de finalité ou à toute demande de suppression. La sphère de sécurité s'est avérée tellement complexe que pendant de nombreuses années, aucun citoyen de l'UE n'a suivi toutes les étapes du processus bureaucratique pour déposer une plainte ».[49]

La directive 95/46 ainsi que les « *Safe Harbour Principles* » ne couvrent pas les données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale[50], ce qui inclut l'ensemble des fichiers de police, de justice et de renseignement. En effet, l'article 1er de la Décision de la Commission du 26 juillet 2000 relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité », indique que la décision ne s'applique qu'aux activités rentrant dans le domaine d'application de la directive 95/46.

Par ailleurs, l'annexe I paragraphe 4 de ladite Décision prévoit que « L'adhésion aux principes peut être limitée par: a) les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois des États-Unis; b) les textes législatifs, les règlements administratifs ou les décisions jurisprudentielles qui créent des obligations contradictoires ou prévoient des autorisations explicites, pour autant qu'une organisation qui a recours à une telle autorisation peut démontrer que le non-respect des principes est limité aux mesures nécessaires pour garantir les intérêts légitimes supérieurs que cette autorisation vise à servir; c) les exceptions ou les dérogations prévues par la directive ou par le droit national, à condition que ces exceptions ou dérogations soient appliquées dans des contextes comparables ».

L'échange de données à caractère personnel entre l'Union européenne et les États-Unis à des fins répressives, y compris la prévention et la répression du terrorisme et d'autres formes graves de criminalité, est régi, du moins en théorie, par un certain nombre d'accords au niveau de l'UE. Il s'agit de l'accord d'entraide judiciaire, de l'accord sur l'utilisation et le transfert des données des dossiers passagers (données PNR), de l'accord sur le traitement et le transfert de données de messagerie financière aux fins du programme de surveillance du financement du terrorisme (TFTP) et de l'accord entre Europol et les États-Unis.

- Lacunes

A la suite des diverses révélations qui nous préoccupent ici concernant des programmes américains de collecte de renseignements à grande échelle, la confiance bâtie notamment sur les « *Safe Harbour principles* » a été sévèrement ébranlée. Ces révélations ont abouti à une prise de conscience de l'insuffisance de la protection dont jouissent actuellement les données à caractère personnel et de la nécessité de revisiter et renforcer les règles en vigueur qui présentent de sérieuses lacunes.

En effet, depuis que le FISA a été amendé et élargi notamment en 2008, des entreprises américaines peuvent être contraintes de transmettre à la NSA des informations électroniques

---

49 Le programme de surveillance des États-Unis et leurs effets sur les droits fondamentaux des citoyens de l'UE, Note de la direction générale des politique internes, Département thématique C : Droits des citoyens et affaires constitutionnelles, IPOL-LIBE_NT(2013)474405_FR.
http://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT%282013%29474405_FR.pdf

50 Article 25 de la directive 95/46.

concernant des non-Américains. L'article 702 de la FISA[51] constitue un mandat général permettant aux autorités américaines de recueillir des données et d'intercepter des informations liées aux affaires étrangères des États-Unis, alors que les données à caractère personnel concernant les Américains bénéficient d'une protection supérieure. L'étendue que peut atteindre une telle délégation de compétences apparait aujourd'hui de manière manifeste et démesurée au regard des révélations de Snowden et des évolutions technologiques permettant la captation de quantités de données gigantesques au niveau mondial.

Le 27 novembre 2013, la Commission européenne a rendu public[52] le fruit de ses réflexions dans (1) un document stratégique (communication) sur les transferts de données transatlantiques, qui présente les enjeux et les risques faisant suite aux révélations sur les programmes américains de collecte de renseignements, ainsi que les mesures à prendre pour y répondre; (2) d'une analyse du fonctionnement de la « sphère de sécurité », qui réglemente les transferts de données à des fins commerciales entre l'Union européenne et les États-Unis; et (3) d'un rapport sur les conclusions du groupe de travail UE-États-Unis (MEMO/13/1059) sur la protection des données, créé en juillet 2013.

Ce rapport révèle aussi que d'importantes entreprises actives dans les nouvelles technologies qui ont participé à l'opération PRISM, sont des entreprises certifiées « *Safe Harbor* » et qu'il est donc permis de déduire que le système *Safe Harbor* doive être considéré comme ayant été un conduit important de données à caractère personnel ayant abouti à la collecte massive de données par la NSA.

Pourtant, ces pratiques, même si autorisées par la loi américaine, ne sont pas prévues dans le cadre juridique du *Safe Harbor* et ont, par conséquent, eu lieu en violation de cet accord et de la décision de la Commission qui le formalise dans le cadre juridique européen. Les principes du *Safe Harbor* ayant été établis pour assurer, aux États-Unis, un niveau de « protection adéquat » garantissant une protection des données à caractère personnel proche du niveau qui leur est garanti au sein de l'EEE, il faut considérer que les États-Unis ont détourné l'esprit de l'accord à leur profit. Le système du *Safe Harbor* n'a certainement pas été mis en place pour permettre le transfert de données qui pourraient ensuite être remises en masse aux autorités américaines de la sûreté, alors même que les autorités européennes de sûreté ne peuvent agir de la sorte.

La Commission européenne considère que la captation massive de données à caractère personnel par la NSA ne peuvent pas être considérées comme étant couvertes par la limitation de la protection des données, prévue dans le *Safe Harbor,* pour les besoins de la sûreté nationale. En effet, le caractère massif et sans autorisation préalable de la captation de données empêche que ce processus puisse être considéré comme nécessaire et proportionné aux intérêts de la sécurité nationale. S'agissant d'une atteinte à un droit fondamental de l'homme, il faut que celle-ci soit appréciée restrictivement comme prévue par la loi et limitée.

Par ailleurs, la Commission européenne présente aussi son réexamen des accords en vigueur sur les données des dossiers passagers (données PNR) (MEMO/13/1054) et sur le programme de

---

[51] Foreign Intelligence Surveillance Act of 1978 (décrit les procédures des surveillances physiques et électroniques, ainsi que la collecte d'informations sur des puissances étrangères soit directement, soit par l'échange d'informations avec d'autres puissances étrangères), modifié en 2008 par le FISA Amendments Act

[52] Newsroom de la Commission européenne: http://ec.europa.eu/justice/newsroom/data-protection/news/131127_en.htm

surveillance du financement du terrorisme (TFTP), qui réglementent les échanges de données à des fins répressives dans ces secteurs.
Dans cette communication, la Commission indique notamment sa volonté d'adopter d'ici au printemps 2014 une réforme de la protection des données dans l'UE afin de garantir que les données à caractère personnel soient plus efficacement et intégralement protégées.
Par ailleurs, s'agissant plus particulièrement des relations transatlantiques, la Commission a présenté 13 recommandations visant à améliorer le fonctionnement de la « sphère de sécurité », jugé déficient à plusieurs égards d'après les conclusions d'une analyse également publiée le même jour par la Commission. Le dispositif devrait donc être revu et amélioré.
S'agissant de la coopération policière et judiciaire en matière pénale, la Commission voudrait faire pression sur l'administration américaine pour qu'elle s'engage, comme principe général, à recourir à un cadre juridique, tel que les accords sectoriels et d'entraide judiciaire conclus entre l'UE et les États-Unis (comme l'accord sur les données PNR et le programme de surveillance du financement du terrorisme), chaque fois que des transferts de données sont nécessaires à des fins répressives. S'adresser directement aux entreprises ne devrait être possible que dans des cas exceptionnels clairement définis et susceptibles d'un contrôle juridictionnel.
Plus largement, la Commission européenne a déclaré souhaiter que le réexamen annoncé par la présidence américaine des activités de l'Agence de sécurité nationale, comporte une protection des citoyens de l'Union européenne ne résidant pas aux États-Unis. Ces derniers devraient pourvoir bénéficier des mêmes garanties que les citoyens américains.

- Réforme globale des règles en matière de protection des données

Comme annoncé en janvier 2012[53], la Commission planche sur une réforme globale en matière de protection des données. La réforme vise à mettre à jour et moderniser les principes inscrits dans la directive de 1995 relative à la protection des données afin de garantir à l'avenir les droits en matière de respect de la vie privée. Cette réforme comprend deux propositions législatives : un règlement définissant un cadre général de l'UE pour la protection des données et une directive relative à la protection des données à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ainsi que d'activités judiciaires connexes.
Les principales modifications envisagées par la réforme sont notamment les suivantes[54]:

- un corpus unique de règles relatives à la protection des données sera valable dans toute l'Union. Les obligations administratives inutiles, comme celles en matière de notification qui incombent aux entreprises, seront supprimées, ce qui représentera pour ces dernières une économie annuelle de quelque 2,3 milliards d'EUR;
- en lieu et place de l'obligation actuelle imposée à toutes les entreprises de notifier l'ensemble des activités concernant la protection de données à des autorités de contrôle compétentes en la matière — cette obligation étant à l'origine de formalités administratives inutiles coûtant 130 millions d'EUR par an aux entreprises, le règlement impose davantage d'obligations aux entités procédant au traitement de données à caractère personnel et accroît leur responsabilité;

Communiqué de presse : http://europa.eu/rapid/press-release_IP-12-46_fr.htm
Communiqué de presse : http://europa.eu/rapid/press-release_IP-12-46_fr.htm

- Ainsi, les entreprises et organisations devront, dans les meilleurs délais (si possible, dans un délai de 24 heures), notifier à l'autorité de contrôle nationale les violations graves de données à caractère personnel;
- les organisations n'auront plus comme interlocuteur qu'une seule autorité nationale chargée de la protection des données dans le pays de l'Union où elles ont leur établissement principal. De même, les citoyens pourront s'adresser à l'autorité chargée de la protection des données dans leur pays, même lorsque leurs données sont traitées par une entreprise établie en dehors du territoire de l'UE. Chaque fois que le consentement de la personne concernée est exigé pour que ses données puissent être traitées, il est précisé que ce consentement ne sera pas présumé, mais devra être donné explicitement.
- l'accès des personnes concernées à leurs propres données sera facilité, de même que le transfert de données à caractère personnel d'un prestataire de services à un autre (droit à la portabilité des données). La concurrence entre prestataires de services s'en trouvera renforcée.
- un « droit à l'oubli numérique » aidera les citoyens à mieux gérer les risques liés à la protection des données en ligne : ils pourront obtenir la suppression de données les concernant si aucun motif légitime ne justifie leur conservation.
- les règles de l'Union devront s'appliquer si des données à caractère personnel font l'objet d'un traitement à l'étranger par des entreprises implantées sur le marché européen et proposant leurs services aux citoyens de l'Union.
- les autorités nationales indépendantes chargées de la protection des données seront renforcées afin qu'elles puissent mieux faire appliquer et respecter les règles de l'UE sur le territoire de l'État dont elles relèvent. Elles seront habilitées à infliger des amendes aux entreprises qui enfreignent les règles de l'Union relatives à la protection des données. Ces amendes pourront atteindre 1 million d'EUR ou 2 % du chiffre d'affaires annuel global de l'entreprise.
- Une nouvelle directive appliquera les règles et principes généraux relatifs à la protection des données à la coopération policière et judiciaire en matière pénale. Les règles s'appliqueront aux traitements aussi bien transfrontières que nationaux de données à caractère personnel ».

B. Souveraineté de la Belgique

Le programme de surveillance dont il est question dans la présente étude, se fonde manifestement sur une structure internationale à laquelle collaborent certainement les États-Unis (NSA) et le Royaume-Uni *(*GCHQ), mais aussi sans doute d'autres États du Conseil de l'Europe et de l'Union européenne. Ces derniers ont sans doute été dépassés par la structure à laquelle ils ont collaboré et se sont retrouvés eux-mêmes victimes de la surveillance massive.
Il faut se rappeler que l'accord sur le renseignement en matière de télécommunications UK-USA, déjà conclu en 1947 et auquel sont parties 5 pays anglo-saxons (États-Unis, Royaume-Uni, Canada, Nouvelle-Zélande et Australie) est l'accord de base pour la surveillance des communications au sens large, et était déjà à la base de l'ossature du système de surveillance Echelon, qui a bousculé

l'Europe dans les années 2000. L'excellente étude que Dimitri Yernault a consacrée à ce système d'écoute garde toute son actualité et pourrait être ici quasi-intégralement reproduite.[55]

Une question fondamentale posée par la surveillance massive de communications électroniques non consenties par l'État sur le territoire duquel la surveillance a lieu, même au départ, d'une installation sur le territoire d'un État tiers, est de savoir si elle viole la souveraineté de cet État. La réponse est positive si l'État n'y a pas consenti, même si ces écoutes sont conformes au droit de l'État qui y procède (directement ou par l'intermédiaire d'entreprises commerciales qui y collaborent volontairement ou contraintes) : ce type d'écoutes porte atteinte à la souveraineté de l'État sur le territoire duquel les communications sont interceptées.

En effet, l'interception de communication est par définition un acte de contrainte — clandestin ou autorisé par la législation de l'État tiers — qui s'exerce sur le territoire d'un autre État et viole sa souveraineté.[56]

L'État sur le territoire duquel s'exerce la contrainte doit donner son consentement préalable.[57] Si ce n'est pas le cas, les écoutes, surveillance, interceptions clandestines, et *a fortiori* celles opérées par des systèmes de *malware* violent la souveraineté de cet État. A ce titre, elle peut justifier une réaction diplomatique.

Il en va de même des écoutes clandestines opérées au départ des ambassades des États tiers situées sur le territoire de l'État sur le territoire duquel les écoutes et surveillances sont effectuées. Elles peuvent pareillement justifier la mise en cause des bonnes relations diplomatiques.

En effet, elles enfreignent la Convention de Vienne sur les relations diplomatiques du 18 avril 1961, notamment l'article 3d qui [ne] permet à la mission diplomatique [que] de

d) S'informer par tous les moyens licites des conditions et de l'évolution des événements dans l'État accréditaire et faire rapport à ce sujet au gouvernement de l'État accréditant ;

Les missions diplomatiques ont en vertu de l'article 41.1 *« le devoir de respecter les lois et règlements de l'État accréditaire. Elles ont également le devoir de ne pas s'immiscer dans les affaires intérieures de cet État »*. Du reste, comme l'exige l'article 41.3, les locaux de la mission ne peuvent être utilisés d'une manière incompatible avec les fonctions de la mission qui comme on vient de le voir, ne peut s'informer que par des moyens licites (art. 3d susmentionné).

Enfin, l'article 27.1. stipule *: «1. L'État accréditaire permet et protège la libre communication de la mission pour toutes fins officielles. En communiquant avec le gouvernement ainsi qu'avec les autres missions et consulats de l'État accréditant, où qu'ils se trouvent, la mission peut employer tous les moyens de communication appropriés, y compris les courriers diplomatiques et les messages en code ou en chiffre. Toutefois, la mission ne peut installer et utiliser un poste émetteur de radio qu'avec l'assentiment de l'État accréditaire ».*

Il va sans dire que ce type d'interception clandestine et sauvage de communications viole en soi le droit à la vie privée, tel que protégé par les dispositions précitées et engage la responsabilité internationale de l'État, qu'il soit membre du Conseil de l'Europe ou non, de l'Union européenne ou non. En effet, si c'est le cas, la responsabilité internationale pour violation de la souveraineté

---

55 Dimitri Yernault, « De la fiction à la réalité : le programme d'espionnage électronique global « Echelon » et la responsabilité internationale des États au regard de la convention européenne des droits de l'homme », *RBDI,* 2000, 137 et suiv.

56 CPJI, *Affaire du Lotus,* 7 septembre 1927, *Recueil,* Série A, n° 9, 18.

57 Voir Les travaux de l'Institut de droit international, *Annuaire de droit international,* vol. 68-I, 1999; voir aussi Dimitri Yernault, *op. cit.,* 180.

de l'État se double de la violation des traités internationaux applicables au droit au respect de la vie privée.

C. Aperçu des moyens d'action à la disposition de l'État, des citoyens et des entreprises

Il est évidemment impossible, à défaut d'être saisi de faits établis précis dénoncés dans des cas particuliers, d'étudier toutes les voies de recours possibles dans une affaire aux dimensions tentaculaires comme celle dénoncée par E. Snowden et dont toutes les responsabilités n'ont pas encore été établies. Une des actions à mener pourrait être de demander la tenue d'une enquête parlementaire pour établir précisément les faits et les éléments de responsabilité des acteurs. L'État sur le territoire duquel des violations structurelles de droits de l'homme ont lieu a l'obligation générale de « prévenir » celles-ci ou de les sanctionner.[58] Il ne peut donc rester indifférent. En l'occurrence, il semble clair que surveillance massive des données à caractère personnel tel qu'effectué par la NSA et/ou d'autres acteurs sur le territoire belge est structurelle.
A ce stade, il ne peut s'agir ici que de soumettre quelques pistes.

1. La Cour internationale de Justice

L'État peut soumettre le différend international, à savoir la mise en cause de la responsabilité internationale de l'État étranger qui a effectué les écoutes illégales ou qui a permis que soient effectuées les écoutes illégales, par exemple en mettant son territoire à disposition de l'interception et l'écoute illégale, et ce devant la Cour internationale de Justice, si les conditions très restrictives de sa compétence sont réunies. La même juridiction peut être saisie de la question du respect de la Convention de Vienne sur les relations diplomatiques et consulaires.

2. La Cour européenne des droits de l'homme[59]

Si l'État responsable de la surveillance ou qui y a collaboré est membre du Conseil de l'Europe, une requête inter-étatique devant la Cour européenne des droits de l'homme est un moyen juridique de faire cesser les violations et d'obtenir réparation. Elle avait été sérieusement envisagée dans l'affaire dite « Echelon ».[60] Si en l'occurrence, l'intervention des services secrets du Royaume-Uni ou d'autres États parties à la CEDH étaient démontrée, il s'agirait d'une action exemplaire.

3. Juridictions belges : piratage informatique et infractions pénales

- Les entreprises belges victimes d'interceptions illégales des données dont elles disposent peuvent, selon les faits qui seront établis, déposer plainte contre l'État étranger devant les juridictions de cet État, mais aussi devant les juridictions belges, s'il est établi que les faits ont un lien avec la Belgique (interception en Belgique). Par exemple, le *malware* qui semble avoir

---

58 Voir notamment Dimitri Yernault, op. cit. 214.

59 Ce recours paraît plus efficace qu'un recours devant le Comité des droits de l'homme, mais cette possibilité ne doit pas être exclue.

60 Voir Dimitri Yernault, *op. cit.,* 154 et suiv.

infecté le système informatique de Belgacom peut faire l'objet d'action judiciaire en Belgique. Un exposé des faits plus précis est toutefois nécessaire pour donner une étude juridique sur cette possibilité !

- Dans la mesure où les dispositions spécifiques sur la protection des données à caractère personnel le prévoient, elles sont évidemment susceptibles de s'appliquer aux personnes privées dès qu'elles sont responsables du traitement de données à caractère personnel au sens des dispositions analysées ci-dessus. Ainsi en est-il particulièrement des directives qui s'adressent aussi aux fournisseurs de réseaux, de services de télécommunication, etc. qui doivent évidemment être affinées dans chaque cas d'espèce. Pour Facebook, par exemple, une étude exhaustive a été réalisée.[61] Elle devrait l'être pour chaque responsable potentiel dont le rôle pourrait être déterminé dans l'affaire qui nous préoccupe.
- Selon l'établissement des faits, s'il était établi que des entreprises privées ont collaboré, à l'insu de l'État, à la mise en œuvre des procédés d'interception (sur le câble optique à Ostende par exemple ou en transmettant volontairement des données à caractère personnel un État étranger (NSA ou autre), l'État ou des particuliers ou des entreprises victimes de ce piratage informatique peuvent déposer plainte au pénal en vertu de la loi sur la protection de la vie privée du 8 décembre 1992, sur la base notamment des articles 550*bis* et 314*bis* du code pénal et 124 et 145 de la loi du 13 juin 2005 relative aux communications électroniques. Le piratage informatique est en effet pénalement sanctionné.[62]

Le titre IX*bis* du code pénal belge est intitulé : *« Infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui sont stockées, traitées ou transmises par ces systèmes ». Les articles 550*bis *et 550*ter *punissent divers comportements de peines allant de 3 mois à 5 ans d'emprisonnement. La loi pénale belge interdit d' « accéder à un système informatique » ou de « s'y maintenir » (article 550bis, § 1er, alinéa 1), mais également de faire « un usage quelconque d'un système informatique appartenant à un tiers » (article 550bis, § 3, 2°) ou de « causer un dommage quelconque à ce système » (article 550bis, § 1er, 3°). La loi punit « celui qui ordonne la commission d'une des infractions visée aux §§ 1 à 5 »* (article 550bis, § 6), et sanctionne *« celui qui, sachant que des données ont été obtenues par la commission d'une des infractions visées aux §§ 1 à 3, les détient, les révèle à une autre personne ou les divulgue, ou fait un usage quelconque des données ainsi obtenues » d'un emprisonnement de six mois à trois ans et/ou d'une amende de 26 à 100.000 euros (article 550*bis, *§7) »*.
Le titre V du code pénal belge (*« Des crimes et des délits contre l'ordre public commis par des particuliers »*) contient un chapitre VII*bis* intitulé *« Infractions relatives au secret des communications et des télécommunications privées »*. L'article 314*bis,* § 1er puni d'un emprisonnement de 6 mois à 1 an et/ou d'une amende de cent à dix mille euros celui qui *« prend connaissance »*, *« enregistre » « pendant leur transmission »* des *« communications privées »*, *« auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications »* ou *« installe ou fait installer un appareil quelconque »* à cette fin. L'article 314*bis,* § 2 puni d'un emprisonnement de six mois à deux ans et/ou à une amende de cinq cent à

---

61 Jean-Philippe Moiny, Facebook au regard des règles européennes concernant la protection des données, *Rev. Eur.de droit de la consommation,* 235.

62 La législation belge est exemplaire à ce sujet.

vingt mille euros celui qui révèle, divulgue, ou *« utilise sciemment d'une manière quelconque une information obtenue de cette façon »*.
Les individus et entreprises qui ont été victimes de ces infractions peuvent déposer une plainte pénale en Belgique, soit auprès du procureur du Roi, soit en se constituant partie civile. La question de la compétence territoriale afin de pouvoir déposer une telle plainte se résout en fonction des faits de la cause. Soit le fait infractionnel a été commis en Belgique (par exemple l'accession illégale à un système informatique en Belgique), soit les conséquences du crime ont fait sentir leurs effets en Belgique (si on applique aux cybercrimes un enseignement classique de la cour de Cassation, initiée à l'occasion d'une affaire relative à un chèque émis à Téhéran, et tiré sur une banque belge[63]).
Cela dit, en droit belge, ces intrusions informatiques peuvent être légales dans le cas où elles sont réalisées, par le biais des dispositions du code d'instruction criminelle relatives à la saisie de données informatiques, via le procédé de la perquisition d'un ordinateur et de l'extension de cette perquisition, ordonnée par le juge d'instruction par ordonnance motivée, « vers un système informatique qui se trouve dans un autre lieu » (article 88*ter* du code d'instruction criminelle) et par l'injonction donnée par le même magistrat à une personne ayant *« une connaissance particulière »* afin d'accéder aux données stockées *« dans une forme compréhensible »* (article *88quater* du code d'instruction criminelle). Cette mesure d'enquête peut également être réalisée à de strictes conditions, en tant que *« méthode exceptionnelle de recueil de données »* par la Sûreté de l'État ou par le Service général du renseignement et de la sécurité des Forces armées (article 18/16, §§ 1 à 5 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité).
Toute intrusion informatique ou utilisation de données recueillies ou utilisées en Belgique, sans autorisation légale, demeure une infraction pénale. Le code d'instruction criminelle belge prévoit en son article 29, une obligation pour tout fonctionnaire qui viendrait à découvrir une infraction, de la dénoncer au procureur du roi. Cette obligation est générale et concerne toute infraction.[64]

4. <u>Usage des informations obtenues par un système de surveillance illégal</u>

La question est de savoir dans le cas où un service de police ou de renseignement reçoit ce type d'information, s'il peut l'utiliser dans le cadre de ses missions. La loi sur le recueil de données prévoit que si une mesure de recueil de donnée exceptionnelle, comme l'intrusion informatique, a été réalisée illégalement, la commission chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données des services de renseignement et de sécurité, conserve ces données et interdit aux services de renseignement et de sécurité, d'exploiter ces données (article 18/10, § 6, alinéa 4 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité). Il est à noter qu'aucune disposition ne réglemente les conséquences à donner dans le cas où cette illégalité a été réalisée par un service étranger. Une indication de la solution à développer peut être trouvée dans les discussions qui ont précédé l'adoption de la loi du 4 février 2010 relative aux MRD. En effet, la loi de 1998 relative aux services de renseignement mentionne la coopération avec les services étrangers en son article 20, § 1er. Néanmoins, le président du

63 Tribunal correctionnel, Dendermonde, 29 septembre 2008, *Tijdschrift voor Strafrecht,* 2009/2, 111-114.
64 Alain Winants, De Veiligheid van de Staat en de BIM-Wet, in Wauter Van Laethem, Dirk Van Daele en Bart Vangeebergen(Eds), *De Wet op de bijzondere inlichtingenmethoden,* Intersentia, Antwerpen Oxford, 141.

Comité permanent R a indiqué que *« le Comité ne peut pas contrôler les services de renseignement étrangers. Il serait indiqué de compléter la loi sur ce point de telle sorte que la légalité des opérations de services de renseignement étrangers amis, admis sur notre territoire, puisse également être contrôlée par la Sûreté de l'État »*.[65] Monsieur Winants a déclaré à cette occasion: *« Si un service de renseignement étranger excède ses pouvoirs, la Sûreté de l'État a la possibilité d'intervenir, sur la base de l'article précité (article 20 de la loi de 1998) »*.[66] Monsieur Hellemans, chef du SGRS, a quant à lui déclaré: *« Le SGR part du principe qu'il est systématiquement informé par les services étrangers dès lors que ceux-ci poursuivent un objectif en Belgique. Le service entretient de bons contacts avec les pays amis et a recours à un système d'échange de données. Le service reste bien évidemment responsable des données qui sont recueillies sur le territoire belge »*.[67]

Il ressort de tout ceci, premièrement, que la réalisation par un service étranger d'une méthode de recueil de donnée exceptionnelle en Belgique, telle que l'intrusion informatique n'est pas réglementée, deuxièmement que cette méthode de renseignement est une infraction pénale, et, troisièmement, qu'il est interdit aux services belges d'utiliser les informations obtenues de manière illégale, à défaut de quoi les services belges se rendraient également coupable de la commission d'une infraction s'ils le font sciemment.

La problématique de la coopération avec les services étrangers et la manière de contrôler celle-ci est une des priorités du Comité permanent R. Dès son rapport d'activités de 2008, le Comité a relaté diverses contributions réalisées à l'étranger afin de promouvoir un contrôle démocratique effectif sur les services de renseignement, et ces initiatives bénéficient du soutien du Rapporteur Spécial des Nations Unies pour la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte contre le terrorisme, Martin Sheinin.[68] L'échange d'informations avec des services « amis » n'est pour le moment soumis qu'à des principes éthiques, et cette faille dans les lois de contrôle des services de renseignement a été critiquée, en proposant que des réglementations nouvelles viennent remplir ce vide juridique.[69]

La question de l'utilisation judiciaire de ce type d'informations se résout différemment. En effet, le droit de la procédure pénale belge prévoit une règle d'exclusion des éléments de preuve obtenus de manière illégale. Cette exclusion n'est néanmoins pas absolue. En effet, la loi du 24 octobre 2013 a inséré dans le code d'instruction criminelle un nouvel article 32, qui se lit de la manière suivante :

« Art. 32. La nullité d'un élément de preuve obtenu irrégulièrement n'est décidée que si :

- *le respect des conditions formelles concernées est prescrit à peine de nullité, ou;*
- *l'irrégularité commise a entaché la fiabilité de la preuve ou;*
- *l'usage de la preuve est contraire au droit à un procès équitable »*.

---

65 *Doc. Parl,* Chambre, Session 52ème législature, 2009-2010, DOC 52 / 2128/000, 41

66 *Ibid.*

67 *op. cit.,* 46

68 Comité permanent R, *Rapport d'activités 2008*, 87.

69 Pour une étude approfondie consacrée à cette question, voir e.a. Elizabeth Sepper, Democracy, Human Rights and Intelligence Sharing, *Texas International Law Journal,* Vol. 46: 151, 2010, pp. 153-206 ; European Parliament, Committee on Civil Liberties, Justice and Home Affairs, *Working Document 5 on Democratic oversight of Member State intelligence services and of EU intelligence bodies,* 11 novembre 2013, DT\1009342EN.doc

Cette loi fait suite à la jurisprudence de la cour de Cassation belge dite « Antigone » du 14 octobre 2003.[70] Cette jurisprudence avait déjà donné lieu à une loi du 9 décembre 2004 *« sur l'entraide judiciaire internationale en matière pénale et modifiant l'article 90*ter *du Code d'Instruction Criminelle »*, qui dispose, en son article 13:
« Art. 13. Ne peuvent être utilisés dans le cadre d'une procédure pénale menée en Belgique, les éléments de preuve:

1° recueillis irrégulièrement à l'étranger, lorsque l'irrégularité :
- *découle, selon le droit de l'État dans lequel l'élément de preuve a été recueilli, de la violation d'une règle de forme prescrite à peine de nullité ;*
- *entache la fiabilité de la preuve ;*

2° ou dont l'utilisation viole le droit à un procès équitable ».

Cette réglementation de la preuve implique donc que toute illégalité/irrégularité n'entraîne pas l'écartement automatique de cet élément de preuve. Néanmoins, à l'occasion d'un livre qui a fait date[71], le président de la section pénale de la cour de Cassation de Belgique a indiqué qu'au-delà des nullités prévues spécifiquement par un texte de loi, ou de celles qui entachent la fiabilité de la preuve ou dont l'usage viole le droit à un procès équitable, il existe également les nullités infractionnelles, c'est-à-dire le cas où la preuve est *« entachée par la commission d'un délit »*.[72] A l'occasion d'une étude de la jurisprudence rendue en la matière, cet éminent magistrat distingue, en ce qui concerne les délits commis par les organes de recherche, la situation d'un délit commis afin d'obtenir une preuve, de celle d'une infraction commise au moment du constat d'une infraction commise par un délinquant.[73] Dans le premier cas, par exemple une intrusion illégale dans un système informatique, la preuve ne sera pas recevable. Dans le second cas, par exemple la participation à un trafic de stupéfiants en vue d'en arrêter les auteurs, *« dès lors que la résolution criminelle est manifestement antérieure à l'intervention policière et que l'autorité verbalisante ne commet que des irrégularités extérieures aux saisies, perquisitions, observations et auditions, la preuve serait recevable »*.[74]

---

70 RG P.03.0762.N
71 Jean de CODT, *Des nullités de l'instruction et du jugement,* Bruxelles, Larcier, 2006, 233 pp.
72 *op. cit.,* 16.
73 *op. cit.,* 103-104.
74 *op. cit.,* 105.