



Commission
européenne



AVIS N° 28 DU GROUPE EUROPÉEN D'ÉTHIQUE
DES SCIENCES ET DES NOUVELLES TECHNOLOGIES

L'éthique des technologies de sécurité et de surveillance

Bruxelles, le 20 mai 2014



Groupe Européen
d'Éthique des Sciences
et des Nouvelles
Technologies

L'éthique des technologies de sécurité et de surveillance

Bruxelles, le 20 mai 2014

Jim Dratwa
Rédacteur en chef

28

Avis N°



***Europe Direct est un service destiné à vous aider
à trouver des réponses aux questions que vous
vous posez sur l'Union européenne.***

**Un numéro unique gratuit (*):
00 800 6 7 8 9 10 11**

(*) Les informations sont fournies à titre gracieux et les appels sont généralement gratuits (sauf certains opérateurs, hôtels ou cabines téléphoniques).

De nombreuses autres informations sur l'Union européenne sont disponibles sur l'internet via le serveur Europa (<http://europa.eu>).

Luxembourg: Office des publications de l'Union européenne, 2014

ISBN 978-92-79-37943-7

doi:10.2796/2409

© Union européenne, 2014

Reproduction autorisée, moyennant mention de la source.

Photo © Gstudio Group

Printed in Luxembourg

IMPRIMÉ SUR DU PAPIER BLANCHI SANS CHLORE ÉLÉMENTAIRE (ECF)

AVIS DU GROUPE EUROPÉEN D'ÉTHIQUE DES SCIENCES ET DES NOUVELLES TECHNOLOGIES AUPRÈS DE LA COMMISSION EUROPÉENNE

L'éthique des technologies de sécurité et de surveillance

N° 28

20.5.2014

Référence: *Demande du président Barroso*
Rapporteurs: *Inez de Beaufort, Linda Nielsen, Siobhán O'Sullivan*

LE GROUPE EUROPÉEN D'ÉTHIQUE DES SCIENCES ET DES NOUVELLES TECHNOLOGIES (GEE),

vu le traité sur l'Union européenne, et notamment l'article 6 de ses dispositions communes relatif au respect des droits fondamentaux,

vu le traité sur le fonctionnement de l'Union européenne, et notamment l'article 16 relatif au droit à la protection des données à caractère personnel,

vu la charte des droits fondamentaux de l'Union européenne, et notamment l'article 1^{er} (Dignité humaine), l'article 3 (Droit à l'intégrité de la personne), l'article 6 (Droit à la liberté et à la sûreté), l'article 7 (Respect de la vie privée et familiale), l'article 8 (Protection des données à caractère personnel), l'article 10 (Liberté de pensée, de conscience et de religion), l'article 11 (Liberté d'expression et d'information), l'article 20 (Égalité en droit), l'article 21 (Non-discrimination), l'article 42 (Droit d'accès aux documents), l'article 47 (Droit à un recours effectif et à accéder à un tribunal impartial), l'article 48 (Présomption d'innocence et droits de la défense) et l'article 52 (Portée des droits garantis) ⁽¹⁾,

vu la Déclaration universelle des droits de l'homme, et notamment les articles 7, 8, 10, 11, 12 et 14 ⁽²⁾,

vu la Convention européenne des droits de l'homme (CEDH), et notamment l'article 5 (Droit à la liberté et à la sûreté) et l'article 8 (Droit au respect de la vie privée et familiale) ⁽³⁾,

vu le Pacte international relatif aux droits civils et politiques, et notamment les articles 14, 17, 18 et 19 ⁽⁴⁾,

vu l'article 6 du septième programme-cadre de l'Union européenne pour des actions de recherche, de développement technologique et de démonstration (2007-2013), qui établit que «Toutes les activités de recherche menées au titre du septième programme-cadre sont réalisées dans le respect des principes éthiques fondamentaux»,

vu la Convention du Conseil de l'Europe sur les droits de l'homme et la biomédecine, signée le 4 avril 1997 à Oviedo ⁽⁵⁾,

vu la Convention du Conseil de l'Europe sur la cybercriminalité, signée le 23 novembre 2001 qui prévoit des moyens flexibles et modernes de coopération internationale ⁽⁶⁾,

⁽¹⁾ Journal officiel C 364 de novembre 2000, p. 1-22.

⁽²⁾ <http://www.worldservice.org/udhr.html#12>

⁽³⁾ http://www.echr.coe.int/Documents/Convention_FRA.pdf

⁽⁴⁾ <http://www.ohchr.org/fr/professionalinterest/pages/ccpr.aspx>

⁽⁵⁾ <http://conventions.coe.int/Treaty/fr/Treaties/Html/164.htm>

⁽⁶⁾ <http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm>

vu le Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, signé le 28 janvier 2003 ⁽⁷⁾,

vu la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques ⁽⁸⁾ (directive cadre),

vu la directive 2002/19/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion ⁽⁹⁾ (directive accès),

vu la directive 2002/20/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'autorisation de réseaux et de services de communications électroniques ⁽¹⁰⁾ (directive «Autorisation»),

vu la directive 2002/22/CE du Parlement européen et du Conseil du 7 mars 2002 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques ⁽¹¹⁾ (directive «Service universel»),

vu la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, 213 RTNU 222, entrée en vigueur le 3 septembre 1953, telle que modifiée par les protocoles n° 3, 5, 8 et 11 qui sont entrés en vigueur respectivement le 21 septembre 1970, le 20 décembre 1971, le 1^{er} janvier 1990 et le 1^{er} novembre 1998, notamment l'article 8 (Droit au respect de la vie privée et familiale) ⁽¹²⁾,

vu la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques,

vu le règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres ⁽¹³⁾,

vu le règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour, COM(2004) 835 final,

vu la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE,

⁽⁷⁾ <http://conventions.coe.int/Treaty/fr/Treaties/Html/189.htm>

⁽⁸⁾ JO L 108 du 24.4.2002.

⁽⁹⁾ JO L 108 du 24.4.2002.

⁽¹⁰⁾ JO L 108 du 24.4.2002.

⁽¹¹⁾ JO L 108 du 24.4.2002.

⁽¹²⁾ <http://www1.umn.edu/humanrts/instrree/z17euroco.html>

⁽¹³⁾ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0001:0006:FR:PDF>

vu la communication de la Commission au Parlement européen et au Conseil — Un espace de liberté, de sécurité et de justice au service des citoyens (Programme de Stockholm), COM(2009) 262/4,

vu la stratégie de sécurité intérieure pour l'Union européenne — Vers un modèle européen de sécurité ⁽¹⁴⁾ du Conseil européen (mars 2010),

vu 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,

vu la décision de la Commission 2000/520/CE 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, publiés par le ministère du commerce des États-Unis d'Amérique [notifiée sous le numéro C(2000) 2441] ⁽¹⁵⁾,

vu le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes de la Communauté et la libre circulation de ces données ⁽¹⁶⁾,

vu la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale ⁽¹⁷⁾,

vu la communication de la Commission au Parlement européen et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire, COM(2013) 847 du 27 novembre 2013 ⁽¹⁸⁾,

vu la directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil ⁽¹⁹⁾,

vu la proposition de règlement du Parlement européen et du Conseil portant création d'un système d'entrée/sortie pour l'enregistrement des entrées et sorties des ressortissants de pays tiers franchissant les frontières extérieures des États membres de l'Union européenne, COM(2013) 95 ⁽²⁰⁾,

vu la proposition de décision du Parlement européen et du Conseil établissant un programme de soutien à la surveillance de l'espace et au suivi des objets en orbite, COM(2013) 107 final 2013/0064 (COD) ⁽²¹⁾,

⁽¹⁴⁾ http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313FRC.pdf

⁽¹⁵⁾ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:FR:HTML>

⁽¹⁶⁾ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:fr:PDF>

⁽¹⁷⁾ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:01:FR:HTML>

⁽¹⁸⁾ http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf

⁽¹⁹⁾ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:FR:PDF>

⁽²⁰⁾ http://ec.europa.eu/dgs/home-affairs/doc_centre/borders/docs/1_en_act_part1_v12.pdf

⁽²¹⁾ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0107:FIN:FR:PDF>

vu la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale ⁽²²⁾,

vu la résolution du Parlement européen du 6 juillet 2011 sur la sûreté aérienne, en particulier sur les scanners de sûreté [2010/2154(INI)] ⁽²³⁾,

vu la résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications (96/C329/01) ⁽²⁴⁾,

vu la résolution du Parlement européen du 23 octobre 2008 sur l'impact des mesures de sûreté de l'aviation et des scanners corporels sur les Droits de l'homme, la vie privée, la dignité personnelle et la protection des données (2010/C 15 E/14) ⁽²⁵⁾,

vu la proposition de règlement du Parlement européen et du Conseil portant création du système européen de surveillance des frontières (Eurosur), COM(2011) 873 final ⁽²⁶⁾,

vu la communication de la Commission au Conseil et au Parlement européen établissant un système de gestion de la sécurité aérienne pour l'Europe, COM(2011) 670 final ⁽²⁷⁾,

vu le règlement (UE) n° 573/2010 de la Commission du 30 juin 2010 modifiant le règlement (UE) n° 185/2010 fixant des mesures détaillées pour la mise en œuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile ⁽²⁸⁾,

vu le règlement (UE) n° 358/2010 de la Commission du 23 avril 2010 modifiant le règlement (UE) n° 185/2010 du 4 mars 2010 fixant des mesures détaillées pour la mise en œuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile ⁽²⁹⁾,

vu le règlement (UE) n° 72/2010 de la Commission du 26 janvier 2010 établissant des procédures pour la conduite des inspections effectuées par la Commission dans le domaine de la sûreté aérienne ⁽³⁰⁾,

vu le règlement (CE) n° 915/2007 de la Commission du 31 juillet 2007 modifiant le règlement (CE) n° 622/2003 fixant des mesures pour la mise en œuvre des règles communes dans le domaine de la sûreté aérienne ⁽³¹⁾,

vu le règlement (CE) n° 297/2010 de la Commission du 9 avril 2010 modifiant le règlement (CE) n° 272/2009 complétant les normes de base communes en matière de sûreté de l'aviation civile ⁽³²⁾,

⁽²²⁾ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:fr:PDF>

⁽²³⁾ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:033E:0125:0134:FR:PDF>

⁽²⁴⁾ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996G1104:FR:HTML>

⁽²⁵⁾ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:015E:0071:0072:FR:PDF>

⁽²⁶⁾ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0873:FIN:FR:PDF>

⁽²⁷⁾ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0670:FIN:FR:PDF>

⁽²⁸⁾ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:166:0001:0005:FR:PDF>

⁽²⁹⁾ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:105:0012:0014:FR:PDF>

⁽³⁰⁾ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:023:0001:0005:FR:PDF>

⁽³¹⁾ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:200:0003:0004:FR:PDF>

⁽³²⁾ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:090:0001:0003:FR:PDF>

vu le règlement (UE) n° 1254/2009 de la Commission du 18 décembre 2009 fixant les critères permettant aux États membres de déroger aux normes de base communes en matière de sûreté de l'aviation civile et d'adopter d'autres mesures de sûreté ⁽³³⁾,

vu la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions. Gouvernance de Schengen — Renforcer l'espace sans contrôle aux frontières intérieures ⁽³⁴⁾,

vu la communication COM(2009) 262/4 de la Commission au Parlement européen et au Conseil. Un espace de liberté, de sécurité et de justice au service des citoyens ⁽³⁵⁾,

vu l'initiative «Frontières intelligentes» de l'UE visant à remplacer l'apposition de cachets sur les passeports des ressortissants de pays tiers par un registre électronique automatisé pour contrôler le séjour de ces visiteurs ⁽³⁶⁾,

vu la communication COM(2010) 673 final de la Commission au Parlement européen et au Conseil: La stratégie de sécurité intérieure de l'UE en action: cinq étapes vers une Europe plus sûre ⁽³⁷⁾,

vu la feuille de route sur l'intégration des RPAS civils dans le système européen de l'aviation (juin 2013) ⁽³⁸⁾,

vu le document de travail des services de la Commission *Towards a European Strategy for the Development of Civil Applications of Remotely Piloted Aircraft Systems (RPAS)* (Vers une stratégie européenne de développement d'applications civiles pour les RPAS) (septembre 2012) ⁽³⁹⁾,

vu la communication de la Commission au Parlement européen et au Conseil Rétablir la confiance dans les flux de données entre l'Union européenne et les États-Unis d'Amérique, COM(2013) 846 final,

vu l'Eurobaromètre spécial 359 — *Attitudes on Data Protection and Electronic Identity in the European Union* (Attitudes à l'égard de la protection des données et de l'identité électronique au sein de l'Union européenne), juin 2011 ⁽⁴⁰⁾,

vu l'Eurobaromètre spécial 390 — *Cyber Security* (Cybersécurité), juillet 2012 ⁽⁴¹⁾,

vu les travaux du groupe d'examen des États-Unis sur les technologies de renseignement et de communication 2013,

⁽³³⁾ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:338:0017:0017:FR:PDF>

⁽³⁴⁾ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0561:FIN:FR:PDF>

⁽³⁵⁾ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0262:FIN:fr:PDF>

⁽³⁶⁾ http://europa.eu/rapid/press-release_IP-11-1234_fr.htm

⁽³⁷⁾ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:FR:PDF#page=2>

⁽³⁸⁾ http://ec.europa.eu/enterprise/sectors/aerospace/files/rpas-roadmap_en.pdf

⁽³⁹⁾ <http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=>
<http://register.consilium.europa.eu/pd/en/12/st13/st13438.en12.pdf>

⁽⁴⁰⁾ http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

⁽⁴¹⁾ http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf

vu l'enquête mondiale relative à la sécurité des informations *Fighting to close the gap*, Ernst & Young, 2012 ⁽⁴²⁾,

vu l'avis n° 26 — L'éthique des technologies de l'information et de la communication du groupe européen d'éthique des sciences et des nouvelles technologies (22 février 2012) ⁽⁴³⁾,

vu le document *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices* ⁽⁴⁴⁾,

vu le rapport de la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures,

vu la table ronde ouverte sur le thème de l'éthique des technologies de surveillance et de sécurité qui a été organisée à Bruxelles le 18 septembre 2013,

vu les contributions des consultations ouvertes menées par le GEE sur l'éthique en matière de surveillance et de sécurité,

vu les déclarations des rapporteurs du GEE (Inez de Beaufort, Linda Nielsen, Siobhán O'Sullivan),

LE GEE ADOPTE L'AVIS SUIVANT:

⁽⁴²⁾ [http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/\\$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf](http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf)

⁽⁴³⁾ http://ec.europa.eu/bepa/european-group-ethics/docs/publications/ict_final_22_february-adopted.pdf

⁽⁴⁴⁾ <http://www.privacybydesign.ca/content/uploads/2013/01/operationalizing-pbd-guide.pdf>

TABLE DES MATIÈRES

Avis du Groupe Européen d'Éthique des Sciences et des Nouvelles Technologies auprès de la Commission Européenne 3

Introduction 13

- I.1. Portée de l'avis 13
- I.2. Une définition de la sécurité 14
- I.3. Une définition de la surveillance 14
- I.4. Les actions politiques de l'UE et le programme de Stockholm 14

Chapitre I. Applications des technologies de sécurité et de surveillance 17

- 1.1. Les télécommunications 17
- 1.2. Les technologies de l'information et de la communication 18
- 1.3. Les technologies de localisation et de suivi 26
- 1.4. Caractéristiques technologiques 28
 - 1.4.1. La miniaturisation 28
 - 1.4.2. L'ubiquité 32
 - 1.4.3. L'automatisation 32
- 1.5. La convergence des technologies 33
- 1.6. Les moteurs de la technologie 33
 - 1.6.1. Les moteurs sociaux 33
 - 1.6.2. Les moteurs politiques 34
 - 1.6.3. Les moteurs économiques 34
- 1.7. Les limites de la technologie 34
- 1.8. Le verrouillage technologique 35
- 1.9. Les technologies renforçant la protection de la vie privée 35
- 1.10. Les défis 36

Chapitre II. Gouvernance — présentation, défis, possibilités 39

- 2.1. L'environnement réglementaire dans le domaine de la sécurité
et de la surveillance 39
- 2.2. Droits de l'homme 39
 - 2.2.1. Droits de l'homme et vie privée 40
 - 2.2.2. La sécurité comme justification pour restreindre
la protection de la vie privée 42
 - 2.2.3. La sûreté en tant que droit de l'homme à part entière 43
- 2.3. Réglementation en matière de surveillance 45
 - 2.3.1. Jurisprudence 45
 - 2.3.2. Caméras de surveillance – vidéosurveillance 45
 - 2.3.3. Surveillance des télécommunications 49

2.4.	Domaines réglementaires spécifiques	50
2.4.1.	Protection des données	50
2.4.2.	Sûreté aérienne, contrôle des frontières, lutte contre la cybercriminalité	52
2.4.3.	Lancement d'alerte	56
2.4.4.	Drones	57
2.4.5.	Recherche	62
2.5.	Préoccupations, défis et possibilités réglementaires?	62
2.5.1.	Comment sont équilibrés les principes éthiques dans l'environnement réglementaire?	63
2.5.2.	Faut-il renforcer la réglementation?	63
2.5.3.	Comment relever les défis mondiaux?	64
2.5.4.	Quelles possibilités de gouvernance doivent être envisagées: la boîte à outils?	65
2.6.	Conclusion	66
Chapitre III. Analyse éthique		67
3.1.	Perspectives historiques et sociopolitiques	67
3.1.1.	L'évolution de la notion de sécurité	67
3.1.2.	Les tensions qui structurent la notion de sécurité ou qui s'y rattachent	71
3.2.	Préoccupations, considérations et concepts éthiques	72
3.2.1.	Sécurité, surveillance, peur et contrôle	72
3.2.2.	Contrôle, sécurité, protection	75
3.2.3.	Public et privé	78
3.3.	Principes éthiques	78
Chapitre IV. Sur la notion de compromis		85
4.1.	Équilibrer les droits	85
4.2.	Le compromis entre sécurité et liberté	86
4.3.	Le compromis entre «emploi et croissance» et «vie privée et liberté»	87
4.4.	Des alternatives aux compromis? Les concepts de «somme positive» et de «gagnant-gagnant»	88
4.5.	Des alternatives aux compromis? Les leçons sur la vie privée tirées des notifications et des consentements	89
4.6.	Au-delà du compromis	91
Recommandations		95
Recommendations		101
Empfehlungen		107



Groupe Européen
d'Éthique des Sciences
et des Nouvelles
Technologies

AVIS DU GROUPE EUROPÉEN D'ÉTHIQUE DES SCIENCES ET
DES NOUVELLES TECHNOLOGIES AUPRÈS DE LA COMMISSION
EUROPÉENNE

L'éthique des technologies de sécurité et de surveillance

Référence: Demande du président Barroso

Rapporteurs: Inez de Beaufort, Linda Nielsen,
Siobhán O'Sullivan

Jim Dratwa

Rédacteur en chef

28

Avis N°

Introduction

1.1. Portée de l'avis

Le 21 mars 2011, le président José Manuel Barroso a demandé au GEE de rédiger un avis sur les répercussions éthiques des technologies de l'information et de la communication et de préparer un avis consécutif et distinct sur les répercussions éthiques des technologies de sécurité, en accordant une attention appropriée au développement des technologies de sécurité et de surveillance. Le 22 février 2012, le GEE a remis à la Commission son avis sur l'éthique des technologies de l'information et de la communication. Il a également rédigé un avis sur la recherche, la production et l'utilisation de l'énergie qui a été publié le 16 janvier 2013, à la suite d'une demande présentée entre-temps par le président de la Commission. Le présent avis aborde les problématiques relatives aux technologies de sécurité et de surveillance d'un point de vue éthique. Au cours de la préparation du présent rapport par le GEE, les révélations d'Edward Snowden ont mis en évidence l'importance d'une réorganisation et d'une réinterprétation de notre approche à l'égard de la sécurité et de la surveillance. En effet, cet avis s'inscrit dans un contexte d'évolution auquel sont rattachées les difficultés liées aux flux de données et aux activités de surveillance mises sous les feux des projecteurs par ces révélations ⁽⁴⁵⁾.

La *sécurité nationale* relève de la responsabilité des États membres, mais le traité de Lisbonne et notamment la charte des droits fondamentaux qui y est inscrite prévoit un périmètre d'action pour l'Union européenne lorsque cela s'avère nécessaire afin de protéger les droits des citoyens. De plus, l'UE partage avec ses États membres des compétences relatives à la sécurité intérieure de l'Union et a élaboré une stratégie de sécurité intérieure pour recenser et coordonner les mesures de lutte contre les menaces communes. Dans le présent avis, nous présentons les façons dont la surveillance a pu être renforcée grâce à la disponibilité de nouvelles technologies et de moyens d'enregistrement, d'analyse et de stockage de volumes importants de données qui sont le résultat des progrès accomplis en matière de technologies de l'information et de la communication.

Tandis que les paradigmes de la *sécurité nationale* et de la *sécurité d'État* relèvent de la capacité des États à se défendre eux-mêmes contre les menaces extérieures, la notion de *sécurité des personnes* est fondée

sur la sécurité individuelle plutôt que sur la sécurité de l'État. Cette remarque doit être analysée à la lumière du contexte ayant trait aux formes de sécurité attendues d'un État-nation de type westphalien ⁽⁴⁶⁾ (dont le contrat social sous-jacent appelle l'État à garantir la sécurité de ses citoyens) et de l'attention accrue découlant de l'usage des technologies à l'égard du contrôle des frontières et de l'«ennemi intérieur».

Les procédures de sécurité relèvent du ressort de l'État qui, en outre, peut se procurer des services auprès de compagnies nationales ou internationales pour disposer des équipements de collecte et de gestion des informations nécessaires pour assurer ses services de sécurité. Les renseignements recueillis à propos de personnes physiques ou d'organisations peuvent dès lors être détenus par l'État dans le cadre d'un système de responsabilité démocratique qui devrait être établi ou par des entités privées. Dans ce dernier cas, les conditions de gestion des documents à caractère sensible ne sont pas forcément rattachées au domaine public et ces derniers peuvent être conservés ou utilisés plus largement que pour les besoins d'un État particulier.

Le présent avis expose les principes qui devraient régir ces formes de surveillance.

En outre, la surveillance de populations par des sociétés ou par d'autres personnes physiques devrait être soumise à des conditions et, une fois encore, **le présent avis expose les principes qui régissent ces formes de surveillance «commerciale» ou individuelle** et les conditions d'utilisation potentielle des données collectées dans le cadre d'un système de fouille ou de profilage de données par des entités privées ou des États.

La révolution numérique et les avancées consécutives relatives aux appareils mobiles, sans fil et en réseau ont grandement contribué au développement des technologies de sécurité et de surveillance. Les nouvelles technologies permettent d'enregistrer les activités quotidiennes de milliards d'individus dans le monde entier. Nos téléphones portables peuvent repérer et localiser notre emplacement à tout moment, les cartes de fidélité permettent aux entités commerciales d'analyser nos dépenses et de suivre l'évolution de nos préférences personnelles, les logiciels de saisie surveillent nos performances et notre productivité sur notre lieu de travail et nos communications électroniques peuvent être

⁽⁴⁵⁾ <http://www.theguardian.com/world/the-nsa-files>

⁽⁴⁶⁾ Paix de Westphalie, 1648.

INTRODUCTION

analysées par des services de renseignement utilisant des filtres par mots-clés ou expressions. De plus, des données à caractère personnel (santé, emploi, déplacements, communications électroniques) sont stockées dans des bases de données et des techniques de fouille permettent d'organiser et d'analyser des volumes très importants de données provenant de ces différentes sources, ce qui facilite la découverte de relations inédites entre ces données. Les technologies de sécurité ne sont plus cloisonnées et la tendance est à la convergence des technologies, ce qui entraîne la création de systèmes en réseau plus puissants. Par conséquent, un nombre d'acteurs jamais atteint auparavant scrute notre vie quotidienne, ce qui est une conséquence non seulement du progrès technologique mais aussi de certains choix politiques ou même parfois de leur absence.

1.2. Une définition de la sécurité

Si l'on part de sa définition, la notion particulière de «sécurité» peut tout d'abord paraître simple, familière et immédiate; mais elle peut aussi passer pour le parangon du «concept essentiellement controversé» de Gallie⁽⁴⁷⁾. En effet, la familiarité apparente de cette notion recouvre toute une série de tensions et d'oppositions importantes, qui sont ancrées historiquement et socio-politiquement et qui mettent en évidence les enjeux éthiques attachés à la sécurité. Ces derniers seront traités plus en détail au chapitre 3.

En vue d'adopter une démarche heuristique initiale sans détour et aux fins de la présente introduction, nous pouvons définir la notion de sécurité de la façon suivante: «protéger les individus et les valeurs de liberté et de démocratie pour que chacun puisse jouir d'une vie quotidienne sans crainte»⁽⁴⁸⁾.

1.3. Une définition de la surveillance

La notion de surveillance, comme celle de sécurité, est polysémique et donc ouverte à de nombreuses significations. Sa définition courante est la suivante: une observation étroite et plus particulièrement une démarche consistant à observer de façon rapprochée

un espion ou un criminel présumé ou encore un lieu où un incident est susceptible de survenir.

Ce substantif est dérivé du verbe français *surveiller* (XVI^e siècle), composé du préfixe *sur-* et du verbe *veiller*, ainsi que du latin *vigilare*, issu lui-même de *vigil* «attentif». Il est intéressant de noter que le verbe «surveiller» recouvrait dès son origine des significations ambivalentes (veiller sur quelqu'un, prendre soin de quelqu'un, faire preuve de méfiance et contrôler quelqu'un). Il recouvrait également dès son origine la notion complémentaire suivante: veiller sur soi et surveiller son propre comportement.

La première occurrence du terme «surveillance» apparaît en 1768, dans un article du journal économique *Ephémérides du citoyen*, faisant référence au rôle de la police sur les places des marchés, où interfèrent des individus, l'État, des intérêts privés et publics ainsi que les services répressifs et judiciaires. Il convient également de noter que le mot «surveillance» est entré dans la langue anglaise à l'époque de la Terreur en France: pendant la Révolution française, des «comités de surveillance» furent créés dans chaque commune par décret de la Convention, en vertu de la loi du 21 mars 1793, afin de surveiller les agissements et les déplacements de tous les étrangers, dissidents et individus suspects, afin de délivrer des certificats de citoyenneté.

Même si toutes les technologies de sécurité ne comprennent pas un volet de surveillance directe et si toutes les technologies de surveillance n'ont pas pour objectif déclaré la sécurité et alors que les termes eux-mêmes de «technologies de sécurité» et de «technologies de surveillance» sont soumis à des variations qui empêchent toute typologie et définition stables, l'approche classique veut que la surveillance soit présentée comme un moyen utilisé à des fins de sécurité.

Ces considérations seront analysées et explorées plus en détail au chapitre 1.

1.4. Les actions politiques de l'UE et le programme de Stockholm

Après l'entrée en vigueur du traité de Lisbonne, la communication de 2010 de la Commission [COM(2010) 673]⁽⁴⁹⁾, qui esquisse la stratégie de sécurité intérieure

⁽⁴⁷⁾ W.B. Gallie, «Essentially Contested Concepts», *Proceedings of the Aristotelian Society*, 1956, p. 167-198; article présenté à l'Aristotelian Society le 12 mars 1956.

⁽⁴⁸⁾ Conseil européen, 2010, Stratégie de sécurité intérieure pour l'Union européenne. Vers un modèle européen de sécurité, p. 12.

⁽⁴⁹⁾ La stratégie de sécurité intérieure de l'UE en action: cinq étapes vers une Europe plus sûre [Communication de la Commission COM(2010) 673]: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:FR:PDF>

de l'UE en s'inspirant du programme de Stockholm et de son plan d'action ⁽⁵⁰⁾, a recensé les défis perçus comme les plus urgents à relever dans le domaine de la sécurité de l'UE dans les années à venir. Elle propose ainsi cinq objectifs stratégiques et actions spécifiques pour la période 2011-2014 qui, parallèlement aux initiatives et efforts en cours, visent à renforcer la sécurité dans l'UE:

1. Perturber les réseaux criminels internationaux menaçant notre société
2. Prévenir le terrorisme et s'attaquer à la radicalisation et au recrutement de terroristes
3. Accroître le niveau de sécurité des citoyens et des entreprises dans le cyberspace
4. Renforcer la sécurité par la gestion des frontières
5. Renforcer la résilience de l'Europe aux crises et aux catastrophes

La communication de la Commission expose les justifications suivantes:

«La grande criminalité et la criminalité organisée prennent des formes diverses: la traite des êtres humains, le trafic de drogues, le trafic d'armes, le blanchiment d'argent, ainsi que le transfert et le déversement illégaux de déchets à l'intérieur ou en dehors de l'Europe. Même des infractions apparemment mineures, telles que les cambriolages, les vols de voiture, la vente de marchandises de contrefaçon ou dangereuses, et les délits commis par des gangs itinérants, reflètent bien souvent au niveau local l'existence de réseaux criminels internationaux. Ces infractions appellent une action européenne concertée. Cela vaut également pour le terrorisme: nos sociétés restent vulnérables aux attaques terroristes telles que les attentats à la bombe qui ont frappé les transports publics madrilènes et londoniens, respectivement en 2004 et en 2005.

⁽⁵⁰⁾ Le programme de Stockholm, qui succède aux programmes de Tampere et de La Haye, est le troisième programme pluriannuel de l'UE, couvrant la période 2010-2014, dans le domaine de la justice et des affaires intérieures. Le programme de Stockholm: Une Europe ouverte et sûre qui sert et protège les citoyens (document 17024/09 du Conseil); Mettre en place un espace de liberté, de sécurité et de justice au service des citoyens européens — Plan d'action mettant en œuvre le programme de Stockholm [Communication COM(2010) 171 de la Commission].

Nous devons redoubler d'efforts et coopérer plus étroitement pour éviter que de nouveaux attentats ne se produisent. La cybercriminalité constitue une autre menace croissante. L'Europe est une cible toute désignée pour la cybercriminalité en raison de son infrastructure internet avancée, de son grand nombre d'internautes et de ses transactions commerciales et systèmes de paiement utilisant l'internet. Il y a lieu de mieux protéger les citoyens, les entreprises, les administrations et les infrastructures critiques contre les formes de criminalité qui tirent parti des technologies modernes. La sécurité aux frontières exige également une action plus cohérente. Du fait des frontières extérieures communes, la contrebande et les autres types d'activité transfrontière illicite doivent être combattus au niveau européen. Un contrôle efficace aux frontières extérieures de l'UE est donc essentiel pour l'espace de libre circulation. En outre, nous avons observé ces dernières années une augmentation de la fréquence et de l'ampleur des catastrophes d'origine naturelle ou humaine en Europe et dans son voisinage immédiat. Cette situation a démontré la nécessité pour l'Union de se doter d'une capacité de réaction plus forte, plus cohérente et mieux intégrée en cas de crise ou de catastrophe, et d'appliquer la politique et la législation existant en matière de prévention des catastrophes.»

Ces cinq enjeux pris conjointement indiquent l'orientation politique actuelle de l'UE et soulignent ses difficultés en matière de «sécurité intérieure»: une série de menaces croissantes et convergentes qui nécessitent un renforcement de la sécurité sous l'égide d'un cadre européen coordonné. La stratégie de sécurité intérieure expose plusieurs orientations pour son action qui incluent une approche fondée sur l'échange dynamique de renseignements entre les services répressifs grâce à l'utilisation des bases de données de l'UE et à une coopération renforcée entre les agences de l'UE dans les domaines politiques de la justice et des affaires intérieures.

Pour comprendre la situation globale et le cadre général, il faut prendre comme repères les priorités politiques exposées dans le programme de Stockholm tel qu'il a été adopté en 2009. Il est également essentiel de souligner deux autres éléments contextuels: premièrement l'enthousiasme institutionnel qui prévalait durant la période englobant l'entrée en vigueur du traité de Lisbonne et deuxièmement le fait que la structure même des institutions de l'UE (au-delà du traité, notamment par l'organisation du Conseil et l'architecture de la Commission composée de directions générales) ont établi un lien étroit à ce moment-là entre «la liberté, la sécurité et la justice».

INTRODUCTION

Par conséquent, il faut citer l'introduction du programme de Stockholm, dans laquelle le Conseil européen «rappelle qu'il considère comme une priorité la mise en place d'un espace de liberté, de sécurité et de justice pour répondre à une préoccupation majeure des peuples des États réunis au sein de l'Union» et «note avec satisfaction que le Parlement européen et les parlements nationaux joueront un rôle accru à la suite de l'entrée en vigueur du traité de Lisbonne. Les citoyens et les associations représentatives auront davantage la possibilité de faire connaître et d'échanger publiquement leurs opinions dans tous les domaines d'action de l'Union, conformément à l'article 11 du traité UE, ce qui renforcera le caractère ouvert et démocratique de l'Union, dans l'intérêt de ses peuples.»

Le programme pluriannuel de Stockholm a constitué un tournant en matière de priorités politiques par rapport à son prédécesseur (le programme de La Haye). Il n'appelle plus à trouver un équilibre ni à établir un compromis entre la liberté et la sécurité. Il met les citoyens au cœur de son programme, en présentant ces deux concepts comme des éléments qui peuvent se renforcer mutuellement de la façon suivante: «Le Conseil européen considère que la priorité pour les années à venir sera la prise en compte des intérêts et des besoins des citoyens. Le défi sera de garantir le respect des droits et libertés fondamentales et l'intégrité de la personne, tout en assurant la sécurité en Europe. Il est primordial que les mesures répressives, d'une part, et les mesures permettant de préserver les droits de la personne, l'État de droit et les règles relatives à la protection internationale, d'autre part, aillent de pair et se renforcent mutuellement.»

Les priorités politiques exposées dans le programme de Stockholm sont les suivantes:

1. Promouvoir la citoyenneté et les droits fondamentaux (en accordant la priorité à la protection des libertés et des droits fondamentaux). «Le respect de la personne et de la dignité humaine ainsi que des autres droits énoncés dans la charte des droits fondamentaux de l'Union européenne et la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales constitue une valeur essentielle. Il s'agit, par exemple, de préserver l'exercice de ces droits et libertés, en particulier la vie privée des citoyens, au-delà des frontières nationales, notamment via la protection de leurs données à caractère personnel. Il s'agit également de prendre en compte les besoins particuliers des personnes vulnérables.»

2. Une Europe du droit et de la justice
3. Une Europe qui protège (en appelant à l'élaboration d'une stratégie de sécurité intérieure comme cela a été indiqué ci-dessus)
4. L'accès à l'Europe à l'heure de la mondialisation
5. Une Europe faisant preuve de responsabilité et de solidarité et travaillant en partenariat en matière d'immigration et d'asile
6. Le rôle de l'Europe à l'heure de la mondialisation — la dimension extérieure (en soulignant l'importance de la dimension extérieure de la politique de l'Union dans le domaine de la liberté, de la sécurité et de la justice en accordant une attention appropriée à la nécessité d'intégrer davantage ces actions dans les politiques générales de l'Union et dans tous les autres aspects de la politique étrangère de l'Union)

L'Union européenne se prépare actuellement à définir les grandes orientations politiques dans le domaine de la justice et des affaires intérieures pour les prochaines années et à fixer les «orientations stratégiques» prévues par le traité de Lisbonne, qui remplaceront le programme de Stockholm dont l'expiration est prévue fin 2014.

Dans ce contexte, le présent avis est également publié à un moment particulièrement opportun.

À la suite de cet avant-propos et de ces remarques introductives, le présent avis s'articule en quatre chapitres et expose en guise de conclusion des recommandations. Le premier chapitre fournit une vue d'ensemble et une analyse plus détaillée des applications des technologies de sécurité et de surveillance, le deuxième chapitre aborde de manière approfondie les aspects juridiques et réglementaires s'y rapportant et présente le contexte et les défis posés en matière de gouvernance. Le troisième chapitre fournit une analyse éthique, qui englobe les approches historiques et sociopolitiques, et examine les concepts, les considérations et les préoccupations éthiques. Le quatrième chapitre passe en revue les principales difficultés liées aux technologies de sécurité et de surveillance dans le domaine de l'éthique et fournit une approche pour les lever. Pour finir, des recommandations sont exposées.

Chapitre I. Applications des technologies de sécurité et de surveillance

La révolution numérique et les avancées consécutives relatives aux appareils mobiles, sans fil et en réseau et aux programmes d'exécution et de connexion de ces appareils ont grandement contribué au développement des technologies de sécurité et de surveillance. Les étiquettes d'identification par radiofréquence (RFID), les nanotechnologies et les technologies de l'information nous permettent d'enregistrer les activités quotidiennes de millions de citoyens européens. Nos téléphones portables peuvent repérer et localiser notre emplacement à tout moment, les cartes de fidélité permettent aux entités commerciales d'analyser nos dépenses et de suivre l'évolution de nos préférences personnelles, les logiciels de saisie surveillent nos performances et notre productivité sur notre lieu de travail et les communications électroniques peuvent être analysées par des services de renseignement en utilisant des filtres par mots-clés ou expressions. De plus, des données à caractère personnel (santé, emploi, déplacements, communications électroniques) sont stockées dans des bases de données et des techniques de fouille permettent d'organiser et d'analyser des volumes très importants de données provenant de ces différentes sources, ce qui facilite la découverte de relations inédites entre ces données. Les technologies de sécurité ne sont plus cloisonnées et la tendance est à la convergence des technologies, ce qui entraîne la création de systèmes en réseau plus puissants. Par conséquent, un nombre d'acteurs jamais atteint auparavant scrute notre vie quotidienne, ce qui est une conséquence du progrès technologique.

L'expression «technologies de sécurité et de surveillance» n'est pas tout à fait appropriée puisque les technologies abordées dans l'analyse suivante ont soit été conçues spécifiquement pour des motifs liés à la sécurité ou bien ont été conçues plus généralement pour d'autres motifs, qui ont trouvé indirectement des applications en matière de sécurité et/ou de surveillance. Il est donc difficile de fournir une définition spécifique des technologies de sécurité et il existe ainsi un lien étroit avec le concept de sécurité qui a été abordé. Les technologies de sécurité désignent aux fins de la présente discussion les technologies employées pour garantir ou améliorer la sécurité des personnes, des biens et des informations.

Le développement et la prolifération des technologies de sécurité et plus particulièrement des technologies de surveillance ont été facilités par les avancées dans plusieurs domaines scientifiques, notamment dans les domaines des télécommunications, de l'information, de l'informatique et du suivi de la localisation.

1.1. Les télécommunications

Au cours de ces trente dernières années, plusieurs évolutions technologiques ont émergé dans le domaine des télécommunications dont l'une des plus emblématiques est le passage à l'utilisation de signaux numériques, de câbles à fibres optiques et de systèmes de commutation informatique. Ces évolutions ont favorisé la création de diverses technologies, qui ont grandement accru les possibilités de surveillance des émissions de télécommunications et de leurs contenus. Les appareils à émission de fréquences radio ont rendu possible la téléphonie mobile accompagnée de son système de messagerie vocale, textuelle et vidéo et les câbles à fibres optiques ont quant à eux facilité les connexions internet à haut débit. L'informatique sans fil résulte de la convergence de ces deux technologies. Il est désormais possible de se connecter à internet à partir d'appareils et de téléphones portables et d'émettre des appels vocaux à partir d'ordinateurs de bureau à l'aide de logiciels de voix sur IP (VoIP), tels que Skype.

Interception des télécommunications

Toutes ces technologies nécessitent la transmission de données qui peuvent être capturées, stockées et analysées, et reliées à d'autres données à des fins de sécurité. Il a été avancé que la surveillance ciblée et l'interception des communications de personnes physiques jouent un rôle primordial pour préserver la sécurité nationale, enquêter sur des activités criminelles graves et même lutter contre le terrorisme. Les techniques manuelles d'écoutes téléphoniques à l'aide d'appareils tels que les équipements d'interception de communications qui enregistrent les numéros des appels sortants et entrants ont été remplacées par des technologies d'écoutes contrôlées à distance de centraux téléphoniques, qui permettent de collecter de grandes quantités de données de communications qui peuvent être filtrées et analysées. Les communications internet, qu'il s'agisse de l'envoi d'un message électronique, de la navigation sur le web ou de l'envoi d'un appel par VoIP, utilisent le protocole IP (*Internet Protocol*). Dans ce protocole, les informations transmises sont regroupées par paquets, qui peuvent être suivis par ce que l'on appelle des logiciels d'analyse de paquets («renifleur de paquets»). Un renifleur de paquets est un système similaire aux systèmes physiques de mise sur écoute des télécommunications. Il peut filtrer les informations en fonction de leur source ou de leur destination ainsi qu'en fonction du contenu des communications.

CHAPITRE I. | APPLICATIONS DES TECHNOLOGIES DE SÉCURITÉ ET DE SURVEILLANCE

Ces technologies ont facilité les opérations d'analyse de routine et automatisée des États de toutes les télécommunications de leurs citoyens afin de détecter des mots-clés ou des expressions et leur permettent d'être informés de l'accès à des ressources en ligne particulières. Depuis 2006, la directive européenne 2006/24/CE sur la conservation des données oblige les fournisseurs de télécommunications à stocker les communications pendant une période allant de six mois à deux ans, à des fins d'enquête pénale. En 2012, Microsoft et Skype ont reçu au total 75 378 demandes de renseignements de services répressifs ⁽⁵¹⁾. Ces demandes ont pu toucher 137 424 comptes. Environ 80 % des demandes déposées auprès de Microsoft ont entraîné la divulgation d'informations autres que des contenus et, dans un faible nombre de cas (2,2 % des demandes), des informations relatives à sa clientèle ont également été divulguées.

L'affaire Snowden

Les activités transnationales de surveillance d'État ont fait les gros titres à travers le monde en juin 2013 à la suite des révélations d'Edward Snowden, un ancien employé contractuel de l'agence de sécurité nationale américaine (*National Security Agency* ou NSA). La série de documents qui ont fait l'objet de ces fuites décrivait le fonctionnement du programme PRISM qui autorise l'interception, le stockage et l'analyse systématiques par la NSA d'environ onze catégories différentes de communications électroniques de citoyens autres que des citoyens américains auprès de compagnies téléphoniques et de multinationales du secteur de l'internet telles que Google, Apple, Microsoft et Facebook ⁽⁵²⁾ ⁽⁵³⁾. Il a été avancé que ce programme facilitait une vaste surveillance des communications stockées et émises en temps réel telles que les courriers électroniques, les transferts de fichiers et les discussions sur le web en accédant directement aux serveurs de ces entreprises. Des

allégations d'espionnage par la NSA de dirigeants du monde, de hauts responsables d'organisations d'aide internationale, de dirigeants des Nations unies, d'entreprises étrangères du secteur de l'énergie et du chef de la division de lutte contre les ententes et les abus de position dominante de l'Union européenne apparaissent toutes dans les documents divulgués par M. Snowden. Des documents ont également révélé l'existence du programme TEMPORA qui est dirigé par l'administration centrale des communications gouvernementales du Royaume-Uni (*Government Communications Headquarters* ou GCHQ). Il a été découvert que l'agence britannique apparentée à la NSA possédait depuis 2011 la capacité d'explorer et de stocker des volumes très importants de données provenant de câbles sous-marins de fibres optiques. Ces documents ont révélé que des dispositifs d'interception avaient été placés par la GCHQ sur 200 câbles de fibres optiques acheminant des communications internet entre les États-Unis et l'Europe, ce qui pouvait donner accès à l'administration à 10 gigabits de données par seconde, principalement sous la forme de métadonnées (c'est-à-dire à des connexions plutôt qu'à du contenu). Le journal *The Guardian* a souligné que cela «équivalait à l'envoi de toutes les informations de tous les ouvrages de la bibliothèque nationale britannique 192 fois toutes les 24 heures» ⁽⁵⁴⁾.

Il a été avancé que la distinction entre les contenus et les métadonnées n'était pas toujours claire. Même si les métadonnées ne contiennent généralement pas de détails personnels ni de détails spécifiques liés aux contenus mais plutôt des informations transactionnelles à propos des utilisateurs, elles peuvent toutefois divulguer des informations personnelles sensibles, par exemple les appels aux centres d'assistance technique par téléphone à propos de violences conjugales.

1.2. Les technologies de l'information et de la communication

Le développement spectaculaire de technologies de l'information et de la communication (TIC) aux performances élevées permet de collecter, de stocker et d'utiliser des volumes très importants de données à caractère personnel à l'aide de méthodes à la simplicité et à l'efficacité inédites. L'un des principaux catalyseurs de ce développement est la disponibilité

⁽⁵¹⁾ Rapport relatif aux demandes des services répressifs en 2012, <http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/>

⁽⁵²⁾ G. Greenwald, «NSA collecting phone records of millions of Verizon customers daily», *The Guardian*, 6 juin 2013: <http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order>

⁽⁵³⁾ B. Gellman et L. Poitras, «U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program», *Washington Post*, 6 juin 2013: http://www.washingtonpost.com/investigations/us-intel-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_print.html

⁽⁵⁴⁾ E. MacAskill et al., «GCHQ taps fibre-optic cables for secret access to world's communications», *The Guardian*, 21 juin 2013: <http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>

accrue de systèmes efficaces de stockage de données à bas coût. Parallèlement à la hausse de la capacité de stockage, les coûts s'y rapportant ont diminué de manière importante. Le volume de données à caractère personnel stockées dans des bases de données a considérablement augmenté au cours des trente dernières années, principalement en raison de l'explosion des données des médias sociaux et des données générées par des appareils, telles que les informations provenant de capteurs, de systèmes de point de vente, de réseaux de téléphonie mobile, de journaux de serveurs web et de sources similaires. Selon l'enquête mondiale relative à la sécurité des informations de 2012 d'Ernst & Young, à laquelle 1 850 personnes issues de tous les secteurs et réparties dans 64 pays ont participé, le nombre d'organisations utilisant la technologie de l'informatique en nuage a doublé depuis 2010 ⁽⁵⁵⁾. Cette adoption massive des services d'informatique en nuage, tels que les référentiels de fichiers en ligne, les services de partage de photos et les réseaux sociaux, génère d'énormes volumes de données et de métadonnées sur les citoyens. Différentes données peuvent désormais être accumulées et faire l'objet de recoupements et de références croisées dans de grandes bases de données à des fins commerciales, administratives, médicales et judiciaires. Roger Clarke a inventé l'expression «surveillance par les données» (*dataveillance* en anglais) pour décrire ces pratiques de surveillance de données à l'aide des traces laissées par les utilisateurs des médias numériques ⁽⁵⁶⁾.

Exploration et appariement de données

Les jeux de données peuvent faire l'objet d'appariements pour recenser des caractéristiques ou des tendances communes au sein de ces données. Les techniques d'appariement incluent le profilage géodémographique, dans le cadre duquel des données géographiques, par exemple un code postal ou des noms de domaine internet, sont associées à des données démographiques de personnes physiques.

Les organisations privées et publiques ont de plus en plus recours aux techniques d'appariement de données pour réduire les activités frauduleuses. Pour

limiter les demandes de prestations sociales frauduleuses, des administrations publiques comparent des données stockées dans différentes bases de données pour détecter les analogies et les différences entre les données collectées à différentes fins, par exemple pour déterminer si une personne paye des impôts sur le revenu et présente dans le même temps une demande de prestations de sécurité sociale ou si une personne décédée dépose une demande d'allocations. Les institutions financières peuvent croiser des données sur des comptes, des cartes bancaires, des plafonds de crédits et des soldes moyens pour procéder à des évaluations de solvabilité et ainsi réduire leurs risques financiers.

L'exploration de données permet d'organiser et d'analyser de grandes quantités de données à caractère personnel provenant de sources disparates, ce qui facilite la découverte de relations auparavant inédites parmi les données concernées. L'extraction de connaissances à partir de bases de données (*Knowledge Discovery in Databases* ou KDD) est un processus heuristique d'exploration de données qui a évolué depuis la convergence de l'apprentissage automatique, des systèmes de base de données, des statistiques et de l'intelligence artificielle. Il s'agit d'un processus composé de plusieurs étapes qui facilite la conversion de grands volumes de données en renseignements valides, inédits, potentiellement utiles et au bout du compte compréhensibles. L'exploration de données est une technique employée pour détecter de nouveaux effets indésirables de médicaments après leur homologation et au cours de leur mise sur le marché pour améliorer la sécurité des patients ⁽⁵⁷⁾. Le projet EU-ADR qui est financé par la Commission européenne a pour objet l'exploration de données cliniques issues de bases de données biomédicales et de dossiers médicaux informatisés (DMI) de plus de 30 millions de patients de plusieurs pays européens afin de dépister de manière précoce les effets indésirables de médicaments, ce qui devrait renforcer la surveillance de la sécurité des médicaments ⁽⁵⁸⁾. Il a également été suggéré que l'exploration de dossiers médicaux informatisés pourrait être utile pour soutenir la recherche médicale et les soins cliniques, par exemple pour surveiller l'observance des traitements ⁽⁵⁹⁾. La mise en relation de données génétiques et de dossiers médicaux informatisés permet d'établir

⁽⁵⁵⁾ Ernst & Young, Enquête mondiale relative à la sécurité des informations (2012).[http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/\\$FILE/2012_Global_Information_Security_Survey____Fighting_to_close_the_gap.pdf](http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey____Fighting_to_close_the_gap.pdf)

⁽⁵⁶⁾ Clarke R., «Communication technology and dataveillance», communications de l'ACM, 1988;31(5): p. 498-512.

⁽⁵⁷⁾ Harpaz R. et al., *Clinical Pharmacology & Therapeutics*, 2012; 91(6): p. 1010-1021.

⁽⁵⁸⁾ Coloma P.M. et al., *Pharmacoepidemiology and Drug Safety*, 2011;20(1): p. 1-11.

⁽⁵⁹⁾ Jensen P.B. et al., *Nature Reviews Genetics*, 2012;13: p. 395-405.

CHAPITRE I. | APPLICATIONS DES TECHNOLOGIES DE SÉCURITÉ ET DE SURVEILLANCE

des corrélations génotypes/phénotypes. Une étude dans ce domaine a permis de recenser des variants génétiques associés à un risque accru de thrombo-embolie chez des patients souffrant d'un cancer du sein qui suivent un traitement au Tamoxifen ⁽⁶⁰⁾. L'exploration de données a également été utilisée récemment pour la surveillance d'épidémies ⁽⁶¹⁾. Des chercheurs ont par exemple démontré que l'«exploration» de messages sur Twitter peut être utilisée pour effectuer un suivi des foyers de grippe et prévoir leur apparition avec une précision d'environ 90 % ⁽⁶²⁾.

Les sociétés commerciales adoptent de plus en plus des modèles d'activité fondés sur l'exploration de données. On constate qu'elles ont tendance à vouloir comprendre les besoins individuels de leurs clients et à tirer parti de ces renseignements pour fournir des produits et/ou des services sur mesure, ce qui accroît leur rentabilité et la fidélisation de la clientèle. L'exploration de données est utilisée pour analyser les tendances des ventes et prévoir l'efficacité des promotions. L'industrie de la vente au détail analyse les paniers pour déterminer les produits qui sont achetés ensemble afin de les disposer sur les étagères en fonction de ces informations. Les entreprises de vente au détail et les experts en marketing peuvent utiliser les techniques d'exploration de données pour mieux comprendre les profils et les comportements des clients. Grâce à l'exploration de données, il est possible de segmenter les bases de données de clients en fonction de données démographiques, d'habitudes d'achat, de données

géographiques, d'attitudes et d'autres variables. Il est ainsi possible de définir des profils d'achat en fonction des préférences des clients et d'élaborer des approches commerciales plus spécifiques pour un groupe de clients plus restreint. Amazon, l'entreprise de vente au détail en ligne, utilise plusieurs sources de données pour déterminer à l'avance les préférences probables de ses clients et proposer des «recommandations» d'articles aux consommateurs. Target, une entreprise américaine de vente au détail, utilise l'analyse prédictive pour commercialiser de manière efficace ses produits auprès de ses clientes enceintes. Grâce à l'analyse de l'historique des habitudes d'achat de femmes ayant créé une liste de naissance, environ 25 produits, tels que des compléments en vitamines et des lotions non parfumées, ont pu être recensés et permettraient de manière conjointe d'établir une note de prévision de grossesse. Selon la note obtenue, des bons d'achat de produits pour bébés sont envoyés aux clientes. L'utilisation de cette technique de commercialisation directe par anticipation auprès d'une jeune femme qui avait reçu ces bons d'achat par voie postale à son domicile a eu l'effet inverse de l'effet recherché. Son père a contacté l'entreprise pour lui faire part de son indignation à propos de l'envoi de publicités d'équipements pour bébés à sa fille qui était adolescente. L'entreprise lui a immédiatement présenté ses excuses mais cet homme l'a ensuite contactée une semaine plus tard pour lui faire lui-même ses excuses puisque sa fille lui avait confié qu'elle était bien enceinte ⁽⁶³⁾.

⁽⁶⁰⁾ Onitilo A. et al., *Breast Cancer Research and Treatment*, 2009;115: p. 643-650.

⁽⁶¹⁾ Kofod-Petersen A., *Medical Journal of Australia* «Machine learning and data mining for epidemic surveillance», 19 mars 2012;196(5): p. 301.

⁽⁶²⁾ Lamos V. et al., «Proceedings of the 2nd IAPR workshop on cognitive information processing», IEEE Press, 2010: p. 411-416.

⁽⁶³⁾ <http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/>

Analyse prédictive

L'analyse prédictive est une technique dérivée de l'exploration de données qui permet de modéliser des relations ou des interactions complexes à partir d'informations existantes pour recenser ou caractériser de nouvelles relations et/ou anticiper des événements. Le secteur commercial utilise cette technique depuis de nombreuses années pour anticiper des tendances ou l'état du marché et orienter des stratégies de vente. Les milieux du renseignement, de la lutte antiterroriste, de la sécurité nationale et des forces de l'ordre ont plus récemment adopté des technologies et des techniques d'exploration de données et d'analyse prédictive.

Time Magazine a proclamé que la «criminologie prédictive» était l'une des cinquante plus grandes inventions de l'année 2011. La compilation et l'analyse de volumes importants de jeux de données issus de sources disparates peuvent donner les moyens aux forces de police d'anticiper et de prévenir les actes criminels et d'intervenir de manière plus efficace. Il est avancé que l'affectation de ressources et le déploiement de forces de l'ordre à partir de l'analyse de ces données constituent une mesure rentable qui renforce la sécurité publique. L'expression «criminologie prédictive» n'est pas sans rappeler *The Minority Report*, une nouvelle de fiction qui a été publiée en 1956 dont l'histoire se déroule dans une société futuriste au sein de laquelle les délinquants sont arrêtés et punis avant d'avoir commis leurs délits. Les méthodes de criminologie prédictive ne permettent pas d'identifier des personnes physiques mais plutôt de détecter des tendances et des modèles sur le plan géographique et dans le temps. Dans les modèles complexes de criminologie prédictive, les informations historiques sur les délits, y compris le lieu, l'heure de la journée, les conditions météorologiques, la proximité géographique des DAB, etc., sont combinées avec des informations en temps réel et des données sociologiques à propos de comportements criminels, telles que la victimisation répétée et le fait que les délinquants ont tendance à commettre leurs délits dans leur environnement immédiat. La modélisation mathématique permet de fournir des informations sur la probabilité d'occurrence d'un délit donné, par exemple un cambriolage dans un lieu particulier, c'est-à-dire un «point névralgique» comme on l'appelle. Elle permet également de découvrir de nouvelles relations, comme dans le cas de viols commis par un étranger pour lesquels les antécédents judiciaires constituaient un facteur fiable de prédiction. Il est intéressant de remarquer que l'analyse prédictive a mis en évidence un résultat surprenant à ce sujet: un antécédent de délit contre des biens s'est révélé être un meilleur facteur de prédiction des viols par un étranger qu'un antécédent d'infraction à caractère sexuel ⁽⁶⁴⁾.

La criminologie prédictive a été expérimentée aux États-Unis et plus récemment au Royaume-Uni et aux Pays-Bas. Au moment de l'adoption de cette technique en 2011 à Santa Cruz en Californie, une baisse de 27 % des cambriolages a été constatée par rapport à l'année précédente. Quatre mois après le déploiement de la criminologie prédictive dans la vallée de Los Angeles fin 2011, les délits avaient diminué de 13 % alors qu'ils avaient augmenté de 0,4 % dans les secteurs environnants dans lesquels ce système n'avait pas été déployé ⁽⁶⁵⁾. Il est difficile de déterminer le degré d'efficacité de l'analyse prédictive dans le maintien de l'ordre puisque les causes de la criminalité sont complexes et multifactorielles et l'effet de l'analyse prédictive doit être distingué d'autres facteurs ayant une incidence sur la baisse de la criminalité, comme le vieillissement de la population. Les informations générées par l'analyse prédictive dépendent de la qualité des données utilisées dans l'analyse et plus ces données sont complètes, plus le pouvoir de prédiction est important. Il est connu que certains délits tels que les vols de véhicules sont plus systématiquement signalés que les activités liées aux stupéfiants et que certains groupes sociaux signalent davantage les délits par rapport à d'autres groupes de la population. D'autres préoccupations ont également été exprimées à propos du fait que ce type d'analyse pourrait instaurer une approche partielle dans le système de justice pénale en perpétuant un cycle de prévision autoproductrice d'accroissement des arrestations dans les secteurs recensés en tant que points névralgiques. Les magistrats et les jurés pourraient également être plus enclins à condamner les personnes que l'on suspecte d'être actives dans les secteurs à fort taux de criminalité. Cette approche est encore plus problématique lorsque la prédiction ne porte pas sur les lieux mais sur les individus. Des services pénitentiaires au Royaume-Uni utilisent l'analyse prédictive pour identifier les délinquants qui

⁽⁶⁴⁾ Coleen McQue, «Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis», 2006, Elsevier/ Butterworth-Heinemann.

⁽⁶⁵⁾ <http://www.predpol.com/results/> consulté le 27 août 2013.

CHAPITRE I. | APPLICATIONS DES TECHNOLOGIES DE SÉCURITÉ ET DE SURVEILLANCE

présentent les risques de récidive les plus élevés après leur sortie de prison ⁽⁶⁶⁾. Des millions de fichiers de détenus ont été analysés pour déterminer à l'avance si les délinquants qui sont confrontés à des difficultés particulières, telles que la toxicomanie, présentent des risques de récidive plus élevés par rapport à d'autres détenus. Des programmes ciblés sont alors conçus pour prendre en charge le comportement de délinquants pendant leur période de détention dans l'optique de réduire le risque de récidive à leur sortie. Des algorithmes ont également été élaborés pour calculer la probabilité qu'un individu en liberté conditionnelle ou en période de probation commette un homicide au cours des deux années faisant suite à sa libération ⁽⁶⁷⁾. Richard Berk, professeur de criminologie et de statistiques à l'université de Pennsylvanie, a analysé les données de plus de 60 000 affaires de délinquants qui avaient déjà été condamnés ou mis en liberté conditionnelle. Selon les prévisions de cet algorithme, entre 1 et 2 % des individus en liberté conditionnelle ou en période de probation allaient être accusés de meurtre ou de tentative de meurtre au cours des deux années à venir. «L'algorithme est capable d'identifier les individus qui utiliseront une arme à feu dans 75 % des cas», déclare le professeur Berk ⁽⁶⁸⁾. L'évaluation du niveau de «dangerosité a posteriori» à l'aide d'applications logicielles est utilisée au cours des audiences de détermination des peines et des libérations conditionnelles pour déterminer quels individus peuvent être libérés ainsi que leurs conditions/niveaux de contrôle.

L'analyse prédictive est également utilisée pour garantir la sécurité aux frontières. Des modèles de prévision mathématique sont utilisés pour déterminer à l'avance quels conteneurs entrant dans un port sont susceptibles de transporter des substances dangereuses, quels passagers d'un aéroport devraient être arrêtés et fouillés et quels véhicules franchissant les frontières paraissent suspects. Les informations relatives au type de véhicule, à son propriétaire et à l'historique de franchissement des frontières ainsi que des données géographiques et météorologiques sont utilisées pour concevoir des modèles d'identification de certains véhicules destinés à l'inspection. Les forces de police frontalière peuvent même disposer d'informations sur le risque le plus élevé en cas d'inspection (comme la présence de stupéfiants ou d'armes) ⁽⁶⁹⁾. Le ministère américain de la sécurité intérieure a mené des tests de logiciels qui ont été développés pour analyser les groupes d'individus dans les files d'attente d'aéroports afin de détecter les comportements suspects ou nerveux, tels que les signes d'impatience, de transpiration et de respiration peu profonde. L'analyse prédictive, qui est au cœur du programme FAST (pour *Future Attribute Screening Technology*), enregistre actuellement un résultat de 78 % de détection des intentions délictueuses et de 80 % de détection des mensonges ⁽⁷⁰⁾. La Commission européenne finance également des travaux de recherche sur la détection de comportements anormaux ou menaçants au titre du septième programme-cadre relatif à la sécurité. Le projet INDECT a pour objet d'élaborer des algorithmes innovants et sophistiqués pour appuyer l'aide à la décision humaine dans la lutte contre le terrorisme et d'autres activités criminelles, telles que la traite des êtres humains, la pédopornographie, la détection de situations dangereuses (par exemple les vols) et l'utilisation d'objets dangereux (comme les couteaux ou les armes à feu) dans les lieux publics ⁽⁷¹⁾. De la même façon, le projet ADABTS vise à mettre au point des modèles de comportements anormaux ou menaçants ainsi que des algorithmes de détection automatique de ces comportements dans les lieux très fréquentés ⁽⁷²⁾.

Des efforts sont menés pour anticiper les actes terroristes à l'aide de statistiques, mais ceux-ci sont rendus compliqués par le fait que la plupart des modèles prédictifs s'appuient sur des jeux de données très importants ⁽⁷³⁾.

⁽⁶⁶⁾ http://www.01.ibm.com/software/success/cssdb.nsf/CS/GREE8F8M82?OpenDocument&Site=default&cty=en_us consulté le 27 août 2013.

⁽⁶⁷⁾ Berk R. et al., *Journal of the Royal Statistical Society, A*, 2009:172(1): p. 191-211.

⁽⁶⁸⁾ <http://www.smartplanet.com/blog/science-scope/in-philadelphia-prediction-and-probability-in-crime-patterns/3598> consulté le 27 août 2013.

⁽⁶⁹⁾ <http://public.dhe.ibm.com/common/ssi/ecm/en/ytw03024gben/YTW03024GBEN.PDF> consulté le 27 août 2013.

⁽⁷⁰⁾ http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_fast-a.pdf consulté le 27 août 2013.

⁽⁷¹⁾ <http://www.indect-project.eu/> consulté le 27 août 2013.

⁽⁷²⁾ ftp://ftp.cordis.europa.eu/pub/fp7/security/docs/adabts_en.pdf consulté le 27 août 2013.

⁽⁷³⁾ Jonas J. et Harper T., «Effective Counterterrorism and the Limited Role of Predictive Data Mining», Cato Institute, document stratégique n° 584 2006 <http://object.cato.org/sites/cato.org/files/pubs/pdf/pa584.pdf> consulté le 27 août 2013.

Contrairement aux habitudes d'achat des consommateurs et à la fraude financière, la fréquence des actes terroristes est insuffisante pour créer des modèles prédictifs valables. L'analyse prédictive peut jouer un rôle important dans un domaine relatif à la lutte contre le terrorisme, à savoir la détection d'activités de blanchiment d'argent ⁽⁷⁴⁾. Les terroristes, leurs réseaux et leurs structures de soutien ont besoin de financements sous une forme ou sous une autre pour exister et mener à bien leurs opérations. Les modèles prédictifs sont capables de détecter des transactions financières inhabituelles ou suspectes et, selon le vieil adage, il faut «suivre l'argent à la trace» pour détecter les sources de financement du terrorisme.

Il ne fait aucun doute que l'analyse des données en masse (*Big data*) révolutionne notre approche en matière de sécurité et de surveillance et offre de nombreux avantages potentiels à une période au cours de laquelle le raz-de-marée virtuel d'informations disponibles à propos de presque chaque aspect de notre vie nécessite de nouvelles méthodologies pour réussir à les interpréter. Il convient toutefois de formuler un avertissement à ce sujet. Cukier et Mayer-Schönberger, auteurs de l'ouvrage *Big Data*, conseillent de manière judicieuse de ne pas accorder une trop grande importance aux données en rappelant à quel point Icare était émerveillé par sa capacité technique à voler, dont l'utilisation inappropriée a entraîné sa chute dans la mer ⁽⁷⁵⁾.

⁽⁷⁴⁾ Le Khac N.A. et al., conférence internationale sur les applications et l'ingénierie informatiques (2009), IPCSIT, 2011;2: p. 504-509.

⁽⁷⁵⁾ Mayer-Schönberger V. et Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Eamon Dolan/Houghton Mifflin Harcourt, 2013).

CHAPITRE I. | APPLICATIONS DES TECHNOLOGIES DE SÉCURITÉ ET DE SURVEILLANCE

La biométrie

Les innovations technologiques dans le domaine des TIC ont ouvert de nouvelles possibilités de création, de gestion et d'utilisation de systèmes d'identification. On compte parmi celles-ci les identificateurs biométriques qui peuvent être définis comme des caractéristiques ou des traits physiques ou physiologiques mesurables, dont l'utilisation permet d'identifier une personne physique ou de vérifier l'identité revendiquée par cette personne. Ces identificateurs biométriques physiologiques peuvent être les empreintes digitales, la géométrie des mains, le visage et l'iris. Les identificateurs biométriques comportementaux incluent la voix, la dynamique de frappe au clavier et la démarche. L'utilisation de l'ADN en tant qu'identificateur biométrique est intéressante puisqu'il s'agit d'un identificateur unique (sauf dans le cas des vrais jumeaux). De plus, la structure de l'ADN d'une personne est stable tout au long de sa vie ⁽⁷⁶⁾. La création d'un profil ADN inclut l'analyse de séquences courtes répétées en tandem d'ADN dit non codant. L'identification fondée sur l'ADN est principalement utilisée pour les tests de paternité, les enquêtes criminelles et la criminalistique. Actuellement, l'utilisation de l'ADN en tant qu'identificateur biométrique est limitée par le fait que la reconnaissance automatique en temps réel n'est pas encore possible. L'utilisation des technologies les plus récentes permet de créer un profil ADN en 90 minutes ⁽⁷⁷⁾. Les ministères américains de la défense, de la justice et de la sécurité intérieure financent des travaux de recherche dans le cadre de leur programme *Accelerated Nuclear DNA Equipment* pour mettre au point des technologies de création rapide et automatisée de profils ADN à des fins d'application biométrique sur le terrain ⁽⁷⁸⁾.

Le profilage ADN

Le profilage ADN est un outil important pour la criminologie qui peut contribuer à déterminer la culpabilité d'auteurs de délits ou inversement à innocenter les personnes accusées à tort. Un nombre croissant de pays (environ 60) à travers le monde exploitent des bases de données ADN à l'échelle nationale. De plus, des bases de données sont créées ou complétées dans au

moins 34 autres pays ⁽⁷⁹⁾. Les bases de données ADN diffèrent selon la catégorie de personnes physiques qui y sont incluses et selon les utilisations autorisées des bases elles-mêmes. Plus de 10 581 700 profils de délinquants, 1 641 400 profils de personnes appréhendées et 514 700 profils de criminalistique étaient recensés en septembre 2013 dans l'index ADN des États-Unis ⁽⁸⁰⁾. Les profils ADN sont fondés sur des séquences courtes répétées en tandem et ne correspondent pas aux séquences complètes du génome. On observe en revanche un accroissement du stockage d'échantillons d'ADN et de séquences complètes de génomes dans des banques de données biologiques. Il est reconnu que les banques de données biologiques constituent des infrastructures cruciales pour la recherche, ce qui a entraîné une forte hausse du nombre de banques spécifiques à certaines maladies ou catégories de populations en Europe et dans le monde ⁽⁸¹⁾. La banque de données biologiques du Royaume-Uni, qui a autorisé des chercheurs à y accéder en 2012, comprend actuellement des échantillons et des données de 500 000 personnes physiques ⁽⁸²⁾.

L'ADN est un identificateur différent des empreintes digitales et des autres identificateurs biométriques puisqu'il permet de fournir des informations à propos de l'appartenance ethnique ou des prédispositions à certaines pathologies et peut surtout être utilisé pour identifier d'autres membres de la famille de l'individu concerné. Le stockage de l'ADN recueilli auprès de personnes physiques et l'inclusion de profils ADN informatisés dans des bases de données informatiques laissent présager l'émergence de capacités de suivi et d'analyse bien plus intrusives au fur et à mesure du développement des avancées technologiques. En janvier 2013, des chercheurs ont signalé qu'ils avaient réussi à identifier des personnes physiques ainsi que leurs familles à partir de données ADN anonymes dans le cadre d'un projet fondé sur l'utilisation d'informations issues de bases de données généalogiques accessibles au public ⁽⁸³⁾. Ainsi, l'ADN est un identificateur de facto, ce qui soulève des questions à propos des moyens tradition-

⁽⁷⁶⁾ Hashiyada Masaki, *The Tohoku Journal of Experimental Medicine*, 2004;204(2): p. 109-117.

⁽⁷⁷⁾ <http://integenx.com/integenx-raises-40-million>

⁽⁷⁸⁾ <http://biometrics.org/bc2010/presentations/RapidDNA/files-DHS-Rapid-and-Low-cost-DNA-Biometrics.pdf>

⁽⁷⁹⁾ Initiative de criminalistique génétique <http://dnapolicyinitiative.org/>

⁽⁸⁰⁾ Statistiques CODIS-NDIS du FBI <http://www.fbi.gov/about-us/lab/biometric-analysis/codis/ndis-statistics>

⁽⁸¹⁾ http://www.eurosfair.prdd.fr/7pc/doc/1280153287_bio-banks_eu_jrc57831.pdf

⁽⁸²⁾ <http://www.ukbiobank.ac.uk/about-biobank-uk/>

⁽⁸³⁾ M. Gymrek et al., *Science*, 2013; p. 339, 321-324.

nels de protection de la vie privée, tels que le codage et l'anonymisation des données dans le domaine de la recherche clinique.

Partout où nous allons, nous laissons involontairement derrière nous des traces d'ADN présent dans nos cheveux, nos cellules cutanées et notre salive. Cette forme de biosurveillance peut être utilisée pour déterminer où nous sommes allés, savoir qui était avec nous et établir notre apparence.

Les identificateurs biométriques peuvent être utilisés à des fins de vérification: le système biométrique permet de confirmer l'identité revendiquée par un individu en comparant des échantillons de données biométriques avec le modèle correspondant qui a fait l'objet d'une inscription. Cela s'appelle la comparaison entre deux éléments. Les identificateurs biométriques peuvent également être utilisés à des fins d'identification. On peut ainsi connaître l'identité d'une personne physique en comparant des échantillons de données biométriques avec tous les modèles d'une base de données, c'est-à-dire en procédant à des comparaisons avec un grand nombre d'échantillons. Les données biométriques, par exemple les empreintes digitales, sont recueillies à l'aide d'un capteur pour créer une représentation numérique des données, qui sont reliées par la suite à l'identité de l'utilisateur et stockées sous la forme de données numériques (modèle) dans une base de données. Ce modèle peut être comparé aux données biométriques «vivantes» présentées à l'aide d'un algorithme mathématique, qui évalue le degré de similitude entre deux modèles. Les systèmes biométriques, qu'ils soient utilisés à des fins de vérification ou d'identification, peuvent être utilisés dans différents contextes, par exemple pour la sécurité, la surveillance et l'application de la loi, le commerce électronique, l'administration en ligne ainsi que l'accès physique et logique, comme l'accès d'enfants dans des établissements scolaires.

Les identificateurs biométriques et l'identification

De plus en plus de gouvernements cherchent à adopter de nouvelles technologies, telles que les identificateurs biométriques, pour vérifier ou déterminer des identités, comme les passeports, et pour surveiller la circulation transfrontalière des personnes physiques. En 2004, l'UE a adopté un règlement instaurant l'inclusion de données biométriques dans les passeports des citoyens de l'UE (à l'exception du Royaume-Uni et de l'Irlande) et les

visas des ressortissants de pays tiers⁽⁸⁴⁾. En vertu de ce règlement, les États membres étaient tenus de veiller à ce que tous les passeports délivrés contiennent une puce avec l'image faciale et les empreintes digitales de son détenteur d'ici 2006 et 2009 respectivement afin d'améliorer la sécurité des documents et d'éviter la falsification de documents. Les passeports biométriques (passeports électroniques) contiennent une petite puce [une puce d'identification par radiofréquence (RFID)], qui est intégrée sur la page de la photographie. Elle inclut la version numérisée de la photographie sur le passeport, un modèle d'empreintes digitales, ainsi que toutes les informations biographiques visibles sur le passeport.

Au sein de l'UE, le système d'information Schengen (SIS II), la base de données Eurodac et le système d'information sur les visas (VIS) sont des bases de données volumineuses qui incluent des données biométriques. Elles ont été conçues pour contrôler les flux migratoires mais également pour identifier et trier les migrants en situation régulière ou irrégulière. Le système Eurodac, qui est opérationnel depuis 2003, a été mis en œuvre pour comparer les empreintes digitales de demandeurs d'asile et d'immigrants en situation irrégulière dans l'UE afin de déterminer quel État membre est responsable de l'examen de la demande d'asile. VIS est un élément central du processus de dépôt des demandes de visas dans l'espace Schengen et permet aux États de cet espace de stocker et d'échanger des données relatives au dépôt des demandes de visas de ressortissants de pays tiers. Au total, cela correspond à la collecte de dix empreintes digitales et d'une photographie numérique des personnes de plus de 12 ans qui déposent une demande de visa dans l'UE. Ces données biométriques et les données fournies dans le formulaire de demande sont consignées dans une base de données centrale sécurisée⁽⁸⁵⁾. Le système d'information Schengen de deuxième génération (SIS II) a été mis en service le 9 avril 2013. SIS II inclut des données relatives aux migrants en situation irrégulière, aux documents de voyage perdus ou falsifiés et aux personnes recherchées ou

⁽⁸⁴⁾ Règlement (CE) n° 2252/2004 du Conseil établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2004R2252:20090626:FR:PDF>

⁽⁸⁵⁾ Proposition de règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour COM(2004) 835.

CHAPITRE I. | APPLICATIONS DES TECHNOLOGIES DE SÉCURITÉ ET DE SURVEILLANCE

disparues et stocke des images numériques et des données biométriques ⁽⁸⁶⁾.

L'identité d'une personne physique était traditionnellement confirmée à partir de son nom et par la suite à partir de documents d'identité, tels que les certificats de naissance, les passeports et les cartes d'identité nationale. Dans un contexte de mondialisation dans lequel les progrès en matière de modes de transport, de communication et de TIC ont favorisé les interconnexions, les personnes physiques sont davantage tenues de prouver leur identité ⁽⁸⁷⁾. D'après une analyse de l'UNICEF, près de deux enfants sur trois en Afrique subsaharienne et en Asie du Sud n'ont pas été inscrits sur des registres de naissance ⁽⁸⁸⁾. Il est important d'être en mesure de prouver son identité car cette démarche est un préalable indispensable pour accéder à certains services, tels que des services financiers, ou pour exercer des droits, comme le droit de vote. Plusieurs programmes mis en place dans des pays en développement ont pour ambition de passer directement à l'utilisation de technologies d'identification biométrique sans utiliser de systèmes traditionnels d'identification par le papier ⁽⁸⁹⁾. Le système indien de «numéro national d'identification unique» est le plus grand projet mondial de technologie biométrique ⁽⁹⁰⁾. Ce programme indien d'identification universelle vise à fournir une identité unique à chacun de ses habitants, soit 1,2 milliard d'individus. Au 31 mars 2013, l'organisme indien chargé du système d'identification unique avait utilisé des identificateurs biométriques (10 empreintes digitales et des analyses d'iris des deux yeux) pour générer au total 311,9 millions de numéros d'identification unique, également connus sous le nom de numéros d'Aadhaar ⁽⁹¹⁾. En fournissant un numéro unique à ses citoyens, le gouvernement indien espère simplifier la prestation des allocations et des services sociaux.

⁽⁸⁶⁾ http://europa.eu/rapid/press-release_MEMO-13-309_fr.htm

⁽⁸⁷⁾ Mordini E. et Massari S., *Bioethics*, 2008;22(9): p. 488-498.

⁽⁸⁸⁾ http://www.unicef.org/protection/files/Progress_for_Children-No.8_EN_081309%281%29.pdf

⁽⁸⁹⁾ Alan Gelb et Julia Clark, Center for Global Development, document de travail 315, janvier 2013. http://international.cgdev.org/sites/default/files/1426862_file_Biometric_ID_for_Development.pdf

⁽⁹⁰⁾ Jacobsen E.K.U., *Security Dialogue*, 2012;43(5): p. 457-474.

⁽⁹¹⁾ <http://pib.nic.in/newsite/erelease.aspx?relid=94946>

1.3. Les technologies de localisation et de suivi

Les innovations technologiques en matière de systèmes d'information géographique (SIG), tels que les systèmes d'identification par radiofréquence (RFID) et de positionnement à capacité globale (GPS), nous permettent de localiser des personnes physiques et des biens et de suivre leurs déplacements. Il existe un vaste éventail de systèmes de navigation et de suivi mais ces derniers utilisent principalement des techniques de triangulation, de détection de proximité et d'analyse de scène ⁽⁹²⁾.

Le système de positionnement à capacité globale

Le système de positionnement à capacité globale (GPS, *Global Positioning System*) est un système de radionavigation mondiale qui est composé d'une constellation de 31 satellites et de leurs stations terrestres. Ce système, qui a été créé par le ministère américain de la défense dans les années 70, est devenu entièrement opérationnel au milieu des années 90. Les technologies GPS facilitent la collecte d'informations de localisation en permettant de localiser de manière précise les appareils (téléphones portables, véhicules, dispositifs de cartographie électronique, etc.) à l'aide de données de référence issues de différentes sources, notamment de signaux radio de référencement d'emplacement GPS provenant de satellites en orbite autour de la terre. Ce système fonctionne par triangulation, en faisant correspondre trois signaux distincts ou plus à partir d'une sélection de satellites de suivi.

Le récepteur GPS utilise le signal d'un quatrième satellite pour déterminer l'altitude, ce qui permet d'établir une position en trois dimensions. Les données sont transmises en continu par les satellites GPS au récepteur GPS qui collecte et stocke les données. De plus en plus de dispositifs «actifs» sont équipés d'un module de communication, par exemple d'un système global de communications mobiles qui communique de façon continue son emplacement actuel à un tiers, ce qui permet un suivi à distance en temps réel du dispositif GPS.

Il est possible de régler la plupart des téléphones portables pour qu'ils fonctionnent comme des dispositifs actifs de suivi de localisation. La plupart des nouveaux téléphones portables sont équipés d'un dispositif GPS

⁽⁹²⁾ Hightower J. et Borriello G., *Computer* 2001;34(8) p. 57-66.

pour suivre en continu leur localisation en cas d'urgence. À l'aide des données GPS du téléphone portable de leur enfant, les parents peuvent non seulement le localiser à tout instant mais peuvent également être alertés lorsque celui-ci s'écarte d'une zone prédéfinie par ceux-ci ⁽⁹³⁾. Des bracelets équipés de technologies GPS et de téléphonie mobile sont distribués aux travailleurs humanitaires intervenant dans les zones de conflit où il existe un risque de prise d'otage. Le bracelet peut se déclencher manuellement lorsque le travailleur humanitaire est menacé ou en cas de retrait forcé de l'appareil. Ces bracelets transmettent en temps réel l'emplacement GPS de la personne qui est équipée de l'appareil, ce qui permet aux équipes de sauvetage de repérer le lieu et l'heure de l'attaque ⁽⁹⁴⁾.

En dehors de la surveillance de la localisation des personnes physiques, la technologie GPS permet de suivre des objets et des marchandises commerciales. Plusieurs fabricants automobiles, y compris Ford, Volvo et BMW, ont élaboré des systèmes d'assistance en cas d'urgence qui ont été conçus à l'aide de la technologie GPS. Ces systèmes peuvent alerter les services d'urgence lorsqu'un coussin gonflable se déploie dans un véhicule, ce qui permet à ces services de le trouver rapidement et de fournir l'assistance médicale nécessaire ⁽⁹⁵⁾.

La technologie GPS permet également d'alerter le propriétaire d'un véhicule par téléphone ou par courrier électronique lorsque l'alarme se déclenche et de lui indiquer où se trouve son véhicule ⁽⁹⁶⁾.

La technologie RFID

La technologie d'identification par radiofréquence (RFID, *Radio Frequency Identification*) est fondée sur l'interprétation et la transmission d'ondes radio sans fil par des transpondeurs (étiquettes) et des lecteurs (émetteurs-récepteurs). Les étiquettes RFID sont actives ou passives: les étiquettes passives ne sont pas équipées de leur propre système d'alimentation électrique et sont approvisionnées en énergie par les ondes radio transmises par le lecteur. Les étiquettes actives possèdent quant à elles leur

propre batterie et peuvent émettre leurs propres ondes radio. Il est possible de lire à distance les informations stockées sur une étiquette RFID en utilisant un système sans contact. La distance maximale de fonctionnement (c'est-à-dire la portée) entre le lecteur RFID et l'étiquette peut être comprise entre quelques centimètres et une dizaine de mètres ⁽⁹⁷⁾. Cette portée dépend de plusieurs facteurs, tels que la fréquence de communication, la puissance du lecteur, les sources d'interférence radio et les objets présents dans l'environnement qui peuvent renvoyer ou absorber les ondes radio.

Ces dispositifs de petite dimension à faible coût étaient initialement utilisés par les entreprises pour le suivi de leur stock. Des entreprises de vente au détail, telles que Tesco, le troisième plus grand distributeur de produits alimentaires dans le monde, utilisent des étiquettes RFID pour améliorer leurs systèmes de contrôle des stocks et assurer leur suivi dans la chaîne d'approvisionnement. Depuis 2003, le groupe Metro en Allemagne dirige un «magasin du futur» basé sur la technologie RFID dont les applications sont variées sur l'ensemble de la chaîne d'approvisionnement ⁽⁹⁸⁾.

Des étiquettes RFID ont été implantées sur des animaux, y compris des animaux de compagnie et du bétail, pour assurer le suivi d'informations relatives à leur propriétaire et à leur historique de vaccination et garantir ainsi la traçabilité nécessaire du bétail à des fins de sécurité sanitaire des aliments. Les animaux de compagnie qui circulent dans les États membres de l'UE (uniquement les chats, les chiens et les furets pour le moment) doivent posséder un «passeport» auquel ces derniers sont associés par une étiquette RFID implantée dans leur corps. Ce passeport a été créé pour protéger les citoyens contre les risques de rage et d'autres maladies véhiculées par les animaux ⁽⁹⁹⁾.

Les dernières innovations relatives à la technologie RFID ont vu son rôle s'élargir en passant des applications d'étiquetage animal et industriel aux implants

⁽⁹³⁾ <http://news.verizonwireless.com/news/2006/06/pr2006-06-12.html>

⁽⁹⁴⁾ «Smart bracelet protects aid workers.» *BBC News*. <http://www.bbc.co.uk/news/technology-22038012>

⁽⁹⁵⁾ http://www.euroncap.com/rewards/ford_sync_emergency_assistance.aspx

⁽⁹⁶⁾ <http://www.techlila.com/trace-stolen-car-using-mobile-phone-technologies/>

⁽⁹⁷⁾ Hodges S. et McFarlane D. (2005), «Radio frequency identification: technology, applications and impact», série des livres blancs Auto-ID Labs, édition 1. <http://www.autoidlabs.org/uploads/media/AUTOIDLABS-WP-HARDWARE-016.pdf>

⁽⁹⁸⁾ Wamba S.F. et Boeck H., *Journal of Theoretical and Applied Electronic Commerce Research*, 2008;3(1): p. 92-105.

⁽⁹⁹⁾ http://ec.europa.eu/food/animal/liveanimals/pets/qanda_fr.htm

CHAPITRE I. | APPLICATIONS DES TECHNOLOGIES DE SÉCURITÉ ET DE SURVEILLANCE

humains. Ces applications ont fait naître des craintes d'«*Ubervveillance*», terme qui a été inventé en 2006 pour désigner une forme de surveillance électronique omniprésente facilitée par l'essor de technologies d'implant de dispositifs de surveillance dans le corps humain ⁽¹⁰⁰⁾. En 2004, l'agence américaine des médicaments et des produits alimentaires (*Food and Drug Administration* ou FDA) a approuvé l'implantation d'étiquettes RFID dans le bras appelées VeriChip, qui permettraient au personnel de soins de santé d'accéder au dossier médical de patients qui se trouvent dans l'incapacité de communiquer. L'exemple d'application qui a eu le plus grand retentissement date de 2004 lorsque le ministre de la justice mexicain et dix-huit membres de son personnel se sont fait implanter des puces, non pas pour bénéficier de soins de santé mais pour accéder à des zones de haute sécurité dans leur lieu de travail ⁽¹⁰¹⁾. En octobre 2011, PositiveID a annoncé que l'armée israélienne avait passé commande de micropuces VeriChip à des fins de gestion des situations d'urgence et de préparation aux catastrophes ⁽¹⁰²⁾. Des recherches sont actuellement menées pour déterminer si des étiquettes RFID ingérables peuvent être utilisées pour surveiller la posologie et l'observance du traitement de patients ⁽¹⁰³⁾ tandis que des études ont été récemment réalisées pour déterminer si la technologie RFID peut être utilisée pour l'identification dentaire en criminalistique en implantant un petit transpondeur dans les dents ⁽¹⁰⁴⁾. Cette technologie ne manque pas de soulever des critiques et il a déjà été proposé d'implanter des dispositifs RFID dans le corps de citoyens «vulnérables», tels que les enfants, les personnes souffrant de troubles psychiques ou mentaux, afin de les protéger des dangers extérieurs. Certains ont dans le même temps demandé que les travailleurs migrants et les délinquants, notamment les pédophiles, se fassent

implanter une étiquette pour que «nous» soyons protégés de «ces individus» ⁽¹⁰⁵⁾.

1.4. Caractéristiques technologiques

Quel que soit le domaine dans lequel les technologies de sécurité et de surveillance ont fait leur apparition, celles-ci partagent des caractéristiques communes, à savoir la miniaturisation, l'automatisation et l'ubiquité.

1.4.1. La miniaturisation

Les progrès technologiques accomplis en matière de miniaturisation électronique depuis la Seconde Guerre mondiale ont transformé le monde dans lequel nous vivons et donné naissance à des capteurs miniaturisés et à des dispositifs micromécaniques. Depuis 1960, nous constatons une miniaturisation exponentielle des composants électroniques, ce qui confirme la célèbre prédiction de Gordon Moore en 1965. Le vieil adage anglais *Small is beautiful* aurait pu être inventé spécialement pour la technologie puisque les objets de petite taille sont rapides, bon marché et rentables dans ce domaine. Les dispositifs de plus petite taille sont généralement plus rapides étant donné que le signal n'a pas à parcourir de grande distance à l'intérieur de ces dispositifs. La miniaturisation des dispositifs a également facilité l'intégration de plusieurs fonctions au sein d'un seul appareil, ce qui a entraîné une baisse des coûts puisque la pénétration sur le marché de ces dispositifs est plus importante.

Les ordinateurs personnels et les tablettes, les téléphones intelligents équipés de GPS et les appareils photographiques ont créé de nouveaux marchés de grande ampleur grâce à la miniaturisation. Toutefois, des doutes ont été émis puisqu'il a été avancé que nous atteignons les limites physiques de la miniaturisation et que la théorie de Moore (la multiplication par deux du nombre de composants sur une puce informatique tous les dix-huit mois) ne pourra plus être vérifiée après 2020 à moins que la nanotechnologie ne vienne révolutionner la technologie actuelle ⁽¹⁰⁶⁾. Le développement des microcapteurs et des nanocapteurs dépendra des progrès accomplis en matière de nanomatériaux et de

⁽¹⁰⁰⁾ Michael M.G. et al., *Computer Communications*, 2008;31(6): p. 1192-1198.

⁽¹⁰¹⁾ <http://www.spychips.com/press-releases/mexican-implant-correction.html>

⁽¹⁰²⁾ <http://finance.yahoo.com/news/PositiveID-Corporation-pz-3900073790.html>

⁽¹⁰³⁾ Rajogopakan H. et Rahmat-Samii Y., colloque international de l'Antennas and Propagation Society (APSURSI), 2010, IEEE, p. 1-4.

⁽¹⁰⁴⁾ Nuzzolese E. et al., *The Open Dentistry Journal*, 2010;4: p. 33-36.

⁽¹⁰⁵⁾ Les dispositifs implantables soulèvent plusieurs questions éthiques. Pour un examen plus approfondi de ces questions, consultez l'avis n° 20 du GEE (16.3.2005), Aspects éthiques des implants TIC dans le corps humain.

⁽¹⁰⁶⁾ <http://www.techspot.com/news/48409-physicist-predicts-moores-law-will-collapse-in-about-10-years.html>

matériaux nanostructurés. Les nanofils inorganiques et les nanocristaux possèdent des propriétés électriques et optiques uniques qui peuvent être exploitées dans le domaine de la détection. Des nanocapteurs, qui sont déjà en cours de développement, offrent la possibilité de détecter des processus ou des événements qui étaient auparavant indétectables. Les nanocapteurs ont plusieurs applications potentielles, y compris le

diagnostic et le traitement de maladies, la détection de polluants environnementaux, les systèmes d'alerte précoce à l'égard des menaces qui pèsent sur les infrastructures ainsi que des applications dans le domaine de la sécurité (voir l'encadré ci-dessous). On estime qu'il sera techniquement réalisable de déployer et de mettre en réseau des nanocapteurs dans un grand nombre de ces domaines d'ici 2020 ⁽¹⁰⁷⁾.

⁽¹⁰⁷⁾ Rapport technique de Rand: «The Global Technology Revolution 2020, In-Depth Analyses». 2006 http://www.rand.org/content/dam/rand/pubs/technical_reports/2006/RAND_TR303.pdf

CHAPITRE I. | APPLICATIONS DES TECHNOLOGIES DE SÉCURITÉ ET DE SURVEILLANCE

Les nanocapteurs

Les nanocapteurs, qui sont développés depuis près de dix ans, sont des capteurs conçus à l'aide de nanocomposants, qui transmettent au monde macroscopique des informations relatives à des nanoparticules. Ces capteurs peuvent être fabriqués pour détecter des différences de volume, de vitesse, de gravité, de charge électrique, de composition chimique, de pression, de température ou de tout autre facteur physique.

Les nanocapteurs peuvent être globalement classés dans trois catégories différentes en fonction des éléments qu'ils détectent. Les nanocapteurs physiques mesurent des propriétés telles que la masse, la pression ou la force tandis que les capteurs chimiques sont capables de détecter une substance chimique ou de déterminer sa concentration. Les biocapteurs sont utilisés pour contrôler des processus au niveau moléculaire tels que la communication cellulaire et les interactions d'anticorps/antigènes. On considère parfois qu'il s'agit d'une sous-catégorie de capteurs chimiques. Les nanocapteurs peuvent être fabriqués de différentes façons; les trois méthodes les plus répandues sont la lithographie par voie descendante, l'assemblage par voie ascendante et l'autoassemblage moléculaire. L'approche descendante implique la décomposition de matériaux de plus grande taille en objets de plus petite taille; l'approche ascendante fonctionne par autoassemblage de molécules et d'atomes individuels pour concevoir des nanostructures. L'autoassemblage moléculaire peut être réalisé selon l'une des deux façons suivantes. La première de ces méthodes utilise comme base des nanostructures qui ont déjà été créées ou qui existent naturellement et intègre celle-ci dans des atomes libres pour créer une nanostructure de taille plus importante. Dans la deuxième méthode, un groupe complet de composants s'assemble automatiquement dans un nanocapteur, ce qui constitue une approche d'autoassemblage beaucoup plus complexe que celle mentionnée précédemment.

Les nanocapteurs sont ultrasensibles et peuvent être déployés à grande échelle grâce à leur petite dimension et leur faible coût potentiel. Ils sont ainsi parfaitement adaptés aux applications dans les domaines de la santé, de la sécurité et de l'environnement. Comme les nanocapteurs ont individuellement une plage de détection limitée, des travaux de recherche sont actuellement menés dans l'optique de développer un dispositif intégré de nanocapteurs doté de capacités de communication, ce qui devrait étendre leurs champs d'application ⁽¹⁰⁸⁾.

Les nanocapteurs reliés aux systèmes GPS permettent de surveiller en temps réel les conditions des sols et des cultures. Les informations tirées de capteurs autonomes dans les champs fournissent des renseignements sur la température du sol et sur le taux d'humidité, ce qui permet de prendre des décisions avisées à propos de la récolte et de la gestion de l'irrigation. En période de sécheresse, des vignerons australiens ont utilisé des nanocapteurs pour contrôler et surveiller la production de raisins destinés à la fabrication de vin d'excellente qualité. Les nanocapteurs peuvent également détecter la contamination chimique ou microbienne d'une culture et des nanostructures font l'objet d'études pour délivrer des traitements au cours de la phase initiale de développement de maladies ⁽¹⁰⁹⁾.

L'un des domaines dans lequel les progrès les plus importants ont été accomplis concerne le développement de biocapteurs dans l'optique de diagnostiquer les maladies de manière précoce et d'améliorer les traitements. Les biocapteurs haute sensibilité pourraient détecter des niveaux de biomarqueurs pronostiques ou prédictifs de manière plus précoce dans le développement des maladies, faire la distinction entre les évolutions favorables et défavorables de tumeurs et fournir une aide pour la poursuite des traitements. Les biocapteurs peuvent être utilisés pour surveiller le taux de glucose chez les personnes diabétiques et le taux de monoxyde d'azote dans l'air expiré chez les personnes asthmatiques et pourraient être également utilisés pour la recherche de nouveaux médicaments ⁽¹¹⁰⁾.

Les nanocapteurs ont également un rôle à jouer dans la surveillance de l'intégrité des infrastructures. Des systèmes microélectromécaniques (SMEM) et des capteurs à base de nanotubes de carbone ont été intégrés dans des blocs et des poutres en béton pour surveiller la température et le taux d'humidité et pour détecter les fissures à l'intérieur du béton. Grâce à la transmission sans fil de signaux, des systèmes d'alerte précoce peuvent être mis en place pour

⁽¹⁰⁸⁾ Usibe B.E. et al., International Journal of Materials Engineering, 2013;3(1): p. 4-10.

⁽¹⁰⁹⁾ Misra A.N. et al., International Journal of Pure and Applied Sciences and Technology, 2013;16(2): p. 1-9.

⁽¹¹⁰⁾ Agrawal S. et Prajapati R., International Journal of Pharmaceutical Sciences and Nanotechnology, 2012;4(4): p. 1528-1535.

surveiller l'intégrité de l'infrastructure de chaussées, de bâtiments et de ponts qui pourraient se trouver soumis à des contraintes dans des conditions défavorables, par exemple en cas de séisme ou d'ouragan ⁽¹¹¹⁾.

Il existe plusieurs applications en matière de défense et de sécurité pour les nanocapteurs. Les nanocapteurs chimiques et biologiques peuvent être utilisés pour détecter les armes chimiques/biologiques à partir d'une concentration minimale d'une seule molécule. Pour détecter les quantités extrêmement faibles de vapeurs chimiques, des nanotubes de carbone, des nanofils d'oxyde de zinc ou des nanoparticules de palladium sont utilisés dans les nanocapteurs. Les caractéristiques électriques de ces éléments détecteurs sont modifiées en cas d'interaction avec des molécules de gaz. Il suffit de quelques molécules de gaz pour modifier les propriétés électriques des éléments détecteurs de ces capteurs, ce qui facilite la détection ou la surveillance même lorsque la concentration de vapeurs chimiques est extrêmement faible. Le SnifferSTAR est un nanocapteur chimique qui peut être intégré dans un microdrone. Cette plateforme mobile de détection chimique peut avoir des applications civiles ou militaires sur le terrain et sert de système d'alerte précoce en cas d'attaque à l'arme chimique ⁽¹¹²⁾. Des scientifiques de la NASA ont conçu une petite puce de la taille d'un timbre-poste qui est composée de 32 nanocapteurs. Ces derniers sont capables de détecter chacun une substance chimique différente. Des applications civiles sont également envisagées en installant des nanocapteurs chimiques à l'intérieur de téléphones intelligents pour surveiller les taux de monoxyde de carbone et de méthane à l'intérieur des domiciles de particuliers ⁽¹¹³⁾. En Allemagne, des scientifiques spécialisés dans les matériaux ont conçu un nanocapteur qui détecte les traces d'explosifs. Actuellement, les méthodes les plus répandues pour détecter ces traces sont la spectrométrie de mobilité ionique, la spectrométrie de masse et la chromatographie gazeuse. Ces trois méthodes prennent du temps et nécessitent du matériel encombrant et onéreux, ce qui limite leur déploiement aux endroits stratégiques tels que les aéroports. Des scientifiques de l'université technique de Darmstadt ont conçu un nanocapteur capable de détecter une seule molécule de tétranitrate de pentaérythritol (PETN), un explosif qui est fréquemment utilisé par les terroristes tels que l'«homme aux sous-vêtements explosifs» en 2009. Il a été proposé d'installer ces nanocapteurs dans les machines à rayons X pour procéder aux vérifications de sécurité dans les aéroports afin de contrôler discrètement les passagers et leurs bagages dans l'optique de détecter les traces d'explosifs ⁽¹¹⁴⁾.

La nanotechnologie associée aux réseaux de capteurs sans fil et aux systèmes microélectromécaniques (SMEM) permet de créer un réseau sans fil de nanocapteurs appelés des nœuds capteurs (*mote* en anglais), que l'on désigne par l'expression «poussière intelligente». La surveillance permanente est ainsi à portée de main depuis le développement de cette «poussière intelligente». Des systèmes de détection, de calcul et de communication autonomes peuvent désormais être assemblés dans un millimètre cube (la taille d'un grain de poussière) pour former la base d'un réseau intégré de capteurs distribués à grande échelle ⁽¹¹⁵⁾. Kris Pister, qui a été le premier à développer le concept de «poussière intelligente», prévoyait des applications potentielles comme les réseaux de capteurs liés à la défense pour la surveillance des zones de combat, la surveillance de l'application des traités, la surveillance des systèmes de transport et l'interception de missiles Scud. Le projet Smart Dust de l'université de Berkeley, qui a été dirigé par Kris Pister, a permis de créer un nœud capteur de la taille d'un grain de sable en 2002 ⁽¹¹⁶⁾. Des scientifiques de l'université de Berkeley et de la marine américaine ont déployé depuis un drone six nœuds capteurs qui formaient un réseau sans fil détectant la vitesse et l'itinéraire de 142 véhicules militaires en transit et renvoyant ces données vers le drone ⁽¹¹⁷⁾. Des inquiétudes surgissent à propos de l'émergence d'équipements de surveillance invisibles à l'œil nu puisque les intrusions dans la vie privée seront plus simples dans les lieux privé et public.

⁽¹¹¹⁾ Saafi M. et al., *Journal of Materials and Structural Integrity*, 2010;4(1): p. 1-24.

⁽¹¹²⁾ <http://www.sciencedaily.com/releases/2003/01/030127074837.htm> consulté le 11 novembre 2013.

⁽¹¹³⁾ <http://gizmodo.com/5881097/this-is-nasas-cancer-sniffing-cellphone-sensor/> consulté le 11 novembre 2013.

⁽¹¹⁴⁾ <http://www.sciencedaily.com/releases/2011/07/110726092952.htm> consulté le 11 novembre 2013.

⁽¹¹⁵⁾ Anderson M., *New Scientist*, 2013;218(2914):26; Anderson M., *New Scientist*, 2013;218(2914): p. 26.

⁽¹¹⁶⁾ Warneke B.A. et al., *Sensors Proceedings of the IEEE*, 2002;2: p. 1510-1515.

⁽¹¹⁷⁾ Anderson A., *The Economist*, 20 novembre 2003. <http://www.economist.com/node/2173026> consulté le 11 novembre 2013.

CHAPITRE I. | APPLICATIONS DES TECHNOLOGIES DE SÉCURITÉ ET DE SURVEILLANCE

1.4.2. L'ubiquité

La réduction de la taille des composants et l'accroissement de leur puissance permettront d'atteindre l'objectif final d'ubiquité des ordinateurs. L'informatique de type ubiquitaire (également appelée informatique diffuse) fait naître l'espoir d'une intégration transparente des infrastructures numériques dans nos vies quotidiennes ⁽¹¹⁸⁾. L'informatique ubiquitaire est fondée sur la convergence de l'internet, de systèmes électroniques sophistiqués et de technologies sans fil. L'objectif est de créer des objets «intelligents» capables d'explorer leurs environnements et de communiquer discrètement avec d'autres produits intelligents afin de fournir des informations et des services aux utilisateurs humains. La sous-division matérielle de l'informatique ubiquitaire est désignée par l'expression «internet des objets». Les technologies telles que les composants RFID et les capteurs sans fil qui sont embarqués dans les objets de notre quotidien permettent de passer d'une intégration des sources d'information des dispositifs traditionnels à notre environnement physique. Les objets du quotidien peuvent être détectés, localisés et contrôlés via l'internet. Il devient facile d'installer des systèmes de capteurs sensibles au contexte dans tous les domaines de notre vie quotidienne, de nos déplacements jusqu'à nos soins de santé en passant par la surveillance de l'environnement et de la sécurité. Comme Weisner, le père de l'informatique ubiquitaire, l'avait fait remarquer: «Les technologies les plus profondes sont celles qui disparaissent. Elles se fondent dans la trame de la vie quotidienne jusqu'à en devenir indiscernables» ⁽¹¹⁹⁾. Ces caractéristiques mettent en évidence les capacités de surveillance de cette technologie. Les technologies de surveillance actuelles ont une portée restreinte en matière de surveillance et de suivi des personnes physiques. Les objets (par exemple les chaussées, les sols, les portes) qui comportent des étiquettes RFID et les personnes physiques qui portent des vêtements avec des étiquettes ou qui sont équipées de téléphones intelligents sont «lisibles» par le système de suivi du réseau sans fil, ce qui permet de localiser instantanément les personnes et les objets recherchés en temps réel. L'internet des objets, qui par certains aspects peut rappeler l'expression «Big Brother vous regarde», représente une source d'inquiétude pour les défenseurs de la vie privée, même si les répercussions d'une intégration aussi profonde de l'informatique

dans nos vies quotidiennes ne sont pas encore clairement établies.

1.4.3. L'automatisation

L'énorme quantité de données générées par les technologies appliquées dans les domaines de la sécurité et de la surveillance, ce que l'on appelle le raz-de-marée de données, peut facilement dépasser notre capacité à transmettre, traiter et utiliser les informations de manière efficace. Il est nécessaire d'automatiser de nombreux systèmes pour tirer des informations pertinentes des données et, dans certains cas, pour prendre des mesures à partir de celles-ci. Depuis le début des années 90, les systèmes et les caméras de télévision en circuit fermé (CCTV) se sont multipliés dans les lieux publics, notamment dans les centres-ville. Selon la British Security Industry Authority (BSIA), il y aurait 4,9 millions de caméras de télévision en circuit fermé au Royaume-Uni, ce qui équivaut à une caméra pour quatorze personnes ⁽¹²⁰⁾. Les opérateurs sont surchargés d'informations et dépassés, ce qui signifie que ces caméras sont uniquement efficaces lorsqu'elles captent leur attention. La surveillance automatisée par CCTV est devenue une réalité depuis l'apparition des caméras numériques associée à l'accroissement des capacités de stockage et de traitement.

L'analyse automatisée des images des caméras de télévision en circuit fermé a été déployée dans le domaine de la reconnaissance automatique des plaques d'immatriculation: les caméras photographient chaque véhicule qui passe devant elles et un logiciel analyse cette photographie pour reconnaître la plaque d'immatriculation. Le système de reconnaissance automatique des plaques d'immatriculation enregistre l'heure et le lieu et stocke ces informations accompagnées de l'image et du numéro d'immatriculation. Cette technologie est apparue initialement pour gérer la circulation sur les réseaux routiers, c'est-à-dire pour le paiement des frais de péage et d'embouteillage. L'installation de caméras sur les véhicules des forces de l'ordre fait partie des utilisations les plus récentes de cette technologie. Les forces de l'ordre peuvent ainsi trouver la correspondance d'une plaque d'immatriculation dans une liste spéciale de numéros de plaques d'immatriculation qui ont été saisis dans le système à la suite d'un vol de véhicule ou d'une inscription dans le registre des personnes présentant un intérêt particulier. Les dernières études dans le domaine de la surveillance automatisée

⁽¹¹⁸⁾ Friedewald M. et Raabe O., 2011; 28(2): p. 55-65.

⁽¹¹⁹⁾ Mark Weiser, «The Computer for the Twenty-First Century», *Scientific American*, p. 94-10, septembre 1991.

⁽¹²⁰⁾ <http://www.bsia.co.uk/cctv>

font état d'inquiétudes à propos de la reconnaissance des personnes physiques et de leurs intentions ⁽¹²¹⁾. Les logiciels de reconnaissance faciale peuvent analyser automatiquement les vidéos, sélectionner un visage dans une foule et identifier l'individu concerné en comparant ces informations avec une base de données de visages connus. Cette personne peut ainsi être suivie d'une caméra à l'autre dans des secteurs géographiques étendus sans aucune intervention humaine. Les caméras automatisées peuvent également être programmées pour détecter les «comportements suspects» ou les «menaces», par exemple l'accès d'une personne dans une zone réglementée ou la présence d'un bagage sans surveillance dans un aéroport. Il est ainsi possible de définir les agissements ou les individus déviants en fonction du degré d'écart à partir de la modélisation des comportements «normaux». Pour consulter l'analyse portant sur les drones autonomes, voir page 58.

1.5. La convergence des technologies

Les progrès accomplis en matière de technologies de sécurité et de surveillance au cours de ces dix dernières années résultent en grande partie de la convergence de disciplines telles que la technologie de l'information, la nanotechnologie, la technologie des matériaux et la biotechnologie. L'intégration et la fonctionnalité transversale des technologies sont désormais la règle plutôt que l'exception. Les consommateurs peuvent désormais téléphoner, accéder à leurs courriers électroniques, naviguer sur l'internet, prendre des photos et consulter des itinéraires à l'aide de leur téléphone intelligent. Ce phénomène de convergence est une tendance qui va perdurer: les exercices de prospective technique prévoient que la technologie en 2020 «continuera d'intégrer des développements de différentes disciplines scientifiques dans un souci de convergence dont les effets sur la société seront profonds» ⁽¹²²⁾.

1.6. Les moteurs de la technologie

Il est difficile de savoir si l'innovation technologique dans le domaine de la sécurité et de la surveillance a été ou est stimulée par les découvertes (ou avancées) scientifiques ou par la demande (ou attractions) du marché. Comme cela a été décrit ci-dessus, il ne fait aucun doute que des innovations sont apparues dans ce domaine. Cependant, certains détracteurs prétendent

que ces technologies ont simplement été conçues pour résoudre des problèmes et non pas pour répondre à un véritable besoin. Le déploiement à grande échelle de technologies de surveillance, telles que les caméras de télévision en circuit fermé, dont les avantages en matière de sécurité sont limités ⁽¹²³⁾ en constitue un exemple. De la même façon, il a été avancé que la collecte automatisée et systématique des données des citoyens par les organismes de sécurité gouvernementaux découlerait de la disponibilité de ces informations et de la capacité de stockage à moindre coût ⁽¹²⁴⁾. L'un des autres moteurs technologiques est l'interopérabilité croissante puisque la capacité de relier plusieurs systèmes constitue un attrait supplémentaire pour les personnes chargées de leur acquisition ⁽¹²⁵⁾. David Lyon explique que la perception d'infailibilité de la technologie est un moteur de l'introduction de systèmes de surveillance puisque le public accepte mieux les systèmes qui sont à l'abri des erreurs humaines. Il cite notamment comme exemple l'introduction des identificateurs biométriques et leur utilisation croissante par les gouvernements pour la vérification des identités ⁽¹²⁶⁾.

Comme le font observer les auteurs du rapport SAPIENT ⁽¹²⁷⁾, en dehors des moteurs technologiques, il existe également des moteurs d'ordre social, politique et économique liés à l'ubiquité croissante des technologies de sécurité et de surveillance.

1.6.1. Les moteurs sociaux

Les citoyens peuvent être les moteurs du développement des technologies de sécurité et de surveillance puisque ces dernières peuvent être perçues comme des mécanismes garantissant notre sûreté et notre sécurité ainsi que celles de nos enfants. Les récits de crime, de violence et de conflit génèrent de la peur et de l'angoisse pour la sécurité personnelle. David Lyon relie cet élément moteur à la notion de «risque perçu» et à l'attrait de la population en faveur du «risque

⁽¹²¹⁾ Adams A.A. et Ferryman J., *Security Journal*, 2013 p. 1-18. ISSN 1743-4645 doi:10.1057/sj.2012.48.

⁽¹²²⁾ Ibid 40.

⁽¹²³⁾ Welsh B.C., Farrington D.P., «Effects of closed circuit television on crime». *Campbell Systematic Review*, 2008. http://www.campbellcollaboration.org/news_/CCTV_modest_impact_on_crime.php

⁽¹²⁴⁾ *Scientific American*, juin 2013 <http://www.scientificamerican.com/article.cfm?id=how-are-the-nsa>

⁽¹²⁵⁾ SAPIENT, «Smart Surveillance State of the Art», 2012 <http://www.sapientproject.eu/docs/D1.1-State-of-the-Art-submitted-21-January-2012.pdf>

⁽¹²⁶⁾ Lyon D., *Bioethics*, 2008;22(9): p. 499-508.

⁽¹²⁷⁾ Ibid 48.

CHAPITRE I. | APPLICATIONS DES TECHNOLOGIES DE SÉCURITÉ ET DE SURVEILLANCE

zéro» ⁽¹²⁸⁾. Furedi affirme quant à lui que la culture de la peur est motivée par la perception des risques: «les craintes à propos de l'avenir sont liées aux inquiétudes résultant des problèmes d'aujourd'hui» — des problèmes qui sont peut-être eux-mêmes issus de périodes incertaines (les notions de peur et de confiance sont abordées de manière plus détaillée à la page 73).

1.6.2. Les moteurs politiques

Pour justifier l'introduction de technologies de sécurité et de surveillance, le système politique explique qu'il a pour obligation de garantir la sécurité des citoyens et de répondre à leurs exigences vis-à-vis de leur sentiment de sécurité (voir l'analyse du contrat social, p. 67). L'introduction qui a été proposée d'un système européen de surveillance des frontières s'appuie sur la justification selon laquelle ce système contribuera à empêcher le franchissement illégal de frontières et à réduire la migration clandestine, ce qui renforcera la sécurité intérieure de l'Union européenne ⁽¹²⁹⁾. La coopération avec d'autres gouvernements ou organismes peut également conduire à l'introduction de nouvelles technologies. L'adoption de passeports biométriques en Europe résulte en grande partie de l'utilisation de cette technologie qui a été imposée aux citoyens européens par les États-Unis pour accéder à leur territoire sans visa.

1.6.3. Les moteurs économiques

Les facteurs économiques sont également les principaux moteurs du développement et de l'adoption de technologies de sécurité et de surveillance. Au titre du programme-cadre «Horizon 2020», l'UE a alloué 1,6 million d'euros en faveur de la recherche dans la sécurité pour la période 2014-2020. Le marché mondial de la sécurité et de la surveillance s'élèverait selon les estimations à une valeur de 81 milliards d'euros par an et le taux de croissance annuel des marchés nationaux serait compris entre 7 et 9 %. Ce montant inclut 11 milliards d'euros qui seraient dépensés par les autorités militaires/gouvernementales ⁽¹³⁰⁾. Le chiffre d'affaires mondial tiré des équipements de vidéosurveillance devrait

passer de 9,6 milliards en 2010 à 20,5 milliards d'euros en 2016. En 2014, le marché mondial de la vidéosurveillance en réseau sera supérieur à celui du marché mondial de la vidéosurveillance analogique ⁽¹³¹⁾. Le marché mondial des systèmes d'analyse vidéo et de surveillance intelligente devrait passer de 13,5 milliards d'euros en 2012 à 39 milliards d'euros d'ici 2020 ⁽¹³²⁾. De plus, de nouveaux débouchés civils sont recherchés pour les technologies développées à des fins militaires et la multiplication des applications civiles de drones en constitue l'illustration. La réduction des coûts qui a entraîné l'adoption accélérée des technologies de sécurité et de surveillance par les consommateurs constitue un facteur supplémentaire de son déploiement à grande échelle. La reconnaissance des empreintes digitales est désormais le système biométrique le plus répandu pour accéder aux ordinateurs portables, aux téléphones portables et aux appareils portables en raison de l'intégration simplifiée de petits capteurs de mouvements des empreintes digitales à faible coût à l'intérieur de ces appareils.

1.7. Les limites de la technologie

Le renforcement des conditions de sécurité dans de nombreux domaines de notre société fait naître un intérêt important en faveur des identificateurs biométriques et entraîne une hausse des attentes relatives aux technologies biométriques. Selon une enquête récente, 81 % des citoyens européens interrogés sont favorables à l'utilisation des identificateurs biométriques dans les enquêtes pénales même si ces personnes interrogées «manquent d'éléments pour comprendre de manière approfondie quels sont les avantages et les applications de la technologie biométrique dans leur vie quotidienne» ⁽¹³³⁾. Aucun système

⁽¹²⁸⁾ Ibid 49.

⁽¹²⁹⁾ [http://ec.europa.eu/immigration/tab3.do?subSec=16&language=7\\$fr](http://ec.europa.eu/immigration/tab3.do?subSec=16&language=7$fr)

⁽¹³⁰⁾ «Surveillance and Security Equipment: Technologies and Global Markets» (numéro de rapport SAS015B), 2013. [http://www.bccresearch.com/pressroom/sas/industrial-commercial-demand-surveillance-equipment-reach-\\$83.8-billion-2017](http://www.bccresearch.com/pressroom/sas/industrial-commercial-demand-surveillance-equipment-reach-$83.8-billion-2017) consulté le 9 octobre 2013.

⁽¹³¹⁾ IMS Research. «The World Market for CCTV and Video Surveillance Equipment», 2013. http://www.imsresearch.com/report/CCTV_and_Video_Surveillance_Equipment_World_2013&cat_id=130&type=LatestResearch http://www.imsresearch.com/report/CCTV_and_Video_Surveillance_Equipment_World_2013&cat_id=130&type=LatestResearch consulté le 9 octobre 2013.

⁽¹³²⁾ ReportsNReports. «Intelligent Video Surveillance, VCA & Video Analytics: Technologies & Global Market — 2013-2020». 2013. <http://www.prweb.com/releases/intelligent-video/surveillance-vca-vr/prweb10565272.htm> consulté le 9 octobre 2013.

⁽¹³³⁾ Enquête Steria, juillet 2013 <http://www.steria.com/media/press-releases/press-releases/article/81-of-citizens-in-favour-of-biometric-identification-finds-steria-survey/> consulté le 10 octobre 2013.

de reconnaissance biométrique n'est précis à 100 % et tous les systèmes biométriques peuvent générer différentes erreurs, comme les erreurs d'inscription, d'acquisition, de validation et de rejet. Les technologies et les systèmes biométriques présentent des risques de pannes intrinsèques et de pannes liées à des attaques externes. Les pannes intrinsèques sont liées aux performances globales en matière de reconnaissance de ces systèmes, c'est-à-dire aux erreurs des systèmes, tandis que les attaques sont des agissements délibérés dont l'objectif est d'accéder aux systèmes en utilisant les défauts de conception ou de contourner ses règles d'accès, comme l'usurpation (le contournement des règles par un imposteur). En 2011, le ministre de l'intérieur des Pays-Bas a suspendu le stockage dans une base de données d'empreintes digitales numériques destinées aux documents de voyage en raison d'un taux de rejet erroné s'élevant à 21 % (les empreintes digitales du système ne pouvaient pas être associées aux détenteurs de passeport) ⁽¹³⁴⁾. En 2011, jusqu'à 10 % de passeports biométriques auraient été obtenus frauduleusement en France ⁽¹³⁵⁾. Plus récemment, la technologie biométrique (les empreintes digitales) de l'iPhone 5 a été piratée 48 heures après sa mise sur le marché ⁽¹³⁶⁾.

L'analyse des données en masse (*Big Data*) qui renforce les opérations de sécurité fondées sur le renseignement est déployée dans les domaines de la lutte contre la cybercriminalité, la fraude et le terrorisme. L'analyse prédictive, associée aux modèles dont les capacités de prévision sont les plus performantes et aux techniques d'exploration de données, est fondée sur des méthodes statistiques sophistiquées, y compris sur des techniques d'analyse à variables multiples, telles que les modèles d'analyse avancée de séries chronologiques et par régression. Il ne fait aucun doute que l'analyse prédictive est un outil puissant pour recenser des tendances, des modèles ou des relations entre des données mais elle présente également des limites. Comme Jeffrey Rosen l'a fait observer, même si l'on pouvait concevoir des modèles dont le pourcentage de précision était de 99 %, l'identification des 19 pirates impliqués dans les attaques du 11 septembre aurait

entraîné l'identification de 3 millions de citoyens en tant que terroristes potentiels parmi la population de 300 millions de citoyens américains ⁽¹³⁷⁾.

1.8. Le verrouillage technologique

Il existe un sentiment profondément ancré selon lequel l'innovation présenterait des avantages et la technologie serait synonyme de progrès. Plus une technologie est adoptée, plus il est probable que cette adoption s'étende. Il a été avancé que ce phénomène pouvait entraîner un «verrouillage» des technologies en place et un rejet des autres solutions ⁽¹³⁸⁾. Les agences de renseignements et les gouvernements ont adopté diverses technologies de sécurité en tant qu'outil universel au service de la sécurité. Comme l'a signalé Ceyhan, dans cette période d'incertitude, «l'adoption d'outils de surveillance et d'identification électroniques est perçue comme la solution ultime pour lutter contre l'insécurité» ⁽¹³⁹⁾. Lyon explique que dans le cas de la surveillance cette croyance en faveur de la technologie est extrêmement excessive si l'on tient compte des éléments de preuve disponibles à propos de son efficacité pour garantir la sécurité des citoyens. Dès lors, «la présence de technologies de pointe parle d'elle-même, ce qui garantit d'une façon ou d'une autre sa propre efficacité» ⁽¹⁴⁰⁾. Les caméras de télévision en circuit fermé en sont l'illustration. L'efficacité et l'efficacités des technologies de sécurité (voir l'analyse s'y rapportant à la page 92) doivent être évaluées à la lumière de leurs effets réels plutôt qu'à la lumière des effets perçus sur le plan de la sécurité. Cette approche fondée sur des éléments de preuve empêcherait toute dépendance excessive à l'égard de la technologie et permettrait de laisser la place à des approches complémentaires.

1.9. Les technologies renforçant la protection de la vie privée

Le développement et le déploiement des technologies de sécurité et de surveillance sont perçus comme des mesures essentielles pour la protection de la sécurité des citoyens européens. Elles peuvent néanmoins également avoir une incidence sur la vie privée et les

⁽¹³⁴⁾ <https://zoek.officielebekendmakingen.nl/kst-25764-46.htm> consulté le 10 octobre 2013.

⁽¹³⁵⁾ <http://www.leparisien.fr/faits-divers/plus-de-10-des-passe-ports-biometriques-seraient-des-faux-19-12-2011-1775325.php> consulté le 10 octobre 2013.

⁽¹³⁶⁾ <http://www.bbc.co.uk/news/technology-24203929> consulté le 10 octobre 2013.

⁽¹³⁷⁾ Jeffrey Rosen. «The Naked Crowd» (New York: Random House, 2004), p. 104-107.

⁽¹³⁸⁾ Arthur W.B., *The Economic Journal*, 1989;99(394): p. 116-131.

⁽¹³⁹⁾ Ceyhan A., *Surveillance & Society*, 2008;5(2): p. 102-123.

⁽¹⁴⁰⁾ Lyon D., «Surveillance Studies: An overview», 2007, Cambridge: Polity Press, p. 147.

CHAPITRE I. | APPLICATIONS DES TECHNOLOGIES DE SÉCURITÉ ET DE SURVEILLANCE

libertés des citoyens dont les attentes à cet égard sont légitimes (voir la page 79 pour une analyse plus détaillée de la vie privée).

Protection de la vie privée par la conception

Au début des années 90, le concept de protection de la vie privée par la conception a été développé pour lutter contre les effets systémiques des TIC et des systèmes de données en réseau ⁽¹⁴¹⁾. La thèse centrale de la protection de la vie privée par la conception est la suivante: la vie privée ne peut être uniquement protégée par le respect des prescriptions des instruments réglementaires et devrait être prise en considération dès la phase de conception des technologies. Au lieu d'utiliser des outils et des fonctionnalités de renforcement de la protection de la vie privée, comme la minimisation de la collecte de données inutiles, il conviendrait d'intégrer ceux-ci dans la conception des systèmes. L'autorité néerlandaise chargée de la protection des données (RGK) et le commissaire canadien à l'information et à la protection de la vie privée de la province de l'Ontario (IPC) expliquent dans un rapport conjoint fondamental de 1995 que les technologies renforçant la protection de la vie privée donnent aux citoyens les moyens de mieux contrôler leurs données à caractère personnel et d'éviter le traitement inutile ou illégal de leurs données ⁽¹⁴²⁾.

Il a également été suggéré que l'analyse des effets sur la vie privée serait utile pour les ingénieurs et les développeurs de logiciels puisque cet outil pourrait les aider à tenir compte des incidences négatives potentielles d'éléments particuliers d'une conception technologique. Le projet PRISE, qui est financé par le septième programme-cadre relatif à la sécurité, a recommandé d'intégrer ces analyses dans les éléments dont les bailleurs de fonds doivent tenir compte. Ce mécanisme pourrait garantir la dépense de fonds publics en faveur de la recherche, ce qui représente une démarche conforme aux valeurs européennes et aux droits de l'homme fondamentaux ⁽¹⁴³⁾.

Protection de la vie privée dans la conception

La protection de la vie privée dans la conception est une notion différente de la protection de la vie privée par la conception. Elle vise principalement à faire connaître les processus à travers lesquels les valeurs et les normes s'intègrent dans l'architecture technologique. La protection de la vie privée dans la conception examine le caractère normatif des choix structurels dans l'optique de promouvoir la transparence et de protéger les droits et les valeurs des citoyens.

Le concept d'évaluation technologique constructive a été élaboré aux Pays-Bas et au Danemark et consiste «à ne plus mettre l'accent sur l'évaluation des incidences des nouvelles technologies mais plutôt sur l'élargissement des processus de conception, de développement et de mise en œuvre» ⁽¹⁴⁴⁾. L'évaluation technologique constructive rejette l'argument de neutralité de la technologie et s'appuie sur l'argument suivant: les technologies peuvent être conçues, consciemment ou inconsciemment, de manière à privilégier certains choix de société et à en exclure d'autres, comme les algorithmes peuvent l'illustrer. Ce modèle met l'accent sur la participation à un stade précoce d'un vaste panel d'acteurs pour faciliter la familiarisation à propos des technologies et la connaissance de leurs effets potentiels. Cela permet de rappeler aux différents acteurs que la conception technologique va de pair avec la conception de la société.

1.10. Les défis

Les technologies qui sont conçues et adoptées pour des applications de sécurité et de surveillance possèdent des caractéristiques communes: réduction de leurs dimensions, connexion accrue, divers degrés d'automatisation intégrée et déploiement ubiquitaire. Cependant, l'intégration ou la convergence de ces développements sont les facteurs qui conditionnent la capacité de ces technologies à exprimer leur plein potentiel et à atteindre leurs effets les plus profonds sur la société. Même s'il a été possible de réglementer des fonctions séparées, par exemple les télécommunications ou l'utilisation de l'ADN pour identifier une personne physique, le véritable enjeu consiste à réglementer des fonctions combinées. Il existe un risque associé aux technologies convergentes, y compris dans le domaine de la sécurité, concernant le retard

⁽¹⁴¹⁾ <http://privacybydesign.ca/> consulté le 12 octobre 2013.

⁽¹⁴²⁾ «Privacy-Enhancing Technologies: The Path to Anonymity (Volume I)», 1995 <http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=329> consulté le 12 octobre 2013.

⁽¹⁴³⁾ http://www.prise.oew.ac.at/docs/PRISE_Statement_Paper.pdf consulté le 12 octobre 2013.

⁽¹⁴⁴⁾ Schot J. et Rip A., «Technology Forecasting and Social Change», 1996;54: p. 251-268.

d'intégration de ces technologies dans un système réglementaire. Il existe un risque tout aussi problématique à l'autre extrémité du spectre, qui concerne les doubles emplois dans les systèmes réglementaires. Pour éviter ces deux écueils, les décideurs politiques et les régulateurs devront être informés de ces évolutions de façon précoce dans les études technologiques.

On estimait auparavant que le déploiement de technologies de sécurité et de surveillance, quelles que fussent leurs origines, constituait la prérogative des États ou de leurs organismes. Cela n'est désormais

plus le cas puisque les entités commerciales et les personnes physiques utilisent des technologies qui leur permettent d'interroger leurs clients et leurs voisins et de tirer des conclusions à propos de leurs futurs comportements à partir d'actions antérieures. Une grande partie de ces technologies induisent des changements et fournissent des avantages concrets aux particuliers et à la société dans son ensemble. Cependant, pour tirer profit de ces avantages, il est nécessaire de s'assurer que l'efficacité de ces technologies a été éprouvée et que leur utilisation est proportionnée.

Chapitre II. Gouvernance — présentation, défis, possibilités ⁽¹⁴⁵⁾

2.1. L'environnement réglementaire dans le domaine de la sécurité et de la surveillance

La sécurité et la surveillance sont des sujets couverts par de nombreux règlements dans les domaines les plus divers et, dans une certaine mesure, à différentes fins. La sécurité est une question qui relève avant tout des États membres. Une vaste gamme d'instruments réglementaires ont par conséquent été introduits dans les différents pays. Il ne sera ni possible ni nécessaire d'aborder l'ensemble de cette énorme masse de règlements dans le détail. Aux fins du présent avis, il est crucial d'avoir une vue générale de la situation et des futurs défis et possibilités réglementaires.

Ce chapitre présente les principaux domaines de réglementation, leur contenu et l'objectif qu'ils poursuivent. Dans ce contexte, certains exemples de règlements intéressants et certaines différences et lacunes réglementaires seront également présentés. La description de l'environnement réglementaire et des lacunes observées serviront à exposer un certain nombre de problèmes de gouvernance et de défis. Enfin, certains instruments de gouvernance seront présentés sous la forme de «boîte à outils» et certaines possibilités de gouvernance seront développées.

Les principaux règlements de protection des droits de l'homme, et notamment du droit à la vie privée, sont les conventions européennes et internationales relatives aux droits de l'homme et la charte des droits fondamentaux de l'UE. Dans le cadre de ces instruments, la sécurité peut aussi bien servir à limiter le droit à la vie privée que constituer un droit à part entière. Des règlements plus spécifiques sur la protection des données sont intégrés dans la réglementation de l'Union et dans les législations nationales. On retrouve également des règlements relatifs à la sécurité dans le contexte de l'Union européenne, où ils couvrent certains domaines politiques, tels que l'aviation, le contrôle des frontières et la cybercriminalité. Lorsqu'il s'agit de surveillance, la situation est plus variable et incertaine. L'utilisation de caméras de surveillance et la surveillance des télécommunications sont couvertes par les réglementations nationales. Plusieurs exemples seront présentés, notamment de

brèves observations relatives à la sécurité nationale en tant que base juridique justifiant la surveillance. Les défis réglementaires posés par les nouvelles technologies, telles que drones et la reconnaissance faciale, sont brièvement décrits et les tendances en matière de lancement d'alerte sont elles aussi exposées. Enfin, les défis réglementaires liés à la recherche sur les technologies de sécurité et de surveillance seront brièvement abordés.

Comme nous le verrons, l'environnement réglementaire en matière de sécurité et de surveillance est disparate et est régi par une mosaïque d'instruments réglementaires mondiaux, nationaux, régionaux, qui créent des risques de lacunes, des vides juridiques et d'ambiguïtés. Le présent chapitre met en outre en évidence un dilemme fondamental. En effet, si les droits de l'homme et la protection de la vie privée sont des droits reconnus au niveau mondial et si la protection des données et certains autres domaines réglementaires sont couverts par la législation de l'UE, la sécurité nationale reste quant à elle principalement du ressort des différents États membres. Des tensions peuvent apparaître lorsque les fonctions de sécurité limitent les droits à la vie privée ou sont présentées comme une valeur ou un droit protégé.

2.2. Droits de l'homme

Les droits de l'homme sont couverts par des conventions mondiales et régionales, mais leur effectivité diffère en fonction de leur interprétation et de leur mise en œuvre. Si la vie privée constitue un élément essentiel des droits de l'homme, le rôle que joue la sécurité dans la justification d'une ingérence dans les droits à la vie privée est soumis à une interprétation dynamique et évolutive ⁽¹⁴⁶⁾.

Les droits de l'homme sont des principes fondamentaux, étroitement liés à l'éthique qu'ils tentent de défendre, destinés à protéger un ensemble de droits fondamentaux pour chaque être humain. Ces objectifs se reflètent dans la *Déclaration universelle des droits de l'homme* (DUDH) qui constitue la base de la gouvernance mondiale dans ce domaine. La *Convention européenne des droits de l'homme* (CEDH) consécutive a été le premier traité juridique international visant à protéger les droits de l'homme doté de mécanismes exécutoires.

⁽¹⁴⁵⁾ La contribution du professeur Herman Nys à ce chapitre, notamment en ce qui concerne les droits de l'homme, a été vivement appréciée.

⁽¹⁴⁶⁾ Paul De Hert, Balancing security and liberty with the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11, *Utrecht Law Review*, 2005, p. 74.

CHAPITRE II. | GOUVERNANCE — PRÉSENTATION, DÉFIS, POSSIBILITÉS

L'engagement *européen* à l'égard des principes de la démocratie pluraliste, des droits de l'homme et de l'état de droit couvre au moins 800 millions de citoyens. L'extension de la CEDH, la *charte des droits fondamentaux de l'Union européenne*, qui a été adoptée en 2000 et est entrée en vigueur en 2009, s'articule autour des principes de la dignité humaine, des libertés fondamentales, de l'égalité, de la solidarité, des droits des citoyens et de la justice. Toutefois, si cette gouvernance mondiale et régionale est capitale, le libellé des dispositions est souvent assez vague, laissant ainsi la place à différentes interprétations, comme c'est souvent le cas avec les principes éthiques (voir chapitre 3).

2.2.1. Droits de l'homme et vie privée

Le droit à la vie privée est un droit ancien, qui trouve ses origines dans diverses traditions religieuses. Ce principe a dès le départ bénéficié d'une protection en tant que droit de l'homme international. Aujourd'hui, la vie privée est reconnue sans équivoque comme un droit de l'homme fondamental consacré dans les principaux instruments juridiques internationaux: *La Déclaration universelle des droits de l'homme* (article 12); *Le Pacte international sur les droits civils et politiques* (article 17) ⁽¹⁴⁷⁾; *La Convention européenne des droits de l'homme* (CEDH) (article 8) ⁽¹⁴⁸⁾; *La charte des droits fondamentaux de l'Union européenne* (article 7) ⁽¹⁴⁹⁾ et la *Convention américaine des droits de l'homme* (article 11) ⁽¹⁵⁰⁾. Le droit à la vie privée est également complété par des droits concomitants, tels que le droit à la liberté d'expression (article 10, CEDH).

Les *États-Unis* sont un acteur primordial dans les questions mondiales de vie privée, non seulement en raison de leur poids et de leur importance au niveau international, mais également du fait de leur domination dans les secteurs des fournisseurs de services internet. Les États-Unis ont une longue et riche histoire en matière de protection de la vie privée, qui se caractérise par des initiatives législatives actives et souvent

innovantes. Toutefois, ils ont également une très forte conception de la liberté d'expression, notamment de la liberté d'expression commerciale, qui a été confrontée à des accusations d'atteinte à la vie privée dans de nombreuses affaires. Cela a donné lieu à un cadre juridique général intéressant qui, dans certains domaines, est véritablement à la pointe, alors que dans d'autres, notamment dans celui de la protection des données, en reste très éloigné ⁽¹⁵¹⁾. Le Privacy Act de 1974 ⁽¹⁵²⁾ établit un système de protection des données, mais uniquement pour les autorités publiques.

Au-delà de l'Europe et des États-Unis, l'environnement *mondial* de la protection de la vie privée est très varié ⁽¹⁵³⁾. La *charte africaine des droits de l'homme et des peuples* ⁽¹⁵⁴⁾ ne prévoit aucune protection explicite de la vie privée. En *Chine*, la protection de la vie privée existe, mais sans véritable garantie constitutionnelle ni loi sur la vie privée ou la protection des données, même si le pays subit de plus en plus de pression pour faire évoluer cette situation. Jusqu'à récemment, l'*Asie du Sud* était nettement en retard dans la préservation de la protection des données et de la vie privée, mais récemment la situation en Inde a radicalement changé, notamment grâce à la jurisprudence de la Cour constitutionnelle et la mise en place d'un vaste projet de loi sur la confidentialité. En *Argentine*, en *Afrique du Sud* et au *Mexique*, les constitutions nationales incluent un droit à part entière à la vie privée.

Par défaut, la confidentialité interdit les ingérences de l'État et des acteurs privés dans l'autonomie des individus: elle les protège des intrusions. L'ampleur et la portée de la vie privée sont, toutefois, indéterminées, puisqu'il appartient aux juges de décider lorsque la vie privée est en jeu et lorsque leur protection peut être légitimement invoquée. En Europe, la base juridique pour la protection de la vie privée se trouve dans la Convention européenne des droits de l'homme: ⁽¹⁵⁵⁾

⁽¹⁴⁷⁾ <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>

⁽¹⁴⁸⁾ www.echr.coe.int/Documents/Convention_ENG.pdf

⁽¹⁴⁹⁾ www.europarl.europa.eu/charter/pdf/text_en.pdf

⁽¹⁵⁰⁾ http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.htm

⁽¹⁵¹⁾ T. Mendel, A. Puddephatt, B. Wagner et al., «Global Survey on Internet Privacy and Freedom of Expression», UNESCO, 2012, p. 87-89.

⁽¹⁵²⁾ <http://www.justice.gov/opcl/privstat.htm>

⁽¹⁵³⁾ L'enquête mondiale de l'UNESCO sur la protection de la vie privée sur Internet et la liberté d'expression, 2012. Voir unesdoc.unesco.org/images/0021/002182/218273e.pdf

⁽¹⁵⁴⁾ www.achpr.org/instruments/achpr/

⁽¹⁵⁵⁾ http://www.echr.coe.int/Documents/Convention_FRA.pdf

«Article 8 — Droit au respect de la vie privée et familiale:

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

La protection, très forte en Europe, de la vie privée se reflète dans la pratique de la Cour européenne des droits de l'homme, qui est en général à la fois dynamique et progressiste dans ses interprétations des droits de l'homme. À de nombreuses reprises, cette Cour a souligné que la Convention européenne était «un instrument vivant qui doit être interprété à la lumière de la situation actuelle» ⁽¹⁵⁶⁾. Dans le même sens, la Cour a souligné à maintes reprises que la Convention visait à garantir «non pas des droits théoriques et illusoire, mais concrets et effectifs». Cette méthode d'interprétation efficace ouvre la voie à l'élargissement de la protection offerte par la Convention et est très fiable lorsqu'il est question de nouveaux développements technologiques dans le domaine de la surveillance qui défient les droits de l'homme d'une manière qu'il n'était pas possible de prévoir lors de la rédaction originale de la Convention. Il a toutefois été avancé que la Cour avait souvent hésité à faire appliquer l'article 8 à différentes formes de traitement des données (données écrites; données biométriques; données visuelles) dans les bases de données ⁽¹⁵⁷⁾.

⁽¹⁵⁶⁾ Cette phrase est apparue dans de nombreux arrêts de la Cour depuis la création de la CEDH. Voir G. Letsas, «ECHR as a Living Instrument: its Meaning and Legitimacy» dans G. Ulfstein, A. Follesdal et B. Peters (eds), *Constituting Europe: The European Court of Human Rights in a National, European and Global Context*, Cambridge University Press (2013), p. 106-141.

⁽¹⁵⁷⁾ Paul De Hert, *Balancing security and liberty with the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11*, *Utrecht Law Review*, 2005, p. 74.

La Cour a estimé que l'utilisation d'une série de mesures de surveillance spécifiques constituait une ingérence dans le droit à la vie privée tel qu'énoncé à l'article 8 de la Convention européenne des droits de l'homme.

Ces 30 dernières années, l'interception des communications par la police, y compris l'interception de messages enregistrés sur le bipeur d'un requérant, l'interception judiciaire de communications, la mise sur écoute d'appartements, l'enregistrement des voix, la divulgation dans les médias de séquences filmées dans une rue par une télévision en circuit fermé (vidéosurveillance), les enregistrements vidéo sans préavis d'une personne sur son lieu de travail, la surveillance des courriels, et le suivi par GPS, ont tous été considérés comme des atteintes à l'article 8. Plus généralement, la Cour a estimé que la simple mémorisation d'informations touchant la vie privée d'un individu par une autorité publique constituait une violation. L'utilisation ultérieure de ces informations stockées n'a aucune incidence sur cette conclusion. Dernier point, mais non le moindre, la Cour a indiqué qu'il y avait atteinte à la vie privée même lorsque l'individu ne pouvait démontrer en avoir été personnellement affecté. L'atteinte au droit à la vie privée n'est pas, en tant que telle, illégale, conformément à la Convention et à la Cour, si l'utilisation de la mesure de surveillance a lieu conformément à la loi, qu'elle poursuit l'un ou plusieurs des buts légitimes visés à l'article 8, paragraphe 2, de la Convention et qu'elle est «nécessaire dans une société démocratique» pour atteindre les objectifs poursuivis... ⁽¹⁵⁸⁾

Pour que les mesures de surveillance respectent la CEDH, elles doivent se fonder sur un droit interne particulièrement précis, offrant aux citoyens une indication correcte des conditions et des circonstances dans lesquelles les autorités sont habilitées à recourir à de telles mesures. La loi doit être accessible à la personne concernée, qui doit être en mesure d'en prévoir les conséquences pratiques. Lorsque des mesures de surveillance secrète sont utilisées, la Cour a développé des garanties minimales qui doivent être énoncées dans la loi, afin d'éviter tout abus de pouvoir.

⁽¹⁵⁸⁾ R. Bellanova, D. Bigo, V. Coroama et al., 'Smart Surveillance — State of the Art' Report of the SAPIENT project, 2012, p. 88-89: <http://www.sapienproject.eu/docs/D1.1-State-of-the-Art-submitted-21-January-2012.pdf>

CHAPITRE II. | GOUVERNANCE — PRÉSENTATION, DÉFIS, POSSIBILITÉS

Quelques affaires peuvent illustrer cela :

Une affaire de 2009 ⁽¹⁵⁹⁾ a eu des implications sur la collecte, le stockage, l'échange et l'utilisation des données biométriques par toutes les parties à la Convention. La pratique britannique de maintenir indéfiniment les empreintes digitales et l'ADN des personnes qui ne sont pas déclarées coupables d'une infraction a été considérée comme une violation de l'article 8 ⁽¹⁶⁰⁾.

En l'occurrence, la Cour a constaté que la durée et la nature aveugle de la rétention ne permettaient pas d'assurer un juste équilibre entre les préoccupations d'ordre public et les droits à la vie privée, et qu'elles ne pouvaient être jugées nécessaires dans une société démocratique.

Un autre arrêt a considéré que les pouvoirs accordés à la police par la loi de 2000 sur le terrorisme pour arrêter et fouiller les personnes violaient l'article 8, dans la mesure où ils n'étaient ni suffisamment circonscrits ni soumis à des garanties juridiques adéquates contre les abus. En tant que telle, la Cour a considéré que les pouvoirs n'étaient pas « conformes à la loi », en violation de l'article 8 ⁽¹⁶¹⁾.

2.2.2. La sécurité comme justification pour restreindre la protection de la vie privée

L'intérêt pour la sécurité constitue un objectif légitime pour limiter ou enfreindre les droits de l'homme. Comme le souligne van Kempen, « la législation en matière de droits de l'homme offre aux autorités la possibilité de restreindre l'éventail des droits ou l'exercice de ceux-ci au nom de la sécurité nationale. Ces intérêts portent notamment sur la sécurité publique, la prévention des troubles ou de la criminalité ou, plus précisément, la défense de toute personne contre la violence illégale ou la prévention contre la récidive, les menaces pour la santé ou, plus spécifiquement, la propagation des maladies infectieuses, la moralité publique, le bien-être économique du pays et/ou

les libertés et droits fondamentaux d'autrui » ⁽¹⁶²⁾. En d'autres termes, la sécurité personnelle d'autrui peut justifier la restriction d'un droit de l'homme.

Dans la Convention européenne des droits de l'homme, le deuxième paragraphe de l'article 8 prévoit la possibilité de restreindre le droit à la vie privée dans certains cas. D'une manière générale, la Cour a déclaré qu'une atteinte sera jugée « nécessaire dans une société démocratique » pour un objectif légitime si elle répond à un « besoin social impérieux » et, en particulier, si elle est proportionnée au but légitime poursuivi et si les motifs invoqués par les autorités nationales pour la justifier sont « pertinents et suffisants ». La Cour n'accorde généralement pas une grande importance aux avantages potentiels des technologies de surveillance, mais des statistiques ont été utilisées pour critiquer la proportionnalité des écoutes téléphoniques dans deux affaires.

Ce qui est particulièrement inquiétant dans ce contexte, c'est l'interprétation large de la notion de « sécurité » comme motif visant à limiter la confidentialité, dans la mesure où elle risque de devenir une clause « fourre-tout ». Comme le fait remarquer van Kempen ⁽¹⁶³⁾ :

« De nombreux motifs de limitation des droits de l'homme sont interprétés et appliqués de façon plutôt large, et certains d'entre eux font même office de facto de clause fourre-tout. En outre, bien que la portée et la signification de quelques rares clauses de limitation ressortent assez précisément de la jurisprudence des organes de défense des droits de l'homme (...) aucune d'entre elles ne bénéficient de définitions précises dans l'un ou l'autre des traités relatifs aux droits de l'homme ou la jurisprudence qui s'y rapporte. En outre, le Comité des droits de l'homme et la Cour européenne des droits de l'homme ont rarement conclu que l'objectif d'une limitation des droits de l'homme n'avait pas un but légitime au sens de la clause de limitation du traité. Ils examinent plutôt en général si l'atteinte était nécessaire et proportionnée au but légitime supposé. Le droit relatif aux droits de l'homme est donc très casuistique dans ses éclaircissements et la plus grande part des motifs de limitation n'aide que très marginalement à définir ce que la sécurité nationale ou d'autres formes de sécurité englobent exactement (...).

⁽¹⁵⁹⁾ S et Marper c. Royaume-Uni, 30562/04 [2008] CEDH 1581.

⁽¹⁶⁰⁾ Voir : <http://www.bailii.org/eu/cases/ECHR/2008/1581.html>

⁽¹⁶¹⁾ Voir : <http://www.bailii.org/eu/cases/ECHR/2010/28.html>

⁽¹⁶²⁾ Piet Hein van Kempen, Four concepts of security — a human rights perspective, Human Rights Review, 2013, p. 13.

⁽¹⁶³⁾ Idem p. 13-15.

Il convient de remarquer que la législation relative aux droits de l'homme ne fournit pas d'approche plus fondamentale de l'exigence de but légitime pour contrôler et limiter quelque peu la politisation ou même l'exploitation de la sécurité.

Van Kempen poursuit et conclut enfin que la législation relative aux droits de l'homme devrait fournir «un concept général et plus substantiel de la sécurité en tant que motif de restriction des droits de l'homme. Dans le cadre de ce concept, la législation relative aux droits de l'homme se doit de souligner que le référent pour la sécurité et la politique de sécurité est finalement l'individu. Elle doit en outre s'opposer à la tendance à vouloir tout qualifier de problème de sécurité.»

2.2.3. La sûreté en tant que droit de l'homme à part entière

Selon le Conseil européen, «la sécurité est en elle-même un droit fondamental» ⁽¹⁶⁴⁾. Même si cette déclaration semble pour le moins définitive, il n'est pas facile d'évaluer ses implications et son importance, dans la mesure où coexistent différentes conceptions de la sécurité en tant que droit de l'homme. Celles-ci englobent des garanties négatives de sûreté individuelle contre l'État et des garanties positives de sûreté obligeant l'État à protéger les individus contre les autres individus ⁽¹⁶⁵⁾.

a) La sûreté en tant que droit individuel négatif contre les intrusions de l'État

Les droits de l'homme trouvent leur origine dans les définitions de la liberté de l'individu contre l'oppression et l'exercice du pouvoir par le souverain et, plus tard, l'État. Les droits de l'homme impliquent tous une obligation négative de la part des autorités, ce qui signifie que tous les droits de l'homme tendent à protéger les individus du pouvoir de l'État. Presque tous les droits de l'homme énumérés dans la Convention européenne des droits de

l'homme et de la charte des droits fondamentaux sont pertinents dans cette perspective de la sécurité.

Comme le pouvoir de l'État en tant que tel est infini, la notion de sûreté négative revêt une importance majeure pour réduire et contrôler ce pouvoir. Toutefois, au sens large, la sûreté humaine est également un concept ouvert et vague. La définition de la «sécurité» du Conseil européen recoupe cette vaste notion de sûreté individuelle négative, mais est encore plus large, car rien ne dit qu'elle ne protège l'individu que de l'État.

En dehors de la notion plus large de sûreté individuelle négative contre l'État, le droit européen relatif aux droits de l'homme implique également une sûreté négative dans un sens plus étroit et en même temps plus explicite. Le premier paragraphe de l'article 5 (droit à la liberté et à la sûreté) de la Convention européenne des droits de l'homme dispose ⁽¹⁶⁶⁾:

1. Toute personne a droit à la liberté et à la sûreté. Nul ne peut être privé de sa liberté, sauf dans les cas suivants et selon les voies légales.

Van Dijk et al. ⁽¹⁶⁷⁾ signalent le sens restreint de la notion de «sûreté de la personne» à l'article 5, paragraphe 1: «À l'article 5, les droits à la liberté et à la sûreté sont mentionnés conjointement, tandis que dans la partie suivante de l'article, seul le droit à la liberté est développé.»

Il est intéressant de noter que l'article 6 de la charte des droits fondamentaux de l'Union européenne contient une disposition similaire à celle de l'article 5, paragraphe 1, de la Convention européenne:

«Toute personne a droit à la liberté et à la sûreté».

Dans leur commentaire sur la charte des droits fondamentaux, le Réseau d'experts indépendants de l'UE en

⁽¹⁶⁴⁾ European Council, Internal Security Strategy for the EU: Towards an Internal Security Model, 2010, p. 19: http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC-3010313FRC.pdf

⁽¹⁶⁵⁾ Piet Hein van Kempen, Four concepts of security — a human rights perspective, Human Rights Review, 2013, p. 16.

⁽¹⁶⁶⁾ Voir également l'article 9, paragraphe 1, du Pacte international relatif aux droits civils et politiques (PIDCP) de l'ONU: «Toute personne a droit à la liberté et à la sûreté. Nul ne peut faire l'objet d'une arrestation ou d'une détention arbitraire. Nul ne peut être privé de sa liberté, sauf dans les cas suivants et selon les voies légales.»

⁽¹⁶⁷⁾ P. Van Dijk et al., Theory and practice of the European Convention on Human Rights, Antwerpen-Oxford, Intersentia, 4^e Édition, 2006, p. 457.

CHAPITRE II. | GOUVERNANCE — PRÉSENTATION, DÉFIS, POSSIBILITÉS

matière de droits fondamentaux pointe les principes relatifs à la sûreté et déclare ce qui suit ⁽¹⁶⁸⁾:

«Il est toutefois plus difficile de définir la signification et la portée du droit à la sûreté. Le Comité des droits de l'homme interprète le droit à la sûreté dans l'article 9 du PIDCP, depuis l'affaire Delgado Paéz c. Colombie de 1990, comme un droit indépendant correspondant à l'obligation de l'État de prendre les mesures raisonnables et appropriées pour protéger les individus qui font l'objet de menaces de mort et d'autres menaces graves contre leur sûreté. Bien que cette interprétation corresponde à la signification habituelle du droit à la sûreté, au sens où on l'entend depuis les premiers documents traitant des droits de l'homme durant la Révolution française, la Cour européenne des Droits de l'homme ne lui a jamais conféré un sens allant au-delà de la liberté personnelle au droit à la sûreté de l'article 5 de la CEDH, en dépit de l'importance croissante accordée aux questions de sécurité dans les discours modernes sur les droits de l'homme.»

Lors de la rédaction de l'article 6 de la charte, le terme «sûreté» a généré de nombreuses controverses, et certains membres ont proposé de le supprimer purement et simplement, au motif qu'il pourrait donner lieu à des interprétations différentes dans certains États membres de l'UE, notamment en France, en Italie et en Allemagne. La Convention (rédaction de la charte), cependant, a décidé de maintenir le terme dans le sens restrictif de la jurisprudence de la Cour européenne en vertu de l'article 5 CEDH ⁽¹⁶⁹⁾.

Un document de travail des services de la Commission européenne ⁽¹⁷⁰⁾ avertit que:

⁽¹⁶⁸⁾ Réseau d'experts indépendants de l'UE en matière de droits fondamentaux, Commentaire de la Charte des droits fondamentaux de l'Union européenne: http://ec.europa.eu/justice/fundamental-rights/files/networkcommentaryfinal_en.pdf

⁽¹⁶⁹⁾ Réseau d'experts indépendants de l'UE en matière de droits fondamentaux, Commentaire de la Charte des droits fondamentaux de l'Union européenne, p. 68.

⁽¹⁷⁰⁾ Document de travail des services de la Commission, Orientations opérationnelles sur la prise en compte des droits fondamentaux dans les analyses d'impact de la Commission, Bruxelles, 6.5.2011 SEC(2011) 567 final, p. 8.

Il serait toutefois erroné de considérer ce droit (le droit à la sûreté) comme une garantie abstraite de «protection» par l'État et comme un prétendu droit à la «sécurité publique». En réalité, l'article 6 de la charte garantit les mêmes droits que l'article 5 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (ou Convention européenne des droits de l'homme, CEDH), et a le même sens et la même portée. En ce qui concerne l'interprétation de l'article 5 de la CEDH, la Cour européenne des droits de l'homme a invariablement statué que «l'article 5 vise la liberté individuelle dans son acception classique, c'est-à-dire la liberté physique de la personne (...). L'expression «sûreté» doit aussi s'entendre au sens de liberté physique plutôt que de sécurité physique. Le choix du terme «sûreté» sert simplement à souligner l'exigence selon laquelle la détention ne peut pas être arbitraire (...).

Van Kempen conclut que «le droit négatif à la sûreté (dans l'article 5 de la Convention européenne et l'article 6 de la charte) revêt tout au plus une importance marginale au sein du concept (plus large) de sûreté négative» ⁽¹⁷¹⁾.

Sur la base des arguments ci-dessus, il est probablement juste de dire que la notion de sécurité du Conseil européen n'est pas protégée par le droit négatif à la sûreté de l'article 5 de la Convention européenne et de l'article 6 de la charte.

b) La sûreté en tant qu'obligation positive de l'État envers les individus

Cette notion de sûreté signifie que la protection des droits de l'homme engage l'État à prendre des mesures appropriées en cas de violation de ce droit par autrui. «La substance de cette notion est donc la garantie apportée par les autorités d'une sûreté positive pour les individus dans la société nationale contre les différents fonctionnaires et — plus particulièrement — d'autres parties» ⁽¹⁷²⁾. Les organes de contrôle des droits de l'homme, tels que la Cour européenne, ont expressément formulé les devoirs de l'État à engager des poursuites pénales contre les personnes tenues responsables de violer les valeurs sur lesquelles ces

⁽¹⁷¹⁾ Piet Hein van Kempen, Four concepts of security — a human rights perspective, Human Rights Review, 2013, p. 11.

⁽¹⁷²⁾ Piet Hein van Kempen, Four concepts of security — a human rights perspective, Human Rights Review, 2013, p. 16.

droits sont basés, à les juger et à les punir. Par exemple, pour protéger le droit à la vie (article 2 de la Convention européenne), la Cour européenne maintient que l'État a pour devoir principal de mettre en place des dispositions de droit pénal permettant de dissuader la commission d'infractions contre les personnes.

Ces obligations sont en outre pertinentes pour certaines violations du droit à ne pas subir de torture et de mauvais traitements, du droit au respect de la vie privée et des libertés d'expression, de religion et d'assemblée. Toujours selon cet auteur «le développement du concept des droits de l'homme de sûreté positive contre d'autres parties renforce considérablement la capacité de ces individus et de ces groupes à contraindre les autorités à les respecter et donc à contrer les menaces auxquelles ils sont confrontés au sein de la société. En outre, le concept reconnaît que les contraintes sur la liberté, l'autonomie et les capacités des individus peuvent ne résulter de l'exercice du pouvoir de l'État, mais qu'elles découlent de forces sociales et du comportement de certains individus, groupes et organisations». Alors que certains chercheurs (notamment van Kempen) émettent de sérieuses objections à l'encontre de l'utilisation du droit pénal pour faire respecter ces obligations positives, ils admettent néanmoins la nécessité «de reconnaître que la sûreté globale est une condition préalable essentielle à l'exercice de la liberté en tant que tel» ⁽¹⁷³⁾.

2.3. Réglementation en matière de surveillance

2.3.1. Jurisprudence

Un grand nombre de règlements couvre la surveillance, cependant ce domaine est traité principalement au niveau national et la législation nationale en matière de surveillance diffère considérablement entre les pays en Europe et dans le monde. En outre, il n'y a guère de précédent en faveur d'un consensus ou d'une coopération dans ce domaine, probablement en partie en raison de la nouveauté de la question, de l'émergence d'approches nationales divergentes et du fait que cela est étroitement lié aux questions de sécurité nationale et de police.

L'UE dispose d'un certain nombre de règlements, de résolutions, de rapports, etc. sur le thème de la surveillance, que ce soit la vidéosurveillance ou la surveillance des télécommunications. Des références peuvent

être faites, notamment à la résolution du Conseil sur les télécommunications de 1995 ⁽¹⁷⁴⁾ et à l'article 16 du traité sur le fonctionnement de l'Union européenne — circulation des données personnelles au sein de l'UE — souvent invoqué pour les questions de «sécurité» ⁽¹⁷⁵⁾.

2.3.2. Caméras de surveillance – vidéosurveillance

La réglementation de la vidéosurveillance en Europe a lieu au niveau national. Si la vidéosurveillance n'est pas courante dans les lieux publics en France, en Allemagne, en Grèce et en Espagne, le Royaume-Uni y a quant à lui largement recours. De nombreux pays européens reconnaissent explicitement que la vidéosurveillance dans les lieux publics est en conflit avec le droit à la vie privée. Une réglementation est donc souvent jugée nécessaire et souhaitable ⁽¹⁷⁶⁾. Les systèmes de permis pour les utilisateurs privés souhaitant surveiller un espace public sont courants. La police dispose souvent de son côté d'un cadre plus large pour utiliser la vidéosurveillance. La loi peut limiter effectivement le recours à la vidéosurveillance et proposer une tribune où faire valoir des critiques, des préoccupations et des limitations légitimes lors d'une demande de permis.

Certains exemples de règlements nationaux relatifs à la vidéosurveillance sont présentés ci-dessous pour donner un aperçu de l'éventail des systèmes réglementaires en vigueur en Europe. Il ne s'agit pas de donner une vue générale de tous les pays. Notre intention n'étant pas de fournir un examen complet, mais d'illustrer les différences entre les diverses formes de règlement, il est important de présenter les exemples suivants.

a) Allemagne

En *Allemagne*, la situation juridique est compliquée par le fait que certains aspects de l'utilisation de la vidéosurveillance, tels que le stockage et l'analyse des données acquises par le biais de dispositifs optico-électroniques, sont réglementés au niveau fédéral et d'autres

⁽¹⁷⁴⁾ Résolution du Conseil, du 7 janvier 1995 relative à l'interception légale des télécommunications (96/C329/01).

⁽¹⁷⁵⁾ Voir: http://ec.europa.eu/justice/data-protection/law/treaty/index_en.htm et http://eur-lex.europa.eu/resource.html?uri=cellar:ccccda77-8ac2-4a25-8e66-a5827ecd3459.0010.02/DOC_1&format=PDF

⁽¹⁷⁶⁾ Marianne L. Gras: «The Legal Regulation of CCTV in Europe», 2004.

⁽¹⁷³⁾ Idem, p. 17.

CHAPITRE II. | GOUVERNANCE — PRÉSENTATION, DÉFIS, POSSIBILITÉS

au niveau des États («Länder»). En général, comparativement à d'autres États membres, l'Allemagne est dotée d'un cadre réglementaire relativement strict sur la protection des données lorsqu'il s'agit de vidéosurveillance. Le principe directeur est le droit à l'autodétermination en matière d'information. Dans sa décision sur le recensement de la population, la Cour constitutionnelle fédérale a «inventé» ce droit fondamental en 1983 à partir de l'article 2, paragraphe 1, de sa législation de base («Droit général de la personnalité») en combinaison avec l'article 1, paragraphe 1, de sa législation de base («Dignité») en appliquant ces droits au domaine de la protection des données. Bien que certains règlements spécifiques relatifs à la vidéosurveillance obligatoire de certaines zones particulières existent (bureaux de banque, entrées de salles de jeu), l'usage privé de la vidéosurveillance est strictement limité (objet, proportionnalité, pertinence, efficacité, obligation de supprimer et/ou d'informer la personne concernée) conformément à l'article 6, point b, de la loi fédérale sur la protection des données (BDSG) ⁽¹⁷⁷⁾. Le droit d'un propriétaire d'installer et d'utiliser un système de vidéosurveillance est limité par plusieurs dispositions et, une fois encore, par le droit concomitant des personnes affectées à l'autodétermination de l'information.

L'utilisation de fibres optiques des appareils électroniques par les organismes publics est régie par les différentes lois de police des différents États et/ou les lois relatives à la protection des données. Les règlements diffèrent légèrement en ce qui concerne la portée de l'utilisation de la vidéosurveillance, la profondeur de l'intervention, la période de stockage, mais elles respectent toutes le droit à l'autodétermination en matière d'information (sauf en cas d'enquête pénale où cette exigence n'est pas nécessaire pour une période de temps déterminée et dans un but spécifique).

b) France

En France, l'autorisation, la mise en œuvre et le contrôle des installations de vidéosurveillance sont assurés par la Commission nationale de vidéoprotection ⁽¹⁷⁸⁾ créée par la loi d'orientation et de programmation pour la

performance de la sécurité intérieure ⁽¹⁷⁹⁾. Le conseil de cette commission nationale de vidéoprotection, installé le 4 janvier 2012 au ministère de l'intérieur, est également chargé de conseiller et d'évaluer l'efficacité de la vidéosurveillance au terme du décret du 25 juillet 2011. À ce titre, il est chargé d'émettre des recommandations concernant les caractéristiques, le fonctionnement et l'emploi des dispositifs de vidéoprotection ⁽¹⁸⁰⁾. Ses membres comprennent cinq représentants des personnes publiques et privées autorisées à mettre en œuvre un système de vidéoprotection; cinq représentants du ministère de l'intérieur; le délégué interministériel à la sécurité privée; un membre de la commission nationale informatique et liberté; deux députés et deux sénateurs; quatre personnes désignées au titre des personnalités qualifiées (un magistrat du siège, un magistrat du parquet et deux personnes nommées par le ministre de l'intérieur en raison de leurs compétences dans le domaine de la vidéoprotection ou des libertés individuelles). Les autorisations doivent être demandées via une procédure de demande adressée à la préfecture compétente (du département où le système sera installé) par courrier ou en ligne ⁽¹⁸¹⁾. Le débat public sur le recours à la vidéosurveillance en France est divisé entre ceux qui défendent ce «nouvel outil» comme un moyen de faciliter les enquêtes et de rassurer le public, et ceux qui le perçoivent comme une violation des libertés civiles, au rapport coûts-bénéfices disproportionné. En octobre 2013, un rapport du Sénat ⁽¹⁸²⁾ a formulé des recommandations pour un moratoire sur les investissements relatifs aux systèmes de vidéoprotection et la création d'un indicateur de performance.

⁽¹⁷⁹⁾ Loi d'orientation et de programmation pour la performance de la sécurité intérieure (généralement désigné par son acronyme LOPPSI), 14 mars 2011.

⁽¹⁸⁰⁾ La Commission nationale de la vidéoprotection est tenue de rédiger un rapport annuel au Parlement pour évaluer l'efficacité de la vidéoprotection et proposer des recommandations.

⁽¹⁸¹⁾ <http://www.interieur.gouv.fr/Videoprotection/Tele-procedure>

⁽¹⁸²⁾ Rapport d'information n° 91 fait au nom de la commission des finances sur les investissements dans la police et la gendarmerie, par M. Jean-Vincent Placé, sénateur (enregistré à la Présidence du Sénat le 22 octobre 2013). Recommandation n° 5: Décider d'un moratoire sur les investissements relatifs à la vidéoprotection, dans l'attente d'une étude scientifique indépendante sur la contribution réelle de la vidéosurveillance en matière de sécurité (en termes de taux de liquidation des dossiers, de lutte contre la délinquance, de sentiment de sécurité, d'aspects psychosociaux, de suppression de la présence humaine, de garanties des libertés civiles,...). Recommandation n° 6: Créer un indicateur de performance pour les dispositifs de vidéoprotection (par ex. mesurer le nombre de cas résolus grâce à ce type de dispositif).

⁽¹⁷⁷⁾ La version anglaise est disponible à l'adresse suivante: http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile

⁽¹⁷⁸⁾ Commission nationale de la vidéoprotection, <http://www.interieur.gouv.fr/Videoprotection/La-commission-nationale-de-vidioprotection>

c) Pologne

En *Pologne*, il n'existe pas de législation uniforme régissant l'installation et l'utilisation de systèmes de vidéosurveillance. La législation relative à la sécurité dans les grandes manifestations publiques (les sports de plein air, les matchs de football) ⁽¹⁸³⁾ impose l'installation d'un système de vidéosurveillance pour en assurer le contrôle. En outre, les services en uniforme (gardes-frontières, agence de sécurité intérieure, police et gardes municipaux) sont autorisés à utiliser la vidéosurveillance en vertu des règlements applicables à leur travail. De même, le droit bancaire autorise la vidéosurveillance pour assurer la sécurité des biens et des clients des banques (Journal officiel 2012, article 1376). En outre, l'administration locale (villes, comtés) peut introduire des résolutions autorisant l'installation de systèmes de vidéosurveillance dans l'intérêt de la sécurité publique. Depuis un certain temps maintenant, les médiateurs pour la protection des droits civils et des données à caractère personnel et plusieurs ONG exhortent le ministère de l'intérieur et l'administration d'accélérer leurs travaux d'élaboration d'une législation spécifique régissant la vidéosurveillance, en soulignant que, dans de nombreux cas, des systèmes de vidéosurveillance ont été installés sans aucun motif juridique. En outre, de récents sondages suggèrent que, dans 42 % des villes polonaises, il n'y a aucune information disponible sur les lieux surveillés et que 35 % des citoyens n'ont pas été consultés avant l'installation de systèmes de vidéosurveillance.

d) Portugal

Au *Portugal*, la vidéosurveillance est régie par la loi sur la protection des données ⁽¹⁸⁴⁾ et est en outre couverte par un ensemble de lois et de règlements spécifiques, qui dépendent de l'entité concernée et de la finalité de la surveillance. La vidéosurveillance par des entités privées est soumise à une autorisation préalable de la Commission nationale de protection des données et à un enregistrement auprès de la police de sécurité publique. D'autre part, la vidéosurveillance assurée par les forces de sécurité est soumise à une autorisation préalable du gouvernement, après avis de la Commission nationale de protection des données ⁽¹⁸⁵⁾. Il existe également des régimes spéciaux pour la vidéosurveillance dans les

taxis et les services de surveillance routière, mais une autorisation de la Commission nationale de protection des données ou une notification de cette même autorité reste toujours nécessaire. La Commission nationale de protection des données est un organe indépendant doté d'un pouvoir d'exécution, responsable de veiller au respect des lois et des règlements dans le domaine des données à caractère personnel.

e) Pays-Bas

Aux *Pays-Bas*, les autorités doivent introduire une demande au conseil municipal pour pouvoir installer des caméras de vidéosurveillance. Celle-ci est examinée en fonction des besoins locaux. La surveillance ne peut être secrète (sauf si cela s'avère nécessaire pour détecter une infraction précise); être destinée à un but bien défini pour détecter ou poursuivre des infractions ou des comportements déterminés; et être jugée nécessaire pour que le propriétaire puisse s'acquitter de ses fonctions. Les devoirs d'une personne privée sont considérés comme limités à son ou ses propres biens. Les lieux publics sont de la responsabilité du maire, assisté par la police. Des mesures moins intrusives doivent être envisagées non seulement avant l'installation, mais aussi régulièrement lors de l'examen du système de vidéosurveillance. Il est possible d'introduire une plainte au conseil local et par voie d'assignation devant un tribunal en cas de surveillance inadaptée. En outre, le Conseil pour la protection des données a le devoir de superviser la vidéosurveillance et dispose de pouvoirs d'inspection. Pour consolider le règlement, le gouvernement néerlandais a élaboré des lois pour la vidéosurveillance et a expressément interdit l'usage secret de la vidéosurveillance dans les lieux publics ⁽¹⁸⁶⁾.

f) Danemark

Le *Danemark* dispose de règlements très stricts en matière de vidéosurveillance ⁽¹⁸⁷⁾ — plus stricts que la plupart des pays européens. La vidéosurveillance est généralement interdite dans les espaces publics, lorsqu'elle est effectuée par des personnes privées. Il existe, toutefois, un certain nombre d'exceptions

⁽¹⁸³⁾ Loi du 20 mars 2009, Journal officiel 2013 art. 6114.

⁽¹⁸⁴⁾ Voir en anglais: <http://www.cnpd.pt/english/bin/legislation/Law6798EN.HTM>

⁽¹⁸⁵⁾ http://www.cnpd.pt/english/index_en.htm

⁽¹⁸⁶⁾ Surveillance & Society CCTV Special (eds. Norris, McCall and Wood) 2(2/3): p. 216-229 <http://www.surveillance-and-society.org/cctv.htm> et [http://www.surveillance-and-society.org/articles2\(2\)/regulation.pdf](http://www.surveillance-and-society.org/articles2(2)/regulation.pdf)

⁽¹⁸⁷⁾ Voir les références dans la note de bas de page n° 186: La réglementation remonte à 1982, mais a été révisée à plusieurs reprises.

CHAPITRE II. | GOUVERNANCE — PRÉSENTATION, DÉFIS, POSSIBILITÉS

pour les propriétaires de certains types de propriétés, tels que les stations-service, les usines, les centres commerciaux, les banques, les distributeurs automatiques de billets, etc. De plus, des exceptions peuvent être faites dans certains cas à des fins préventives. Une telle autorisation peut être accordée pour une période de cinq ans. Lorsqu'une surveillance est mise en place, il y a lieu de prévoir une signalisation ou tout autre moyen d'information. Les autorités et les forces de police sont autorisées à recourir aux systèmes de vidéosurveillance et cette dernière peut le faire secrètement. Ces exceptions peuvent sembler importantes, mais l'interdiction générale reste la règle. L'approche danoise de la réglementation en matière de vidéosurveillance est cependant plutôt unique en Europe.

g) Royaume-Uni

Au *Royaume-Uni*, l'ampleur de la surveillance des télécommunications est assez conséquente (on estime que 1,85 million de caméras de vidéosurveillance sont utilisées en Grande-Bretagne, la très grande majorité par des entreprises privées ⁽¹⁸⁸⁾). Dans le même temps, le Royaume-Uni offre un exemple intéressant de gouvernance dernier cri, avec son code de pratique introduit en 2013.

Le ministère britannique de l'intérieur a publié le «Surveillance Camera Code of Practice» ⁽¹⁸⁹⁾ en juin 2013, avec 12 principes directeurs fournissant des conseils sur l'utilisation appropriée et efficace des systèmes de vidéosurveillance par les autorités britanniques concernées (principalement la police et les autorités locales), qui sont tenues de se plier à ce code lorsqu'elles exercent des fonctions couvertes par celui-ci. Les autres opérateurs et utilisateurs de systèmes de vidéosurveillance au Royaume-Uni sont encouragés à adopter le code sur une base volontaire. Selon le gouvernement britannique, le code est perçu comme «une étape importante pour respecter l'engagement pris par le gouvernement de mettre en place une nouvelle réglementation de la vidéosurveillance, une tâche qu'il juge préférable de gérer de façon graduelle et progressive» ⁽¹⁹⁰⁾.

Le gouvernement a indiqué qu'il pourrait plus tard inclure d'autres organismes que les autorités compétentes qui devront eux aussi respecter le code, conscient que les caméras de vidéosurveillance forment un environnement complexe en termes de propriété et d'exploitation.

Le rapport insiste sur le fait que le gouvernement est tout à fait favorable à l'utilisation visible de caméras de surveillance dans les espaces publics, pourvu que cette utilisation: poursuive un objectif légitime; soit nécessaire pour répondre à un besoin pressant; soit proportionnée, efficace et compatible avec les obligations juridiques pertinentes. Le but déclaré du code est de veiller à ce que les individus et les communautés dans leur ensemble comprennent que les caméras de vidéosurveillance sont déployées en vue de les protéger et de les soutenir, et non de les espionner. Le gouvernement estime que là où la vidéosurveillance d'espaces publics poursuit un but légitime et répond à un besoin pressant, cette surveillance doit être considérée comme une surveillance par consentement et que ce consentement par la communauté doit être informé et non pas assumé par un gestionnaire de réseau. Ici, le gouvernement dresse une analogie avec ce qu'on appelle «le maintien de l'ordre par consentement», en d'autres termes le consentement implicite du public d'être contrôlé par les autorités de répression et la légitimité de ces autorités qui découle de la transparence de leurs pouvoirs témoignent de leur intégrité dans l'exercice de ces pouvoirs et de leur responsabilité en la matière. Le code a été développé pour répondre aux préoccupations relatives aux risques d'abus ou de détournement de la surveillance par l'État dans des lieux publics, en mettant d'abord l'accent sur la réglementation des activités des autorités locales et de la police. Pour soutenir l'application pratique des principes directeurs par un gestionnaire de réseau, le commissaire chargé de la vidéosurveillance fournira des informations et des conseils sur les normes opérationnelles et techniques approuvées et appropriées.

Les principes directeurs se concentrent sur les éléments suivants:

1. Un but précis est nécessaire, la surveillance doit poursuivre un objectif légitime et répondre à un besoin pressant.
2. Les effets sur les personnes et leur vie privée doivent être pris en considération.
3. L'utilisation d'un système de vidéosurveillance doit être aussi transparente que possible.

⁽¹⁸⁸⁾ <http://www.theguardian.com/uk/2011/mar/02/cctv-cameras-watching-surveillance>

⁽¹⁸⁹⁾ Le Code de pratique est émis par le secrétaire d'État au titre de la Section 30 de la loi 2012.

⁽¹⁹⁰⁾ Home Office (2013) Surveillance Camera Code of Practice, disponible à l'adresse suivante: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

4. Il convient d'assumer clairement la responsabilité de toutes les activités de vidéosurveillance.
5. Des règles, des politiques et des procédures claires doivent être mises en place avant le recours à la vidéosurveillance.
6. Il convient de ne pas stocker plus d'images et d'informations que ce qui est strictement nécessaire.
7. L'accès aux images et aux informations stockées doit être limité.
8. Les opérateurs de vidéosurveillance doivent tenir compte de toutes les normes opérationnelles, techniques et de compétence en rapport avec un système et son objectif.
9. Des mesures de sécurité doivent être prises pour se prémunir contre l'accès et l'utilisation illicites des données.
10. Des mécanismes de vérification et d'audit doivent être mis en place pour veiller au respect des exigences juridiques et politiques et des normes.
11. Le système doit être tenu à jour.

2.3.3. Surveillance des télécommunications

Dans une perspective *mondiale*, le fait que les données de télécommunication soient stockables, accessibles et consultables n'a généralement pas permis d'aboutir à une réglementation complète régissant la divulgation et l'utilisation de ces données par les autorités de l'État, alors même que l'analyse de ces données peut s'avérer à la fois très révélatrice et particulièrement envahissante, surtout lorsque les données sont combinées et agrégées. Dans de nombreux pays, les lois et pratiques n'ont pas été réévaluées et mises à jour pour traiter des menaces et des défis liés à la surveillance des communications à l'ère du numérique. L'absence de lois réglementant la surveillance mondiale des communications et les accords de partage a donné lieu à des pratiques ad hoc qui échappent au contrôle des autorités

indépendantes. Aujourd'hui, dans de nombreux États, les données de communication peuvent être accessibles par un large éventail d'organismes publics, pour toute une série d'objectifs, souvent sans autorisation judiciaire ni contrôle indépendant. En outre, les États ont cherché à adopter des accords de surveillance censés avoir un effet extraterritorial ⁽¹⁹¹⁾.

Le rapporteur spécial des Nations Unies, *Frank La Rue*, a critiqué l'absence de réglementation ou l'insuffisance de la réglementation régissant la légitimation des techniques de surveillance intrusive sans contrôle ou examen indépendant:

«Dans la plupart des États, les normes juridiques sont inexistantes ou insuffisantes pour traiter des technologies modernes de surveillance des communications. En conséquence, les États cherchent de plus en plus à justifier l'utilisation des nouvelles technologies avec de vieux cadres juridiques, sans reconnaître que les capacités étendues dont ils disposent maintenant vont au-delà de ce que ces cadres envisageaient. Dans de nombreux pays, cela implique que des dispositions juridiques vagues et relativement larges sont invoquées pour légitimer et sanctionner l'utilisation de techniques hautement intrusives. Sans législation explicite autorisant ces technologies et techniques et définissant la portée de leur utilisation, il est impossible de prévoir, ou même de connaître, leur application. Dans le même temps, des lois sont adoptées pour élargir la portée des exceptions nationales en matière de sécurité, en légitimant les techniques de surveillance intrusive sans surveillance ou examen indépendant.» «Alors que traditionnellement la surveillance des communications devait être autorisée par le pouvoir judiciaire, cette exigence est de plus en plus affaiblie ou retirée. Dans certains pays, l'interception des communications peut être autorisée par un ministre, un de ses représentants ou un comité.»

Et d'insister sur la situation particulière des services nationaux de renseignement:

⁽¹⁹¹⁾ Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue, Organisation des Nations Unies, Assemblée générale, le 17 avril 2013 /A/HRC/ 23/40): http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

CHAPITRE II. | GOUVERNANCE — PRÉSENTATION, DÉFIS, POSSIBILITÉS

«Dans de nombreux cas, les services nationaux de renseignement bénéficient également d'exceptions générales à l'exigence d'une autorisation judiciaire. Par exemple, aux États-Unis, le Foreign Intelligence Surveillance Act permet à la NSA d'intercepter des communications sans autorisation judiciaire lorsqu'une partie de la communication est située en dehors des États-Unis et lorsqu'un participant peut raisonnablement être considéré comme membre d'une organisation terroriste désignée par l'État.» En outre, l'Allemagne, le Royaume-Uni et la Suède sont cités dans le rapport (voir ci-dessous).

Dans le contexte *européen*, la responsabilité des États membres est essentielle pour assurer la réglementation dans le domaine de la surveillance des télécommunications. Plusieurs pays européens ont pris des dispositions rendant obligatoire l'obtention d'une autorisation judiciaire spécifique et détaillée avant l'écoute électronique ou l'interception des communications électroniques ⁽¹⁹²⁾, même si les réglementations en la matière varient fortement.

Le droit allemand autorise la mise sur écoute automatisée sans mandat pour les communications intérieures et internationales par les services de renseignement de l'État pour défendre l'ordre démocratique, l'intégrité ou la sécurité de l'État. En Suède, la loi sur les renseignements relatifs aux transmissions dans des opérations de défense autorise l'Agence de renseignement suédoise à intercepter sans mandat ou ordonnance du tribunal l'ensemble du trafic téléphonique et internet à l'intérieur des frontières suédoises ⁽¹⁹³⁾. Au Royaume-Uni, le secrétaire d'État autorise l'interception des communications ⁽¹⁹⁴⁾.

La comparaison entre l'Allemagne et les États-Unis offre un exemple intéressant d'approches différentes dans ce domaine ⁽¹⁹⁵⁾. Toutes deux contiennent des règles détaillées qui régissent la surveillance des télécommunications par les services répressifs et une loi sur les «renseignements personnels» bien conçue. Toutefois, l'Allemagne a d'une certaine façon créé un cadre juridique supérieur pour la réglementation de la surveillance des télécommunications. En Allemagne, la Constitution protège le secret des télécommunications dans son article 10, qui a été interprété dans une série de décisions importantes de la Cour constitutionnelle comme protégeant non seulement le contenu des télécommunications, mais aussi les télécommunications elles-mêmes. La Constitution allemande impose donc des limites substantielles à la capacité du corps législatif à promulguer des lois qui limitent l'article 10 ou d'autres droits constitutionnels fondamentaux. Une loi est jugée nulle si elle enfreint la protection fondamentale de la confidentialité des télécommunications prévue par l'article 10, si elle viole la «dignité humaine» telle que protégée par la loi fondamentale, ou si elle ne respecte pas «l'état de droit», qui a été utilisé par la Cour constitutionnelle pour développer le «principe de proportionnalité».

Ces exemples de règlements en matière de surveillance montrent que la situation est variable. Dans de nombreux pays, les notions particulièrement vagues et imprécises de la «sécurité nationale» sont devenues une justification acceptable pour l'interception et l'accès aux communications. Il est probablement juste de dire que l'essentiel de la réglementation est dépassé, dans la mesure où cette dernière ne tient pas compte du nouveau visage de la surveillance et où la législation ne parvient pas à suivre le rythme des changements technologiques.

2.4. Domaines réglementaires spécifiques

2.4.1. Protection des données

Le concept de protection des données est bien plus récent que celui de la vie privée. Il trouve son origine dans la collecte croissante de données personnelles sur des individus par le gouvernement. L'avènement des ordinateurs, puis de l'internet, a considérablement stimulé le développement du concept de protection des données. Le concept de base qui sous-tend la

⁽¹⁹²⁾ Benjamin J. Goold, Université d'Oxford: «Editorial: Making sense of Surveillance in Europe». *European Journal of Criminology*, Vol. 6, 2009, p. 115-117.

⁽¹⁹³⁾ Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression.

⁽¹⁹⁴⁾ Voir, par exemple, le site internet du commissaire chargé de l'interception des communications, <http://www.iocco-uk.info>, et le code de pratique pour l'interception des communications publiée par le ministère des affaires intérieures en 2002: https://www.gov.uk/gouvernement/uploads/system/uploads/attachment_data/fichier/97956/interception-comms-code-pratique.pdf; ISBN 978-0-11-341281-5.

⁽¹⁹⁵⁾ Paul M. Schwartz, *German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance*, 54 *Hastings L.J.* 751 (2002), Disponible sur la page: <http://scholarship.law.berkeley.edu/facpubs/1184>

protection des données est que les individus ont le droit de contrôler la collecte et l'utilisation de données permettant de les identifier (données à caractère personnel). Comme la protection de la vie privée, celle des données est soumise à certaines limites, dont l'une des plus évidentes est l'enquête judiciaire. La protection des données peut être comparée à la protection de la vie privée pour autant que les notions fondamentales qui la sous-tendent soient assez claires et recueillent un consensus suffisamment large, quoiqu'avec certaines variations importantes.

Au niveau mondial, l'Organisation des Nations unies a défini dix principes directeurs pour la protection des données. Ils sont surtout pertinents pour la législation nationale, mais peuvent également être contraignants pour les organisations internationales, moyennant certaines adaptations. Ils s'appliquent aux fichiers informatisés détenus par des entités publiques et privées contenant des données sur les individus et peuvent être étendus pour couvrir des fichiers manuels et/ou des données sur les personnes morales. Les principes directeurs comprennent la légalité et l'équité; l'exactitude; la spécification de la finalité; l'accès de la personne concernée; la non-discrimination et la sécurité. Les principes directeurs reconnaissent que des exceptions aux cinq premiers principes peuvent s'avérer nécessaires, mais seulement pour protéger la sécurité nationale, l'ordre public, la santé et la moralité publique, ou les droits et les libertés d'autrui. Ils invitent à désigner une autorité de contrôle indépendante chargée de veiller au respect des principes, et à prévoir des systèmes de sanctions en cas de violation des règles. Ils plaident également pour l'établissement de limites sur la circulation des informations dans les pays qui n'offrent pas de garanties comparables ⁽¹⁹⁶⁾.

Bien que la Cour européenne des droits de l'homme ait traité de la question de la protection des données personnelles en tant que partie intégrante du droit à la vie privée, au niveau de l'Union, le droit à la protection des données est considéré comme un droit autonome. Les données personnelles sont protégées par la loi, même si le droit à la vie privée n'est pas en cause. L'article 8 de la charte des droits fondamentaux dispose

clairement que «toute personne a droit à la protection des données à caractère personnel la concernant». La protection des données est à la fois plus large et plus spécifique que le droit à la vie privée puisqu'il ne vise pas uniquement à concrétiser la protection de la vie privée, mais qu'il s'applique systématiquement lorsque des données à caractère personnel sont traitées.

La directive relative à la protection des données énonce les conditions dans lesquelles le traitement des données est légitime. 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. La directive relative à la protection des données ne s'applique pas «aux opérations de traitement concernant la sécurité publique, la défense, la sécurité de l'État et les activités de l'État en matière pénale». Le respect de ces règles est soumis au contrôle d'une autorité indépendante. La directive relative à la protection des données peut être complétée par des régimes spécifiques de protection des données applicables à certains secteurs particuliers.

Comme le signale *González Fuster*, la protection des données est également limitée lorsque le traitement des données concerne la sécurité nationale:

«Sans surprise, la sécurité a toujours également joué différents rôles dans la législation européenne sur la protection des données. Elle peut notamment servir à limiter son champ d'application, comme dans le projet de règlement et la directive sur la protection des données (voir l'avis du GEE n° 26): sa portée est limitée au traitement des données personnelles dans le cadre des activités couvertes par le droit de l'Union, ce qui exclut explicitement le traitement de données relatives à «la sécurité nationale.» ⁽¹⁹⁷⁾

La formulation de cette limitation a été critiquée par le contrôleur européen de la protection des données qui estime que le sens de l'expression n'est pas clair:

⁽¹⁹⁶⁾ Organisation des Nations unies, résolution de l'assemblée générale 45/95 du 14 décembre 1990, Principes directeurs pour la réglementation des fichiers personnels informatisés.

⁽¹⁹⁷⁾ Gloria Gonzalez Fuster, Security and the future of personal data protection in the European Union, Security and Human Rights, 2012, n° 4, p. 339.

CHAPITRE II. | GOUVERNANCE — PRÉSENTATION, DÉFIS, POSSIBILITÉS

«En ce qui concerne l'exception pour les «activités n'entrant pas dans le champ d'application du droit de l'Union», le CEPD souhaite formuler une observation plus générale. Si la «sécurité nationale» n'entre pas dans le champ d'application du droit de l'Union, ce que cette notion recouvre n'apparaît pas toujours très clairement, étant donné qu'elle relève de la politique nationale des États membres. Au niveau national, l'utilisation du libellé «sécurité nationale» ou «sûreté de l'État», selon les États membres, avec un champ d'application différent, peut également prêter à confusion. De toute évidence, le CEPD ne conteste pas l'exception, mais considère qu'il convient d'éviter qu'elle soit indûment utilisée pour légitimer le traitement des données à caractère personnel en dehors du champ d'application du règlement et de la directive, par exemple dans le cadre de la lutte contre le terrorisme.»⁽¹⁹⁸⁾

Le 8 avril 2014, la Cour européenne de Justice a déclaré que la directive relative à la conservation des données⁽¹⁹⁹⁾, qui oblige les fournisseurs de services internet et les opérateurs de télécommunications à conserver les données et les informations des utilisateurs européens de réseaux de communication électronique, était «invalide»⁽²⁰⁰⁾. Alors que la Cour a reconnu que la rétention des données à caractère personnel à des fins d'enquête était compatible avec la charte des droits fondamentaux, elle a constaté que les obligations énoncées dans la directive étaient disproportionnées et contraires aux articles 7, 8 et 52, paragraphe 1, de la charte. La Cour s'est notamment inquiétée du fait que la notion d'infraction grave n'était pas délimitée et que la période de rétention des données (de 6 mois à 2 ans) était trop générale et non associée à l'objectif spécifique poursuivi. La Cour a constaté que *l'ingérence vaste et particulièrement grave de cette directive dans les droits fondamentaux en cause n'est pas suffisamment encadrée afin de garantir que cette ingérence soit effectivement limitée au strict nécessaire.*

⁽¹⁹⁸⁾ Avis du contrôleur européen de la protection des données sur le paquet de réformes relatif à la protection des données, le 7 mars 2012, Bruxelles, p. 15.

⁽¹⁹⁹⁾ Directive 2006/24/CE.

⁽²⁰⁰⁾ Voir: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=900848>

«37. Force est de constater que l'ingérence que comporte la directive 2006/24 dans les droits fondamentaux consacrés aux articles 7 et 8 de la charte s'avère, ainsi que l'a également relevé M. l'avocat général notamment aux points 77 et 80 de ses conclusions, d'une vaste ampleur et qu'elle doit être considérée comme particulièrement grave. En outre, la circonstance que la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes concernées, ainsi que l'a relevé M. l'avocat général aux points 52 et 72 de ses conclusions, le sentiment que leur vie privée fait l'objet d'une surveillance constante.»

Au niveau national, il existe une grande variété de d'actes législatifs relatifs à la protection des données. Toutefois, dans les États membres de l'UE, les dispositions relatives à la protection des données forment la base juridique de cette réglementation.

2.4.2. Sûreté aérienne, contrôle des frontières, lutte contre la cybercriminalité

a) Sûreté aérienne

Il existe de nombreux règlements dans le domaine de la sûreté aérienne. Le but de ces dispositions est la sécurité, or l'expérience des contrôles de sécurité dans les aéroports montre que ce domaine devient de plus en plus complexe. Les nouveaux outils technologiques dans le domaine de la sécurité sont, dans une certaine mesure, couverts par la réglementation et/ou des résolutions, etc. Le scanner corporel est un exemple éloquent, à l'égard duquel le Parlement européen a souligné que «les personnes contrôlées doivent au préalable recevoir des informations complètes, en particulier sur le fonctionnement du scanner de sûreté, sur les conditions de protection des droits à la dignité, à la vie privée et à la protection des données et sur la liberté de refuser cette méthode d'inspection/de filtrage»⁽²⁰¹⁾. Le contrôleur européen de la protection des données, le

⁽²⁰¹⁾ Résolution du Parlement européen du 6 juillet 2011 sur la sûreté aérienne, en particulier sur les scanners de sûreté (2010/2154 (INI).

groupe de travail «Article 29»⁽²⁰²⁾ et l'Agence des droits fondamentaux de l'UE ont émis des réserves vis-à-vis de l'utilisation des scanners corporels⁽²⁰³⁾.

Moins visibles, mais non moins omniprésentes, les mesures relatives à la sûreté aérienne comprennent également la collecte et l'échange de données sur les passagers aériens, ce que l'on appelle les «dossiers passagers» (PNR pour *Passenger Name Records*). Les informations recueillies par transporteurs et stockées dans les bases de données de réservation et de contrôle des départs des compagnies aériennes sont transmises aux forces de l'ordre dans le but avoué de lutter contre la criminalité organisée et le terrorisme. L'UE a signé des accords PNR bilatéraux avec les États-Unis, le Canada et l'Australie⁽²⁰⁴⁾. Une proposition de la Commission européenne de 2011 pour un régime PNR de l'Union qui obligerait les transporteurs aériens à fournir aux pays de l'UE les données des passagers entrant ou quittant l'Union européenne a été rejetée par la commission des libertés civiles du Parlement européen en 2013 en raison des inquiétudes liées à la conformité de la proposition avec les principes de proportionnalité, de l'incidence sur la protection des données et de la possibilité de profiler les passagers⁽²⁰⁵⁾.

b) Contrôle aux frontières

Les frontières sont devenues un lieu de surveillance intensive et ont connu une prolifération de technologies de sécurité déployées. Au niveau de l'UE, le système d'information Schengen (II), la base de données Eurodac et le Système d'information sur les visas (VIS) sont de vastes

bases de données qui incluent le stockage de données biométriques visant à contrôler les flux migratoires et à identifier et trier les migrants réguliers et irréguliers, comme indiqué au chapitre 1. Le système d'information Schengen II est entré en vigueur le 9 avril 2013 pour remplacer la première génération du SIS par un instrument d'analyse plus abouti. SIS II contient des données sur les migrants en situation irrégulière, les documents de voyage falsifiés et perdus et les personnes recherchées ou disparues. Il stocke des images numériques et des données biométriques. Au moment de la publication des propositions de la Commission sur le SIS II, le CEPD s'est inquiété de savoir si une étude approfondie des principes de proportionnalité et de nécessité avait été prise en compte, constatant l'absence d'analyse d'impact sur les infractions potentielles aux droits fondamentaux⁽²⁰⁶⁾. Ces préoccupations étaient pertinentes étant donné les obstacles pratiques et juridiques rencontrés par certains ressortissants de pays tiers qui tentent d'accéder, de faire rectifier ou de supprimer leurs informations personnelles détenues sur le Système d'Information Schengen de première génération⁽²⁰⁷⁾.

Le 28 février 2013, la Commission européenne a présenté de nouvelles propositions pour un système d'entrée-sortie (SEE) et un Programme d'enregistrement des voyageurs (PEV) pour l'espace Schengen, connus sous le nom de «Paquet Frontière intelligente»⁽²⁰⁸⁾. Le système entrée-sortie propose un système de stockage centralisé des données sur l'entrée et la sortie des ressortissants de pays tiers admis pour de courts séjours dans l'espace Schengen. Il comprend le stockage de données biométriques pendant une période transitoire de trois ans après l'introduction du SEE. Le groupe de travail «Article 29» sur la protection des données s'inquiète plus particulièrement de savoir si le système d'entrée/sortie *satisfait aux*

⁽²⁰²⁾ Voir: http://ec.europa.eu/justice/data-protection/article-29/index_fr.htm

⁽²⁰³⁾ Communication de la Commission au Parlement européen et au Conseil du 15 juin 2010 relative à l'utilisation de scanners de sûreté dans les aéroports, COM(2010) 311.

⁽²⁰⁴⁾ Accord entre les États-Unis et l'Union européenne sur l'utilisation et le transfert des données PNR au département américain de la sécurité intérieure, JO L 215/5, 08.11.2012; Accord entre la Communauté européenne et le gouvernement du Canada sur le traitement d'information préalable sur les voyageurs et des données PNR, JO L 82/15, 21.03.2006; Accord entre l'Union européenne et l'Australie sur le traitement et le transfert de données PNR par les transporteurs aériens aux douanes australiennes et au Service de protection des frontières, JO L 186/4, 14.7.2012.

⁽²⁰⁵⁾ Proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, COM(2011) 32, 2.2.2011.

⁽²⁰⁶⁾ Avis du contrôleur européen de la protection des données sur la proposition de décision du Conseil sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), JO C 91/38, 19.4.2006.

⁽²⁰⁷⁾ Brouwer, E. (2008), *The Other Side of the Moon: The Schengen Information System and Human Rights — A Task for National Courts*, Document de travail du CEPS, n° 288, avril 2008. Voir également l'avis du CEPD sur le SIS II, dans lequel il cite le cas d'un avocat américain mal identifié et détenu comme terroriste parce que ses empreintes digitales correspondaient à celles trouvées sur le site des attentats de Madrid.

⁽²⁰⁸⁾ Proposition de règlement du Parlement européen et du Conseil portant création d'un système d'entrée/sortie pour l'enregistrement des entrées et sorties des ressortissants de pays tiers franchissant les frontières extérieures des États membres de l'Union européenne COM(2013) 95.

CHAPITRE II. | GOUVERNANCE — PRÉSENTATION, DÉFIS, POSSIBILITÉS

critères de nécessité et de proportionnalité indispensables pour justifier ses conséquences sur le droit à la protection des données à caractère personnel prévu à «l'article 8 de la charte des droits fondamentaux de l'Union européenne»⁽²⁰⁹⁾. De même, le CEPD a émis très clairement des inquiétudes dans un avis sur les propositions de la Commission:

Il n'y a pas d'indications claires selon lesquelles les propositions de la Commission visant à créer un système de frontières intelligentes pour les frontières extérieures de l'UE atteindront l'objectif poursuivi... L'un des objectifs annoncés dans les propositions est de remplacer le système existant, jugé «lent et non fiable», alors que les estimations de la Commission elle-même ne permettent pas d'affirmer que l'alternative sera suffisamment efficace pour justifier la dépense et les intrusions dans la vie privée⁽²¹⁰⁾.

Outre les préoccupations exprimées concernant la conformité des bases de données à l'échelle de l'UE avec les principes de nécessité et de proportionnalité, une question reste ouverte, celle de savoir si ces bases de données de l'UE — qui visent ostensiblement à contrôler les frontières — sont conformes au principe de finalité. La possibilité des services répressifs d'accéder à des données sur les demandeurs d'asile (EURODAC) et les migrants (le SIS II et potentiellement aussi le SEE) ouvre la voie à l'utilisation des bases de données à des fins qui dépassent leurs fonctions initialement prévues. Les chercheurs ont relevé que ces technologies étaient susceptibles d'embrouiller la distinction entre l'immigration, la criminalité et l'application de la loi, en attirant l'attention sur le fait que les individus enregistrés pour des raisons liées à l'immigration risquaient davantage d'être la cible de mesures de répression et de surveillance secrète. La possibilité de traiter des données en se focalisant sur un groupe spécifique d'individus pour un contrôle plus rigoureux constitue une violation des principes de non-discrimination qui a été soulignée par la Cour de Justice⁽²¹¹⁾. Ces préoccupations sont reflétées par le CEPD dans son avis sur les propositions «Frontières intelligentes»:

La tendance générale qui est de donner accès aux autorités répressives aux données d'individus qui ne sont a priori coupables d'aucun crime est dangereuse. Le CEPD recommande fermement que la valeur ajoutée précise d'un tel accès, comparé à l'accès aux bases de données biométriques existantes, soit identifiée⁽²¹²⁾.

Enfin, le système européen de surveillance des frontières (EUROSUR) est devenu opérationnel en décembre 2013⁽²¹³⁾. EUROSUR vise à interconnecter les systèmes de surveillance maritime des États membres de l'UE dans le cadre d'une architecture commune de partage et d'analyse d'informations. Le système s'appuie sur l'utilisation de technologies de surveillance (notamment des images satellites et des capteurs) pour suivre l'activité des ports, des navires et des zones maritimes, afin de dresser un «tableau commun du renseignement en amont des frontières»⁽²¹⁴⁾. Les objectifs officiels d'EUROSUR sont à la fois sécuritaires (lutter contre la criminalité transfrontalière, contrôler la mobilité non désirée) et humanitaires (améliorer le sauvetage en mer et empêcher les tragédies causées par le naufrage d'embarcations transportant des migrants sur la Méditerranée). Le Comité Meijers, le Comité permanent des experts de l'immigration internationale, des réfugiés et du droit pénal, note ce qui suit:

Lors de son évaluation de la teneur de l'actuelle proposition de règlement portant création du système européen de surveillance des frontières, le Comité Meijers a émis des doutes quant à la nécessité et l'efficacité des mesures proposées (compte tenu notamment des coûts permanents que cela implique) et s'inquiète des effets que pourrait avoir EUROSUR sur les droits fondamentaux des demandeurs d'asile et des réfugiés, entre autres le droit à la vie privée et la protection des données. Le Comité Meijers met notamment en garde contre les risques d'une intensification de la surveillance, qui pourrait aussi augmenter le coût humain des migrations clandestines.

⁽²⁰⁹⁾ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp206_fr.pdf

⁽²¹⁰⁾ CEPD (2013) «Frontières intelligentes»: la proposition clé est coûteuse, insuffisamment justifiée et intrusive, 19 juillet 2013, communiqué de presse 2013/08.

⁽²¹¹⁾ Affaire C-524/06 Huber c. Allemagne [2008] Rec. p. I-9705.

⁽²¹²⁾ CEPD (2013) «Frontières intelligentes»: la proposition clé est coûteuse, insuffisamment justifiée et intrusive, 19 juillet 2013, communiqué de presse 2013/08.

⁽²¹³⁾ Règlement (UE) n° 1052/2013 du 22 octobre 2013 portant création du système européen de surveillance des frontières (EUROSUR), JO L 295/11, 11.6.2013.

⁽²¹⁴⁾ Ibidem.

La surveillance des frontières aura en effet une incidence sur les routes migratoires, mais pas sur les causes profondes de la migration ⁽²¹⁵⁾.

Le Comité a souligné que l'objectif de la proposition EUROSUR d'accroître la connaissance de la situation impliquait également une augmentation de la responsabilité en vertu du droit international des réfugiés et du régime de recherche et de sauvetage fondé sur la Convention internationale sur la recherche et le sauvetage maritimes. Dans le même ordre d'idées, le Rapporteur spécial des Nations unies sur les droits de l'homme des migrants, François Crépeau, a soulevé un certain nombre de questions et de préoccupations en ce qui concerne le nouveau système:

Pourtant, le Rapporteur spécial regrette que le projet ne prévoie aucune procédure, ligne directrice ni système visant à garantir que le sauvetage en mer soit mis en œuvre efficacement comme un objectif primordial. En outre, le projet de règlement ne définit pas exactement comment les choses seront organisées, et aucune procédure ne décrit la marche à suivre avec les personnes «sauvées». Dans ce contexte, le Rapporteur spécial craint qu'EUROSUR ne soit voué à devenir juste un outil supplémentaire à la disposition des États membres pour sécuriser les frontières et empêcher les arrivées, plutôt qu'un véritable outil de sauvetage ⁽²¹⁶⁾.

c) Cybercriminalité

En ce qui concerne le règlement de la cybercriminalité, la Convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001 et le Protocole additionnel à la Convention sur la cybercriminalité du 28 janvier 2003 ⁽²¹⁷⁾ constituent une base solide. La Convention

est le premier traité international définissant les infractions pénales commises via internet et d'autres réseaux informatiques, en particulier les infractions portant atteinte aux droits d'auteurs, la fraude liée à l'informatique, la pornographie enfantine ainsi que les infractions liées à la sécurité des réseaux. Son principal objectif est de poursuivre une politique pénale commune destinée à protéger la société contre la cybercriminalité, notamment par l'adoption d'une législation appropriée, et d'encourager la coopération internationale. Elle prévoit aussi une série de pouvoirs et de procédures comme la recherche de réseaux informatiques et l'interception.

L'exposé des motifs de la Convention ⁽²¹⁸⁾ note que

«La révolution des technologies de l'information a radicalement changé la société et continuera vraisemblablement de le faire dans un avenir prévisible. Cette révolution a simplifié bien des tâches. Alors qu'initialement, seuls certains secteurs de la société avaient rationalisé leurs méthodes de travail en s'appuyant sur les technologies de l'information, il ne reste pour ainsi dire plus aucun secteur qu'elles n'aient marqué de leur empreinte. Les technologies de l'information se sont insinuées, d'une manière ou d'une autre, dans tous les aspects des activités humaines.

La Convention sert de lignes directrices pour tout pays élaborant une législation exhaustive en matière de cybercriminalité, mais aussi de cadre pour la coopération internationale contre la cybercriminalité parmi les États Parties. Elle sert également de point de référence juridique pour l'Union européenne, qui est en train d'élaborer un ensemble de politiques visant à accroître la cybersécurité.

Les derniers développements de l'UE sont la communication de la Commission sur la stratégie en matière de cybersécurité de février 2013 ⁽²¹⁹⁾, qui expose la vision de l'UE sur la façon de renforcer la sécurité dans le cyberspace et énonce les actions dans ce domaine, et la nouvelle directive de l'Union européenne 2013/40/UE relative aux attaques contre les systèmes d'information

⁽²¹⁵⁾ Note du Comité Meijers sur la proposition de règlement portant création du système européen de surveillance des frontières, 9.12.2012.

⁽²¹⁶⁾ Rapport du Rapporteur spécial des Nations unies sur les droits de l'homme des migrants, François Crépeau — Étude régionale: la gestion des frontières extérieures de l'Union européenne et ses incidences sur les droits de l'homme des migrants, 24 avril 2013, A/HRC/23/46.

⁽²¹⁷⁾ <http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm> et <http://conventions.coe.int/Treaty/fr/Treaties/Html/189.htm>

⁽²¹⁸⁾ <http://conventions.coe.int/Treaty/fr/Reports/Html/185.htm>

⁽²¹⁹⁾ <http://ec.europa.eu/dgs/connect/en/content/cybersecurity-strategy-european-union>

CHAPITRE II. | GOUVERNANCE — PRÉSENTATION, DÉFIS, POSSIBILITÉS

entrée en vigueur le 3 septembre 2013 ⁽²²⁰⁾. La directive a pour objet les cyberattaques de grande envergure et vise à obliger les États membres à renforcer leur législation en matière de cybercriminalité et à introduire des sanctions pénales plus sévères.

2.4.3. Lancement d'alerte

Les lancements d'alerte ne se limitent pas à des questions de sécurité et de surveillance, mais les actions d'Edward Snowden ont servi à mettre en évidence des lacunes dans les systèmes censés veiller à ce que les actions entreprises par les États au nom de la sécurité nationale respectent les exigences juridiques, et le fait que, lorsqu'il y a des raisons de croire que des restrictions juridiques ont été ignorées, des mécanismes permettent de recourir à des systèmes appropriés pour répondre aux préoccupations.

Un récent rapport de Transparency International ⁽²²¹⁾ présente une évaluation globale de l'adéquation des législations de protection des lanceurs d'alertes des 27 pays membres de l'UE. Seuls quatre pays de l'Union européenne (UE) disposent de cadres juridiques pour la protection des lanceurs d'alertes qui peuvent être considérés comme avancés: le Luxembourg, la Roumanie, la Slovénie et le Royaume-Uni. Parmi les 23 autres pays de l'UE, 16 offrent une protection juridique partielle aux employés qui dénoncent des actes fautifs. Les sept pays restants n'ont aucun cadre juridique ou alors un très limité. En outre, plusieurs dispositions de protection des lanceurs d'alertes actuellement en place comportent des failles et des exceptions, si bien que les employés qui se croient protégés contre les représailles pourraient découvrir, après avoir dénoncé des méfaits sur la place publique, qu'ils n'ont, en réalité, aucun recours juridique. Il est encourageant de constater que plusieurs pays de l'UE ont pris, au cours des dernières années, des mesures visant à renforcer les droits des lanceurs d'alertes, y compris l'Autriche, la Belgique, le Danemark, la France, la Hongrie, l'Italie, le Luxembourg, Malte, la Roumanie et la Slovénie. La Finlande, la Grèce, l'Irlande, les Pays-Bas et la Slovaquie ont émis

des propositions ou annoncé des projets de loi. Mais de nombreux pays manquent de volonté politique.

Transparency International demande instamment à tous les pays de l'UE de consacrer les droits des lanceurs d'alertes dans leurs lois et d'ouvrir un dialogue public sur cette question. Bien que ce rapport se concentre sur la lutte contre la corruption, nombre de ces principes restent très pertinents dans le contexte de la sécurité et de la surveillance et devraient être dûment examinés dans ce cadre.

La Commission européenne et les États membres devraient veiller à ce qu'un mécanisme efficace et global de protection des lanceurs d'alertes soit mis en place dans les secteurs public et privé, comme l'a également rappelé le Parlement européen en octobre 2013.

Transparency International fournit également un ensemble de principes comme «les meilleures pratiques législatives pour protéger les lanceurs d'alertes et soutenir la dénonciation dans l'intérêt public». Le principe 19 prévoit le lancement d'alertes dans le domaine de la sécurité nationale ou du secret d'État.

19. La sécurité nationale/le secret d'État — lorsque la dénonciation porte sur des questions de sécurité nationale, officielle, des secrets militaires ou des renseignements classifiés, des procédures et des garanties spéciales qui tiennent compte du caractère sensible du sujet peuvent être adoptées pour favoriser un suivi et résolution satisfaisante en interne et éviter toute exposition extérieure. Ces procédures devraient permettre les divulgations internes, la divulgation à un organisme de surveillance autonome qui soit indépendant sur le plan institutionnel et opérationnel du secteur de la sécurité, ou la divulgation à des autorités ayant une habilitation de sécurité du niveau approprié. La divulgation externe (c'est-à-dire aux médias ou à des organisations de la société civile) pourrait s'avérer justifiée dans des cas de menace grave et avérée pour la santé publique, la sécurité ou l'environnement, si une divulgation interne peut occasionner un préjudice personnel ou entraîner la destruction d'éléments de preuve, et si la divulgation n'a pas pour objet ou ne risque pas de nuire de manière significative à la sécurité nationale ou à des particuliers.

⁽²²⁰⁾ Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil, Journal officiel L 218/8 14/8/2013: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:FR:PDF>

⁽²²¹⁾ Transparency International, Whistleblowing in Europe, Legal Protection for whistle-blowers in the EU, 2013.

2.4.4. Drones

Comme la technologie des drones est encore relativement nouvelle, il n'est pas surprenant que le cadre réglementaire régissant leur utilisation soit très limité. Néanmoins, elle pose un important défi pour les régulateurs.

La Commission européenne a adopté la communication intitulée «Une nouvelle ère de l'aviation — Ouvrir le marché de l'aviation à l'utilisation civile de systèmes d'aéronefs télépilotés, d'une manière sûre et durable» le 8 avril 2014. La présente communication décrit comment la Commission envisage d'inscrire l'exploitation des systèmes d'aéronefs télépilotés (RPAS, «Remotely Piloted Aircraft Systems») dans un cadre d'action au niveau européen qui permettra le développement progressif du marché commercial des RPAS tout en assurant la protection de l'intérêt public.

Elle s'appuie sur des études et des travaux préparatoires qui examinent la situation législative à l'égard de drones dans les États membres de l'UE, en mettant l'accent sur les utilisations civiles ⁽²²²⁾.

Une perspective plus large, englobant également d'autres utilisations de ces technologies, est fournie ci-dessous dans l'encadré sur les drones.

⁽²²²⁾ Ces documents sont disponibles à l'adresse suivante: <http://ec.europa.eu/enterprise/sectors/aerospace/uas/>

CHAPITRE II. | GOUVERNANCE — PRÉSENTATION, DÉFIS, POSSIBILITÉS

Drones

Les aéronefs télépilotés, ou systèmes aéronefs télépilotés, également connus sous le nom de drones, peuvent être aussi grands qu'un Boeing 737 ou aussi petits qu'un insecte. Les progrès accomplis dans les technologies du vol et de la radio dans les années 1970 ont permis le développement de drones, notamment par l'armée de l'air israélienne. Ces premiers drones ont été utilisés pour des missions de reconnaissance en 1991, durant les guerres d'Iraq, et les modèles suivants, notamment le «Predator», ont régulièrement survolé les Balkans en appui des opérations de l'OTAN dans la région ⁽²²³⁾. Le premier drone armé, le Predator MQ-1B, a mené sa première attaque en lançant des missiles Hellfire au Yémen en novembre 2002 ⁽²²⁴⁾. Après les attaques terroristes de 2001 aux États-Unis, les drones utilisés jusque-là à des fins de surveillance uniquement ont commencé à être utilisés pour effectuer des frappes ciblées dans les régions les plus reculées d'Afghanistan et du Pakistan. En 2007, le Reaper MQ-9 a été lancé. Ce drone présente une autonomie neuf fois supérieure et peut atteindre des altitudes deux fois plus élevées que le Predator. Il utilise un certain nombre de capteurs (y compris infrarouge) pour viser sa cible et est équipé d'une caméra couleur et d'une caméra de vision nocturne qui émettent en flux en direct ⁽²²⁵⁾. Il est spécialement conçu pour servir de «système d'arme de chasse», plutôt que comme engin de surveillance.

Traditionnellement, les drones sont considérés comme parfaitement adaptés aux tâches dites «désagréables, dégoûtantes et dangereuses», appelées les 3D ⁽²²⁶⁾. Les techniques de télécommunication de pointe permettent aux drones d'opérer à haute altitude, pendant de longues périodes, sur des distances considérables. Ainsi, les missions de surveillance, considérées comme désagréables ou dangereuses, profitent de la capacité des drones à survoler des zones pendant de longues périodes (entre 18 et 82 heures) sans mettre le personnel en danger. Compte tenu de la nature des drones, ils peuvent également être utiles pour des tâches dites «dégoûtantes», comme le survol de zones touchées par un produit chimique, une attaque biologique ou par une catastrophe naturelle.

Les drones sont maintenant devenus une arme de choix dans la lutte contre le terrorisme et sont censés remplacer les aéronefs pilotés dans les 40 prochaines années. En 2002, le ministère américain de la défense avait 167 drones en fonctionnement. En 2010, on en comptait 7 000 en fonctionnement dans le monde. Depuis 2009, l'armée américaine a formé plus de pilotes d'aéronefs télépilotés que de pilotes de chasse ⁽²²⁷⁾. Des frappes de drones ont été lancées en Afghanistan, au Pakistan, au Yémen, en Somalie, en Libye, à Gaza et en Iraq. Les estimations du nombre de civils tués par les frappes de drone varient considérablement, dans la mesure où les données sont compilées dans des bulletins d'information dont la crédibilité peut varier. Selon le Bureau of Investigative Journalism, entre 416 et 951 civils ont été tués par des frappes de drones de la CIA au Pakistan depuis 2004, dont 168 à 200 enfants ⁽²²⁸⁾.

La prochaine génération de drones sera non seulement sans pilotes, mais elle sera programmée pour prendre des décisions cruciales de façon autonome. Des drones ont été développés pour pouvoir décoller et atterrir automatiquement, sans intervention du contrôleur sur le terrain. Le X-47B a été commandé par l'US Navy et, en mai 2013, sa capacité de décoller et d'atterrir sur le pont d'un porte-avions a été testée. Le groupe britannique BAE Systems est en train de développer le drone de combat télépilote semi-autonome Taranis destiné à attaquer des cibles aériennes et au sol. Le ministère britannique de la défense a confirmé que les premiers essais en vol avaient déjà eu lieu dans le sud de l'Australie ⁽²²⁹⁾. L'avènement d'une technologie autonome couplée à l'usage offensif des Predators et des Reapers a agité le spectre de la «robotique létale autonome», des systèmes d'armement qui, une fois engagés, pourraient sélectionner et attaquer des cibles sans aucune intervention humaine. Le Georgia Institute of Technology's School of Computer Science a entrepris des recherches pour développer une architecture éthique pour les drones autonomes. En apprenant aux drones à utiliser des informations issues d'engagements

⁽²²³⁾ Deri, AR. *Intersect* 2012;5: p. 1-16.

⁽²²⁴⁾ <http://news.sky.com/story/139261/cia-acted-alone-in-yemen-strike> consulté le 14 novembre 2013.

⁽²²⁵⁾ <http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104470/mq-9-reaper.aspx> consulté le 14 novembre 2013.

⁽²²⁶⁾ Attribué à Peter Singer, directeur du Centre for 21st Century Security and Intelligence.

⁽²²⁷⁾ Committee on Oversight and Government Reform 2010.

⁽²²⁸⁾ <http://www.thebureauinvestigates.com/category/projects/drones/monthly-updates/> consulté le 8 janvier 2014.

⁽²²⁹⁾ <http://www.janes.com/article/28899/taranis-makes-maiden-flight> consulté le 14 novembre 2013.

précédents, par exemple relatives à une zone de destruction, ceux-ci pourraient régler leur «comportement», notamment le choix des armes à utiliser lors de futures missions.

L'utilisation au combat des aéronefs télépilotes et la perspective de l'avènement des drones autonomes ont soulevé un certain nombre de questions quant à la légalité des attaques de drones, la nature changeante de la guerre et la responsabilité. Christof Heyns, le rapporteur spécial des Nations unies sur les exécutions extrajudiciaires décrit les attaques de drones comme une forme de force de police mondiale qui pourrait saper plutôt que de renforcer la sécurité internationale ⁽²³⁰⁾. Heyns a également plaidé pour un moratoire mondial sur «l'essai, la production, l'assemblage, le transfert, l'acquisition, le déploiement et l'emploi» de robots létaux autonomes jusqu'à ce que de nouveaux règlements sont mis en place pour régir leur utilisation ⁽²³¹⁾. Ben Emmerson, rapporteur spécial des Nations unies sur les droits de l'homme et la lutte contre le terrorisme, met en doute dans un rapport intérimaire la légalité des attaques de drones et invite les États à respecter l'ensemble du droit international applicable, à se montrer transparents dans leur utilisation des drones et à enquêter sur les allégations d'exécutions illégales ⁽²³²⁾. Certains craignent que l'avènement des drones ne modifie le coût perçu de la guerre. Le détachement facilité par les attaques de drones peut réduire la menace d'une guerre à la fois pour le système politique et le public en général et la modération essentielle due au coût élevé de la guerre tant sur le plan économique qu'humain risque d'être sapée. Le développement des drones autonomes constitue un problème éthique d'autant plus grand que ces engins devront en principe décider ou non de tuer des êtres humains. Krishnan explique que cela élève les drones «sur le plan ontologique et peut-être même sur le plan moral du statut de simple objet à celui d'objet capable d'actions moralement significatives» ⁽²³³⁾.

Les drones peuvent être déployés dans toute une série de contextes et à des fins très diverses. Le nombre de pays disposant de systèmes d'aéronefs télépilotes à usage militaire, commercial ou civil est passé de 41 en 2005 à 76 en 2011 ⁽²³⁴⁾. Une étude de marché réalisée en 2012 par Teal Group estime que dans le monde les dépenses consacrées aux drones, dans tous les secteurs, vont dépasser les 89 milliards de dollars dans les dix prochaines années ⁽²³⁵⁾.

Les drones sont généralement considérés comme des armes de guerre, mais récemment des applications civiles sont apparues. Des aéronefs télépilotes ont été déployés dans des opérations de recherche et de sauvetage, pour surveiller les foules lors de manifestations sportives, pour surveiller la circulation, pour détecter des menaces sur de grandes infrastructures et pour suivre les populations d'espèces sauvages. Les utilisations civiles potentielles de drones au sein de l'Union européenne ont été largement débattues. Le document de travail de la Commission sur une stratégie européenne pour le développement des applications civiles des drones affirme qu'il existe plus de 400 applications en développement au sein de l'UE ⁽²³⁶⁾.

En matière d'environnement et d'écosystème, l'utilisation de drones peut concerner l'agriculture de précision, la cartographie de l'érosion du littoral, ou encore la surveillance des espèces et des habitats. Les drones équipés de

⁽²³⁰⁾ http://justsecurity.org/wp-content/uploads/2013/10/UN-Special-Rapporteur-Extrajudicial-Christof-Heyns-Report-Drones.pdf?utm_source=Press+mailing+list&utm_campaign=6de0426c90-2013_10_17_Heyns_drones_report_UN&utm_medium=email&utm_term=0_022da08134-6de0426c90-286021377 consulté le 9 janvier 2014.

⁽²³¹⁾ http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A-HRC-23-47_fr.pdf consulté le 9 janvier 2014.

⁽²³²⁾ <http://www.lawfareblog.com/wp-content/uploads/2013/10/Emmerson-Report.pdf> consulté le 9 janvier 2014

⁽²³³⁾ Armin Krishnan, *Killer Robots: Legality and Ethicality of Autonomous Weapons*. Burlington: Ashgate Publishing Company, 2009) p. 33.

⁽²³⁴⁾ United States Government Accountability Office 2012. <http://dronewarsuk.files.wordpress.com/2012/09/us-gao--noprolieration-of-uavs.pdf> consulté le 8 janvier 2014.

⁽²³⁵⁾ Teal Group 2013 Market Profile and Forecast World Unmanned Ariel Vehicle Systems <http://tealgroup.com/index.php/aboutVteal/tealVgroupVinVtheVmedia/3/66VtealV> <http://tealgroup.com/index.php/aboutVteal/tealVgroupVinVtheVmedia/3/66VtealV> consulté le 8 janvier 2014.

⁽²³⁶⁾ Document de travail des services de la Commission: Vers une stratégie européenne pour le développement d'applications civiles des systèmes d'aéronefs télépilotes (RPAS) Septembre 2012. <http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13438.en12.pdf> consulté le 10 janvier 2014.

CHAPITRE II. | GOUVERNANCE — PRÉSENTATION, DÉFIS, POSSIBILITÉS

caméras, de systèmes de communication et de détecteurs peuvent non seulement capter des images, mais également fournir des informations en temps réel sur les catastrophes naturelles et collecter et transmettre des données météorologiques. Les drones peuvent survoler des zones à risque, contaminées et non accessibles à l'homme ou à des aéronefs habités. Des drones ont été utilisés pour collecter des données relatives à la vitesse du vent dans l'œil des ouragans et la National Aeronautical and Space Administration (NASA) a déployé des drones dans les panaches de dioxyde de soufre émanant du cratère du volcan Turriabla au Costa Rica, pour recueillir des données sur la température, la hauteur de cendres et les concentrations de gaz qui leur ont permis de prédire le sens du panache volcanique ⁽²³⁷⁾. Des drones ont également été utilisés pour mesurer les niveaux de radiation et évaluer les dégâts subis par les réacteurs nucléaires de la centrale de Fukushima, au Japon. Des drones sont spécifiquement conçus par le Japon en coopération avec l'Agence internationale de l'énergie atomique (AIEA) pour surveiller le niveau des radiations autour de la centrale nucléaire de Fukushima touchée par le tsunami. Ils devraient être opérationnels d'ici 2015 ⁽²³⁸⁾.

Des «écodrones» ont été utilisés pour la surveillance de la déforestation et du braconnage en Afrique, en Asie et en Amérique du Sud. Le gouvernement brésilien a investi 350 millions de dollars pour acheter 14 drones permettant à la police de l'environnement de São Paulo de surveiller la déforestation en Amazonie, la pêche illégale et les opérations minières ⁽²³⁹⁾. En 2012, Google a versé au Fonds mondial pour la nature (WWF) 5 millions de dollars pour l'utilisation de drones, et d'autres technologies, dans les activités de surveillance des mouvements de la faune et de pistage des braconniers. Les relevés aériens à distance et les logiciels d'analyse permettront aux patrouilles de Rangers d'être mieux informées et donc de mieux protéger les espèces menacées d'extinction. Il est à espérer que l'utilisation de technologies innovantes, telles que les drones, permettra d'enrayer le commerce illicite de la faune et de la flore qui, selon le WWF, atteint 7 à 10 milliards de dollars par an ⁽²⁴⁰⁾.

Les progrès rapides dans les technologies de drones ont également suscité l'intérêt des forces de l'ordre, dans la mesure où ces technologies leur permettraient de renforcer leur capacité de surveillance. Des drones pourraient être déployés pour une fraction du coût des véhicules habités et d'hélicoptères qui sont en outre limités à des zones auxquelles ils peuvent accéder. Les drones équipés de caméras, de dispositifs d'écoute et d'interception de communication et capables d'associer les images captées à des logiciels de reconnaissance faciale pourraient suivre en permanence des individus dans un espace public. Aux États-Unis, l'Office of Justice Programs (OJP) et l'Office of Community Orientated Policing Services (COPS) ont accordé 1,2 million de dollars à sept organismes locaux chargés de l'application de la loi pour tester ou utiliser des drones ⁽²⁴¹⁾. Les drones ont été jugés particulièrement adaptés à l'application de la loi, car ce type d'avion a la capacité de «manœuvrer discrètement dans les zones où le respect de la vie privée n'est pas bien défini, comme dans le voisinage immédiat de résidences». L'American Civil Liberties Union (ACLU) craint que la multiplication des déploiements de drones finisse par mettre en place une surveillance aérienne de routine qui modifiera profondément la nature de la vie publique. L'ACLU a demandé de fixer des limites et de mettre en place des règlements pour l'utilisation de drones par les forces de l'ordre, afin d'éviter de créer une «société de la surveillance dans laquelle tous nos gestes sont surveillés, suivis, enregistrés et contrôlés par les autorités» ⁽²⁴²⁾.

Les préoccupations concernant la protection de la vie privée sont aggravées par les progrès accomplis dans la miniaturisation des drones. Les chercheurs se sont inspirés des oiseaux et des insectes comme modèles et ont imité leurs techniques de navigation complexes et aérodynamiques pour produire des microdrones. Leur petite taille leur permet d'accéder à des espaces confinés et de naviguer en intérieur plus efficacement que les robots terrestres, et ce sans que les personnes observées ne se rendent compte de leur présence. La Defense Advanced Research Projects Agency (DARPA) des États-Unis a financé le développement d'un minuscule drone appelé «nano hummingbird»,

⁽²³⁷⁾ http://www.nasa.gov/topics/earth/earthmonth/volcanic-plume-uavs.html#_UtaAaSvs7RM0 consulté le 10 janvier 2014.

⁽²³⁸⁾ <http://www.iaea.org/newscenter/focus/fukushima/japan-report2/japanreport120911.pdf> consulté le 10 janvier 2014.

⁽²³⁹⁾ Brazilian Eyes In The Sky Focus On The Disappearing Rainforest. Scientific American 26 octobre 2011.

⁽²⁴⁰⁾ <http://worldwildlife.org/stories/google-helps-wwf-stop-wildlife-crime> consulté le 12 janvier 2014.

⁽²⁴¹⁾ <http://www.justice.gov/oig/reports/2013/a1337.pdf> consulté le 10 janvier 2014.

⁽²⁴²⁾ <https://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf> consulté le 12 janvier 2014.

dont le but est la surveillance invisible. Il se faufile par les fenêtres et les portes. Il peut voler jusqu'à 11 kilomètres par heure et voler pendant huit minutes. Avec une envergure de seulement six pouces et demi et un poids de 19 g (moins qu'une seule pile AA), le hummingbird est doté d'une caméra vidéo et d'un système de communication ⁽²⁴³⁾.

La capacité de surveillance omniprésente qu'offrent les drones ne sera à l'avenir pas réservée aux gouvernements ou aux organisations. La révolution des drones personnels profite de la popularité de la technologie dont peuvent disposer les consommateurs, notamment des téléphones intelligents. Les batteries petites, mais efficaces, les récepteurs GPS et les puces mémoires bon marché sont autant de composants des microdrones. Produite en masse, l'électronique miniature a rendu les drones suffisamment petits et bon marché pour être accessibles aux particuliers. La société française Parrot a vendu à plus d'un demi-million de l'AR-drone 2.0 depuis son lancement en 2010. Il peut être exploité par un téléphone intelligent ou une tablette et peut être acheté sur Amazon pour environ 250 dollars.

Des communautés en ligne d'amateurs de drones fabriqués maison ont vu le jour sur l'internet, ce qui agite le spectre d'un ciel saturé de drones utilisés pour des applications personnelles allant de la photographie aérienne à l'espionnage des voisins.

Aux États-Unis, il est illégal de faire fonctionner un drone à plus de 120 mètres d'altitude et au-delà de la ligne de vue pour tout objectif non militaire, sans autorisation de l'autorité fédérale de l'aviation (Federal Aviation authority FAA). Entre 2007 et février 2013, la FAA a délivré 1 428 permis à des agences fédérales et des organismes chargés de l'application de la loi, ainsi qu'à des universités engagées dans des projets de recherche ⁽²⁴⁴⁾. En prévision de l'expansion de l'utilisation des drones, Barack Obama a signé la loi sur la modernisation de la FAA en février 2012, qui charge la FAA d'ouvrir l'espace aérien américain aux drones désarmés à l'horizon 2015. En novembre 2013, la FAA a publié une feuille de route pour l'intégration de systèmes aériens civils sans pilote dans l'espace aérien national ⁽²⁴⁵⁾.

Comme aux États-Unis, les drones survolant l'espace aérien européen sont limités à une altitude de 120 mètres, à l'écart des bâtiments et des personnes, et à la ligne de vue de l'opérateur. L'utilisation systématique des drones à des fins civiles au sein de l'UE est actuellement entravée par l'absence de cadre réglementaire clair, intégrant des règles pour la certification et le contrôle opérationnel et pour la collecte et le transfert de données. Les permis de vol pour les drones sont délivrés au cas par cas et se limitent à des espaces aériens réservés. Dans les États membres, un certain nombre d'autorités de l'aviation civile ont émis des règlements qui ne sont pas nécessairement alignés, contribuant ainsi davantage à la fragmentation d'une approche réglementaire de l'Union. La Commission européenne a entrepris une consultation sur l'avenir des systèmes d'aéronefs télépilotes entre 2009 et 2012. L'un des résultats de cette consultation a été la création d'un groupe directeur européen sur les systèmes d'aéronefs télépilotes chargé de concevoir une feuille de route pour l'intégration en toute sécurité des systèmes d'aéronefs télépilotes à usage civil dans l'espace aérien européen d'ici 2016. Le groupe directeur a publié son rapport final en juin 2013. Il recense des améliorations au cadre réglementaire existant et présente un plan stratégique de recherche et développement, en mettant en avant les activités de recherche et les technologies nécessaires à l'intégration en toute sécurité des systèmes d'aéronefs télépilotes dans l'espace aérien européen. La feuille de route aborde également l'incidence sociétale des drones et reconnaît que l'acceptation de cette technologie dépend de l'établissement d'un niveau adéquat de responsabilité et d'obligation de rendre compte.

Le 19 novembre 2013, les ministres de la défense des sept États membres de l'UE (la France, l'Allemagne, la Grèce, l'Italie, les Pays-Bas, la Pologne et l'Espagne) ont signé une lettre d'intention demandant à l'Agence européenne de défense (AED) d'étudier les exigences et les coûts d'un futur drone de surveillance de l'Union européenne qui pourrait être produit après 2020. La réunion du Conseil européen de décembre 2013 «a accueilli favorablement les projets de coopération soutenus par l'Agence européenne de défense dans les domaines des systèmes d'aéronefs télépilotes» ⁽²⁴⁶⁾.

⁽²⁴³⁾ <http://www.avinc.com/nano> consulté le 12 janvier 2014.

⁽²⁴⁴⁾ United States Government Accountability Office — février 2013 <http://www.gao.gov/assets/660/652223.pdf> consulté le 12 janvier 2014.

⁽²⁴⁵⁾ http://www.faa.gov/about/initiatives/uas/media/UAS_Roadmap_2013.pdf consulté le 12 janvier 2014.

⁽²⁴⁶⁾ <http://european-council.europa.eu/home-page/highlights/security-and-defence-policy-high-on-the-agenda-at-the-european-council?lang=fr> consulté le 12 janvier 2014.

CHAPITRE II. | GOUVERNANCE — PRÉSENTATION, DÉFIS, POSSIBILITÉS

2.4.5. Recherche

Un nombre sans cesse croissant de personnes a aujourd'hui accès à des documents de recherche, des technologies ou des connaissances permettant des abus. De plus, la science progresse aujourd'hui dans des domaines (par ex. dans la recherche de la sécurité proprement dite, mais également dans la biologie synthétique, la nanotechnologie, etc.) où les abus pourraient avoir des répercussions d'envergure pour les hommes, les animaux, les plantes, les économies et les sociétés. L'action des autorités publiques, avec toute l'attention nécessaire accordée à «qui garde les gardiens», revêt une importance primordiale.

La recherche est traditionnellement plus ou moins réglementée, mais certaines restrictions sont en place. La recherche financée par l'UE est soumise à une évaluation éthique, dans laquelle l'éthique de la recherche est prise en considération. Dans *«Une stratégie globale sur la façon de réduire les abus dans la recherche et les risques d'utilisation abusive des recherches dans les recherches financées par l'UE»* deux des principaux domaines de préoccupation concernant l'utilisation frauduleuse sont *«l'application et le développement des technologies de surveillance»* et *«les technologies d'exploration des données et de profilage.»* Il faudrait notamment garantir que les normes européennes relatives à la protection des données sont respectées par les pays non-candidats à l'adhésion et veiller à ce que des garanties techniques et/ou organisationnelles soient introduites afin que les résultats ne puissent être employés que de façon conforme à l'éthique de l'UE.

La question de la recherche de la sécurité et de la possibilité d'abuser de la recherche a bénéficié d'une attention renouvelée ces dernières années, notamment vu l'effet que de tels abus ont eu sur le public en général et la prise de conscience croissante de son incidence potentielle.

L'affaire Amerithrax aux États-Unis en 2001 ⁽²⁴⁷⁾ a non seulement coûté la vie à cinq personnes, mais a également généré des dommages économiques estimés à 1 milliard de dollars (cf. Rapport 2010 sur les fautes et les abus éventuels de la recherche). La nécessité de se protéger contre de tels abus a donné lieu à de nombreuses initiatives législatives dans divers pays.

Elle a également stimulé le débat entre les scientifiques, les institutions scientifiques et les éditeurs pour établir et mettre en œuvre des codes de conduite visant à réduire les risques d'utilisation abusive de la recherche. Plusieurs institutions de financement ont développé et mis en place de tels mécanismes de contrôle pour s'assurer que les risques de tels abus soient réduits au minimum.

Outre le contexte d'utilisations terroristes et militaires contraires à l'éthique de la recherche, d'autres domaines d'utilisation abusive potentielle ont suscité des interrogations ces derniers temps. La stigmatisation et la discrimination à l'égard de certains individus ou groupes d'individus en est un exemple. Ainsi, dans plusieurs pays, les législateurs nationaux ont introduit une nouvelle disposition visant à se prémunir contre ce type d'abus dans le contexte des données génétiques.

Les récentes expériences menées en Europe sur le gain de fonction ont également jeté un nouvel éclairage sur le fait qu'il importe de repenser et de mettre en place des mécanismes de surveillance pour les activités de recherche susceptibles d'être à double usage (Dual Use Research of Concern, DURC), autrement dit des recherches destinées à générer des bénéfices, mais qui pourraient facilement être détournées aux fins de nuire.

Un autre exemple est la possibilité de mauvaise utilisation des technologies modernes de l'information et de la communication à des fins contraires à l'éthique. C'est ce qui a motivé les législateurs à élaborer et constamment mettre à jour une nouvelle législation, principalement dans le contexte de la protection des données personnelles, pour protéger les individus contre de tels abus. Toutefois, à mesure que la recherche progresse, de nouveaux outils sophistiqués permettant la personnalisation de données anciennement anonymes (comme les technologies d'extraction de données enfouies ou de reconstruction d'images) sont développés. Équilibrer les besoins de sécurité et les risques que représentent ces technologies pour la vie privée restera un défi permanent pour les spécialistes de l'éthique et les législateurs.

2.5. Préoccupations, défis et possibilités réglementaires?

D'un point de vue éthique, les principales préoccupations d'ordre réglementaire sont:

⁽²⁴⁷⁾ <http://www.fbi.gov/about-us/history/famous-cases/anthrax-amerithrax>

- Comment sont équilibrés les principes éthiques dans l’environnement réglementaire?
- Un règlement plus protecteur sur le plan éthique est-il nécessaire?
- Comment les défis mondiaux peuvent-ils être relevés?
- Quelles possibilités de gouvernance doivent être envisagées?

2.5.1. Comment sont équilibrés les principes éthiques dans l’environnement réglementaire?

L’environnement réglementaire semble se concentrer principalement sur la protection mondiale des *droits de l’homme*, notamment le *droit à la vie privée*, mais avec des niveaux de protection, de précision et d’efficacité très différents.

La protection de la vie privée gagne en importance partout dans le monde. La protection dans le cadre européen semble plus solide qu’ailleurs, avec des exceptions plus précises et un éventail d’interprétations de la Cour européenne des droits de l’homme. Néanmoins, l’importance de la protection de la vie privée reste subordonnée à la capacité de suivre le rythme de l’évolution des technologies et de fixer un «équilibre raisonnable» entre la vie privée et les intérêts de la sécurité nationale, de la sécurité publique, de la prévention de la criminalité, etc.

Malgré la reconnaissance généralisée de l’obligation de protéger le droit à la vie privée, le contenu spécifique de ce droit n’est pas complètement abouti pour ce qui est de l’équilibre avec les questions de sécurité. L’absence d’articulation explicite du contenu de ce droit a contribué à générer des difficultés dans son application et son respect. Comme le respect de la vie privée est un droit, son interprétation pose des difficultés pour déterminer ce que constitue la sphère privée et encadrer le concept d’intérêt public. Les évolutions rapides et importantes observées ces dernières décennies dans les technologies de l’information et de la communication ont également affecté de manière irréversible notre perception des limites entre sphères privée et publique.

Le Rapporteur spécial des Nations unies Frank La Rue souligne que «la sécurité nationale et l’activité criminelle peuvent justifier l’usage exceptionnel de technologies de surveillance des communications. Toutefois, les lois nationales réglementant ce qui constitue une

intervention nécessaire, légitime et proportionnelle de l’État dans la surveillance des communications sont souvent insuffisantes ou inexistantes. L’insuffisance des cadres juridiques crée un terrain propice aux atteintes arbitraires et illicites au droit à la vie privée dans le secteur des communications et, par conséquent, menace la protection du droit à la liberté d’opinion et d’expression» ⁽²⁴⁸⁾.

Le principal problème réglementaire réside dans la tension et l’équilibre entre la protection de la vie privée et l’autonomie d’une part et les restrictions fondées sur la protection, la sécurité nationale et l’activité criminelle de l’autre. Ce dilemme repose principalement sur la notion très générale, incertaine et souvent non documentée de la «sûreté» en tant que motif juridique permettant de limiter la vie privée. Il est essentiel, pour relever le défi d’un point de vue éthique, d’assurer plus de clarté, d’enrichir les documents existants et de trouver un équilibre plus explicite. En outre, la sûreté joue un rôle en tant que droit négatif d’être protégé contre l’intrusion de l’État, mais ne semble pas impliquer le principe déclaré de la sûreté en tant que droit positif. Enfin, l’absence ou l’insuffisance de gouvernance dans le domaine de la surveillance présente un problème.

2.5.2. Faut-il renforcer la réglementation?

Des lacunes existent donc avant tout au niveau de la mise en œuvre de la vie privée, du juste équilibre entre protection de la vie privée et sécurité, et de l’introduction de régimes de gouvernance dans le domaine de la surveillance, notamment des drones.

Comme la réglementation dans le domaine de la surveillance est rare — même dans le contexte de l’UE —, il convient de réfléchir à l’opportunité de mettre en place davantage de règles ou d’autres formes de gouvernance.

À l’échelle mondiale, le Rapporteur spécial des Nations unies sur la promotion et la protection du droit à la liberté d’opinion et d’expression, Frank La Rue, a exprimé certaines préoccupations au sujet de la surveillance dans le domaine des télécommunications, etc. ⁽²⁴⁹⁾. Le

⁽²⁴⁸⁾ Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d’opinion et d’expression, Frank La Rue, Nations Unies, Assemblée générale, 17 avril 2013 /A/HRC/23/40). Conseil des droits de l’homme, vingt-troisième session, p. 3: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

⁽²⁴⁹⁾ Ibid.

CHAPITRE II. | GOUVERNANCE — PRÉSENTATION, DÉFIS, POSSIBILITÉS

but de son rapport est «de recenser les risques que les nouveaux moyens et les nouvelles modalités de surveillance des communications font peser sur les droits de l'homme, notamment le droit à la vie privée et à la liberté d'opinion et d'expression». Certaines de ses préoccupations sont également pertinentes dans le contexte européen. Il souligne la nécessité de davantage réglementer le domaine de la surveillance: «Les techniques et les technologies de communication ont considérablement évolué, changeant ainsi la façon dont la surveillance des communications était réalisée par les États. Les États doivent donc mettre à jour leur interprétation et leur réglementation de la surveillance des communications et modifier leurs pratiques pour s'assurer que les droits de l'homme soient respectés et protégés.»

«La surveillance des communications devrait être considérée comme une mesure très intrusive, susceptible d'interférer avec les droits à la liberté d'expression et au respect de la vie privée et de menacer les fondements d'une société démocratique. La législation doit disposer que la surveillance des communications par les États ne peut avoir lieu que dans des circonstances exceptionnelles et uniquement sous le contrôle d'une autorité judiciaire indépendante. Des garanties doivent être prévues par la loi quant à la nature, l'étendue et la durée des mesures envisagées, les motifs nécessaires pour y avoir recours, les autorités compétentes habilitées à les autoriser, les mettre en œuvre et les contrôler, ainsi que les possibilités de recours prévues par la loi.

Les intéressés devraient avoir le droit d'être informés que leurs communications ont fait l'objet d'une surveillance ou que leurs données de communications ont été consultées par l'État. Une notification préalable ou simultanée risquerait de compromettre l'efficacité de la surveillance, mais les intéressés doivent néanmoins être avertis une fois la surveillance terminée et avoir la possibilité de demander réparation pour l'utilisation de mesures de surveillance des communications les concernant.

Des cadres juridiques doivent veiller à ce que les mesures de surveillance des communications:

- a) soient prescrites par la loi, en respectant une norme de clarté et de précision suffisante pour s'assurer que les individus soient mis au courant et puissent prévoir leur application;
- b) soient strictement et manifestement nécessaires à la réalisation d'un objectif légitime; et

- c) adhèrent au principe de proportionnalité et ne soient pas employées lorsque des techniques moins invasives sont disponibles et n'ont pas encore été épuisées.

Les États devraient pénaliser la surveillance illégale par les acteurs publics ou privés. Ces lois ne doivent pas être utilisées pour cibler les lanceurs d'alertes ou tout autre individu cherchant à dénoncer des violations des droits de l'homme, et ne devraient pas entraver le contrôle légitime des actions du gouvernement par les citoyens.»

Les propositions du Rapporteur spécial des Nations unies ont leur intérêt dans le contexte européen, même si elles sont essentiellement axées sur les défis mondiaux.

Les systèmes juridiques actuels (en Europe et ailleurs) n'ont pas été conçus pour les techniques de surveillance contemporaines. La réglementation n'est donc pas cohérente et un certain nombre de problèmes demeurent non résolus. Ce problème est flagrant lorsque l'on se penche sur la situation mondiale, mais il vaut également, dans une certaine mesure, pour la situation de l'Union européenne. Les réglementations nationales semblent avoir le même problème. Elles ne sont pas adaptées aux nouvelles technologies et aux nouveaux usages. Les solutions régionales et mondiales font défaut. Le sujet est cependant à l'ordre du jour dans de nombreux pays. Il est peut-être temps de proposer une réglementation dans ce domaine.

2.5.3. Comment relever les défis mondiaux?

L'un des enseignements les plus marquants tirés des récentes révélations concernant la surveillance de masse est la nécessité de trouver une solution mondiale en matière de sécurité et de surveillance. Les transferts de données de plus en plus fréquents dans le contexte de la sécurité et de la coopération policière posent un risque en l'absence de normes communes en matière de confidentialité et de protection des données. En outre, de récentes preuves démontrent que certains services publics souhaitant capitaliser sur la faiblesse de la supervision réglementaire et les lacunes des régimes juridiques des partenaires internationaux pratiquent une politique «à la carte» en la matière. Cependant, la réalisation d'une solution internationale pose des défis considérables, vu les nombreux efforts nécessaires pour parvenir à un consensus international sur la gouvernance mondiale dans un certain nombre de domaines, où la nécessité d'aboutir à des solutions universelles est reconnue.

Compte tenu de ces expériences et d'une approche réaliste, il peut s'avérer plus intéressant de signer des accords bilatéraux avec le plus grand nombre de pays possible. Il semble évident de démarrer avec les autres pays de l'UE et, bien sûr, les États-Unis, qui sont aussi un partenaire naturel pour nouer des accords. À cet égard, la diplomatie publique constituerait un bon point de départ ⁽²⁵⁰⁾. Dans ce sens, le Parlement européen a publié un appel pressant à l'Union européenne et aux États-Unis pour qu'ils poursuivent les négociations sur un accord-cadre relatif à la protection des données dans le domaine de la coopération policière et judiciaire et qu'ils revoient les accords de transfert de données existant ⁽²⁵¹⁾.

2.5.4. Quelles possibilités de gouvernance doivent être envisagées: la boîte à outils?

Les tensions entre la vie privée et les (nouvelles) technologies ont été pour l'essentiel abordées par l'intermédiaire de quatre instruments: La technologie, l'éducation, l'autoréglementation et le droit ⁽²⁵²⁾. Ce chapitre se concentre sur les solutions de gouvernance, mais d'autres outils peuvent également s'avérer pertinents.

La gouvernance par la technologie part du principe que la difficulté liée au caractère mondial de l'information peut être contournée par des solutions d'origine technologique. Ainsi, il est plus facile de diffuser des renseignements personnels aux quatre coins du monde grâce aux réseaux d'information et de communication lorsque la technologie implique des opérations menées par différents acteurs situés dans différents pays régis par différentes juridictions. Il est alors difficile de définir correctement les règles applicables en matière de protection de la vie privée ou de protection des données personnelles et d'avoir accès à des autorités habilitées à les appliquer. Un bon moyen d'utiliser la technologie à cet égard est de recourir aux *technologies renforçant*

la protection de la vie privée, lorsque le risque de contrevenir aux principes de protection de la vie privée et à la législation est limité par une technologie spécifique. Parmi les autres instruments de gouvernance technologique figurent la vie privée dès la conception, la vie privée dans la conception, l'évaluation de l'incidence sur la vie privée et l'évaluation de l'incidence de la surveillance.

La gouvernance par l'autoréglementation vise à promouvoir un comportement (vertueux) en faisant intervenir les parties prenantes et en établissant une réglementation souple du bas vers le haut. Habituellement, la gouvernance par l'autoréglementation est un mélange entre la régulation par le marché et l'autoréglementation. La responsabilité sociale des entreprises (RSE) et les mesures d'incitation des pouvoirs publics pour la recherche peuvent faire progresser la technologie dans un sens plus éthique. Les codes éthiques et la RSE ont toutefois peu d'importance dans le domaine de la sécurité. Le Code du Royaume-Uni sur la vidéosurveillance mentionné ci-dessus est un exemple en la matière, mais d'autres instruments de législations non contraignantes, notamment des codes de conduite, pourraient être mis en place.

La réglementation traditionnelle est efficace en ce sens que la législation contraignante peut être appliquée, mais cela implique aussi certaines difficultés. L'une d'entre elles concerne les normes universelles, qui ont souvent tendance à être trop vagues, abstraites et difficiles à mettre en œuvre. Un bon exemple est le principe de la proportionnalité, dont les formes juridiques et les traditions sont très variées. Des désaccords peuvent ainsi surgir sur l'importance à accorder à des intérêts divergents et sur les indicateurs à utiliser pour évaluer les résultats. La loi peut être interprétée et précisée par des décisions de justice.

Dans le domaine de la *surveillance*, l'UE peut prendre des initiatives pour mettre cette question à l'ordre du jour et encourager les États membres à promulguer ou réviser les règlements dans le domaine. Il semble important de veiller à ce que la surveillance publique et la surveillance par des parties privées soient toutes deux soumises à la réglementation. Une approche plus axée sur le processus serait de commencer avec les mesures d'autorégulation, autrement dit une législation non contraignante. Le Code de conduite britannique et des expériences dans d'autres domaines peuvent servir d'inspiration.

Le consentement est souvent utilisé comme condition préalable à l'action, mais dans le domaine de la

⁽²⁵⁰⁾ M. Leonard, *Public diplomacy*, Londres, 2002; J. Melissen, ed. *The New Public Diplomacy, Soft Power in International Relations*, New York, 2005; J. S. Nye, *Soft Power. The Means to Success in World Politics*, New York, 2004.

⁽²⁵¹⁾ Rapport de la commission LIBE du Parlement européen sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures.

⁽²⁵²⁾ «Ethical and Regulatory Challenges to Science and Research Policy at the Global Level.» Commission européenne, 2012.

CHAPITRE II. | GOUVERNANCE — PRÉSENTATION, DÉFIS, POSSIBILITÉS

surveillance, du contrôle des frontières, etc. cette solution pose problème, dans la mesure où le but de la surveillance et du contrôle des frontières ne peut souvent pas être rempli si le consentement est revendiqué. C'est pourquoi une réglementation est nécessaire pour assurer d'autres formes de protection.

Les droits de l'homme et de la protection de la vie privée sont d'une importance cruciale dans le cadre réglementaire, aujourd'hui mais aussi probablement à l'avenir. Si la vie privée est jugée primordiale, il y a lieu d'envisager d'étendre, de préciser, de contrôler et de mettre en œuvre le concept de la vie privée. L'Europe semble être à l'avant-garde lorsqu'il s'agit de la protection de la vie privée et de la protection des données. Une collaboration à l'échelle mondiale serait fructueuse à cet égard, puisque de nombreux défis sont mondiaux. Toutefois, pour développer des solutions mondiales, la meilleure voie à suivre à ce stade consiste peut-être à obtenir des consensus bilatéraux, fondés sur la diplomatie publique.

L'expansion peut faire partie d'un processus global, en essayant d'atteindre un consensus plus large du point de vue de l'étendue et du contenu. La spécification peut s'avérer pertinente pour équilibrer la vie privée et la sécurité, etc. Sur la base de la proposition du Rapporteur spécial de l'ONU, il est possible de proposer de soumettre le droit à la vie privée à certaines restrictions, notamment si : ces restrictions sont prévues par la loi ; l'essence même d'un droit de l'homme n'est pas soumise à ces restrictions ; ces restrictions sont nécessaires dans une société démocratique ; ces restrictions sont conformes au principe de proportionnalité, appropriées pour remplir leurs fonctions de protection, le moyen le moins intrusif parmi ceux susceptibles d'aboutir au résultat désiré, et proportionnées à l'intérêt à protéger. Le contrôle et la mise en œuvre peuvent aussi être à l'ordre du jour.

Il serait bon de procéder à un échange d'expériences entre les États membres pour tenter de parvenir à un consensus plus large. En outre, il pourrait s'avérer utile de nommer une personne ou une institution en particulier pour contrôler, critiquer, proposer et convaincre.

2.6. Conclusion

Le paysage réglementaire de l'UE en matière de sécurité et de surveillance dans son ensemble semble contrasté et à bien des égards incertain. Les principaux instruments de gouvernance ont pour but de protéger les droits de l'homme, notamment le droit à la vie privée et

la protection des données. Si les droits de l'homme et la protection de la vie privée sont dans une large mesure des droits universellement reconnus, l'UE est à la pointe lorsqu'il s'agit de protéger la vie privée et les données, en partie grâce à la Cour européenne des droits de l'homme et à ses interprétations dynamiques. L'UE dispose également d'un certain nombre d'instruments de gouvernance pour l'aviation, le contrôle des frontières et la cybercriminalité, qui font également office dans une certaine mesure de dispositions universelles.

Les défis et les possibilités sont les suivants :

1. Il est difficile de trouver le juste équilibre entre les droits de l'homme et la protection de la vie privée d'un côté et la sécurité nationale et la prévention de la criminalité de l'autre. La vie privée est limitée pour des raisons de sécurité, mais souvent les dispositions relatives à la gouvernance sont très vagues et les solutions théoriques. Ce défi peut être relevé en établissant des règles plus solides dans le domaine et en introduisant des conditions plus précises pour un juste équilibre.
2. Certains domaines de la sécurité nationale et de la surveillance, qui restent largement de la compétence des États membres, présentent de nombreux défis en matière de mesures de gouvernance. Les caméras de vidéosurveillance et la surveillance des télécommunications méritent un intérêt particulier. Les réglementations nationales diffèrent, mais tout le monde s'accorde sur le fait que les mesures de gouvernance ne sont pas suffisamment solides et protectrices. Une solution pourrait être de veiller à mettre en place des limitations et des permis pour la vidéosurveillance et un contrôle judiciaire pour la surveillance des télécommunications.
3. De nouvelles technologies de surveillance, tels que les drones, présentent des défis dans la mesure où la réglementation actuelle peut ne pas être suffisante.
4. Le lancement d'alertes est à l'ordre du jour, et dans de nombreux pays européens l'expansion des mesures de gouvernance visant à protéger les lanceurs d'alertes permettent d'assurer une meilleure protection grâce à la réglementation traditionnelle.
5. Une meilleure coopération internationale dans le domaine de la gouvernance pourrait contribuer à accroître la protection juridique dans des domaines cruciaux.

Chapitre III. Analyse éthique

3.1. Perspectives historiques et sociopolitiques

3.1.1. L'évolution de la notion de sécurité

La *sine cura* dans une réflexion

Un premier fondement de la notion contemporaine de la sécurité est la *sine cura* (du latin *securus* qui signifie «exempt de souci, tranquille» avec la préposition *sine*, ou *se cura* qui se compose de *se* «sans, exempt de» et de *cura* «la charge», mais aussi «l'inquiétude, le souci»). Dans ce contexte antique, cet état de sécurité, de tranquillité d'esprit, était l'objectif que plusieurs philosophies de l'ataraxie (stoïcisme, épicurisme, scepticisme) poursuivaient. Trois éléments de tension sont particulièrement importants à noter en ce qui concerne la création du concept. Tout d'abord, les tensions entre la notion de sécurité synonyme de liberté d'esprit, d'insouciance, et de légèreté et celle synonyme de négligence, de nonchalance et d'imprévoyance ⁽²⁵³⁾. Ensuite, l'accent mis dans ce contexte sur les dimensions subjectives et internes permettant d'atteindre cet état de sécurité (par rapport aux réalités extrinsèques). Troisièmement, la double notion de la sécurité à laquelle ce développement initial a donné lieu: la première correspond au sens de la sécurité tel que nous l'entendons généralement aujourd'hui, à savoir le fait d'être en sûreté, protégé, exempt de danger; la seconde acception se réfère aux faux sentiments de sécurité, à la confiance mal placée dans l'état ou la position de quelqu'un (James Der Derian illustre remarquablement bien ce sens de la sécurité en citant *Macbeth* de Shakespeare «la sécurité est la plus grande ennemie des mortels» — et un certain nombre de sermons des XVI^e au XIX^e siècle, qui soulignent la façon dont le mot a été utilisé de façon négative lorsqu'il s'agissait de se prémunir contre le péché de la sécurité sous peine d'en subir les conséquences) et est donc antithétique à la première ⁽²⁵⁴⁾.

⁽²⁵³⁾ Michael Dillon, *Politics of Security: Towards a Political Philosophy of Continental Thought*, Londres: Routledge, 1996.

⁽²⁵⁴⁾ Les développements présentés dans ce chapitre de l'évolution de la notion de sécurité reposent sur les ouvrages de Frédéric Gros, «Le Principe Sécurité», Paris: Gallimard, 2012 et de Jim Dratwa, «Risque, Rixe, Rhizome: Guerre et Paix avec l'Analyse des Risques et les Organisations Internationales», Techniques et Philosophies des Risques, éd. G. Hottois & C. Kermisch, Paris: Vrin, 2007.

Contrat social, sécurité et le rôle de l'État

Dans la pensée antique et médiévale, la notion de sécurité a été subordonnée à la réalisation des finalités éthiques et religieuses des individus et de la communauté politique. La question de la sécurité devient centrale avec la sécularisation de la pensée politique moderne et la naissance de l'État moderne. L'État est le lieu où la sécurité est garantie; la sécurité est justifiée — et réglementée — par la «raison d'État».

Le début du XVI^e siècle a radicalement transformé le cadre (européen) de la sécurité. C'est à cette époque que la sécurité commence à être perçue comme un problème politique, portant sur la protection extérieure contre la guerre et la violence. Nicolas Machiavel (*Le Prince*, 1513) l'associe à l'exercice du pouvoir politique absolu, en considérant le phénomène de la sécurité de l'État (de la principauté) comme une réaction à des risques, des menaces, des difficultés et des dangers visant à garantir la sécurité des citoyens de l'État.

Thomas Hobbes (*Leviathan*, 1651) considère l'état de nature comme l'état d'origine dans lequel l'individu instinctif agit librement et égoïstement selon ses propres intérêts (principe de l'autopréservation). Hobbes estime que la transition de l'état de nature à un état civilisé est essentielle pour surmonter la condition intolérable du danger permanent, du conflit et de l'agressivité (*homo homini lupus*), sources de peur individuelle et d'insécurité sociale. La reconnaissance de l'aspiration naturelle de l'homme à la sécurité justifie l'état civilisé: pour sécuriser l'autoprotection (conservation de la vie et de la paix), un contrat social est fixé, autrement dit un pacte d'*unionis* et *subjectionis*. Les citoyens s'associent et renoncent à une part de leur liberté, en la déléguant au souverain qui acquiert un pouvoir absolu pour garantir la sécurité. La sécurité devient l'objectif des citoyens et la justification morale du pouvoir absolu de l'État et de la limitation de la liberté des citoyens: la volonté de se soumettre à souverain politique absolu n'est justifiée que par la préservation de la sécurité, autrement dit la préservation de la vie et de la paix, la protection de (la crainte de) la mort et de la violence.

Spinoza (*Traité politique*, 1677) considère la sécurité comme l'origine et le but de l'État: l'État existe parce que l'ordre social (la paix) — assurée par la menace de la force — est une condition nécessaire (mais pas suffisante) pour satisfaire l'aspiration de l'individu à la sécurité (principe de l'autopréservation) et au bien-être.

CHAPITRE III. | ANALYSE ÉTHIQUE

En opposition à la perspective absolutiste, John Locke (*Deuxième traité du gouvernement civil*, 1690) interprète la notion de sécurité et de contrat social dans un cadre libéral: l'état de nature est un état dans lequel existent des lois naturelles innées (la vie, la santé, la liberté, la propriété, l'égalité) qui, en raison de leur précarité, doivent être garanties par la constitution d'un État social, par l'intermédiaire d'un contrat social. La précarité est synonyme d'insécurité dans un état de nature due à l'absence d'un État garantissant la sécurité par des lois et des sanctions judiciaires impartiales en cas de transgression de ces lois. La sécurité est associée à la paix (la préservation, le maintien et le renforcement des droits naturels), c'est-à-dire la conservation de la vie et de la santé, la jouissance de la liberté et de la propriété, la préservation de l'égalité.

Même si elle se développe dans un autre contexte théorique (celui de l'absolutisme et du libéralisme), l'école de la loi naturelle théorise la sécurité avec certains éléments communs: 1) la condition et la légitimation du pouvoir politique; 2) la justification du contrat social en tant que renonciation volontaire d'une part de sa liberté pour vivre libre et en sécurité dans une société pacifique; 3) la protection contre les menaces extérieures (la violence, la guerre).

C'est au XIX^e siècle que la «sécurité politique» s'est enrichie par l'intermédiaire de la «sécurité sociale» et de l'État-providence. La notion d'État-providence est intimement liée à la fois à la sécurité individuelle et à la sécurité d'État. Le terme allemand Sozialstaat («État social»), par exemple, est utilisé depuis 1870 pour décrire les programmes d'aide d'État mis au point par les Sozialpolitiker allemands («politiciens sociaux») et mis en œuvre dans le cadre des réformes de Bismarck. L'équivalent littéral en anglais «social state» n'a jamais pris dans les pays anglophones, jusqu'à la Seconde Guerre mondiale, lorsque l'archevêque anglican William Temple (l'auteur du livre *Christianisme et ordre social*, publié en 1942) a popularisé le concept en utilisant l'expression «welfare state», pour opposer l'État-providence de la Grande-Bretagne pendant la guerre au «warfare state» de l'Allemagne nazie.

Après la Deuxième Guerre mondiale, le principe de destruction mutuelle garantie et la théorie des relations internationales

Il est important de prêter attention non seulement à l'évolution des configurations géopolitiques, mais aussi à l'évolution des *Weltanschauungen* (visions du monde), des descriptions ou des modes de pensée grâce auxquels elles sont comprises ou prennent sens.

Il convient de noter le lien étroit entre la guerre froide et l'avènement et la mise en place d'études de sécurité en tant que discipline ou domaine universitaire. À cet égard, la Deuxième Guerre mondiale a marqué un tournant dans l'intérêt présumé et la capacité des États à protéger leurs propres citoyens de dommages physiques. Si le principe de souveraineté original est un compromis étrange dont le principal avantage était la réduction de la probabilité de guerre entre les États et, par extension, de massacre de masse (ou d'autres dommages), après la Deuxième Guerre mondiale, il est devenu manifestement nécessaire de restreindre le principe de souveraineté pour protéger la vie des gens ordinaires (des minorités notamment) qui, au cours des siècles précédents, auraient été protégés (par principe au moins des dommages physiques) en échange de leur soutien au pouvoir de l'État. Le sens à accorder à la notion de «sécurité» a également suscité un vif débat (tout comme le fait de savoir si les États — l'unité de base dans la théorie des relations internationales — restaient utiles en tant que centres du débat et justifications).

Il est important de mettre en lumière les liaisons existant entre le «contrat social» examiné ci-dessus et les tensions analysées par la suite dans l'opinion entre les différents encadrements de la sécurité, en ce qui concerne les «compromis» et la sécurité de l'individu par rapport à la sécurité de l'État. Tout d'abord, les arguments du contrat social (ou politique) soutiennent traditionnellement que les individus ont consenti, explicitement ou tacitement, à renoncer à certaines de leurs libertés et de se soumettre à l'autorité du souverain (ou à la décision de la majorité) en échange de la protection des droits qui leur restent. Il est fondamental de noter ici que le contrat social commet ainsi le «péché originel», à savoir le compromis initial qui sous-tend ceux qui suivent ⁽²⁵⁵⁾. Concentrons-nous sur la conceptualisation de Hobbes. Comme indiqué ci-dessus, le contrat social

⁽²⁵⁵⁾ Il convient également de noter ici que «le nom de contrat social (ou contrat originel) couvre souvent deux types de contrats différents qu'il est utile de distinguer pour retracer l'évolution de la théorie. Les deux étaient courants au XVII^e siècle et les deux trouvent leur origine dans la pensée politique grecque. (...) [Le premier] implique généralement une théorie de l'origine de l'État. La deuxième forme de contrat social peut être plus précisément appelée contrat de gouvernement, ou contrat de soumission...» J. W. Gough, *The Social Contract*, Oxford: Clarendon Press, 1936, p. 2-3. En d'autres termes, le premier concerne l'origine de l'État, tandis que le deuxième concerne le contrat — le *modus vivendi* — entre le(s) dirigeant(s) et les dirigés, entre le gouvernement et les gouvernés. Cette dualité du contrat social est au cœur de la critique du concept menée par David Hume.

marque l'instant à partir duquel les individus se sont réunis et ont cédé certains de leurs droits individuels pour que d'autres cèdent les leurs, c'est-à-dire un compromis mutuel. Cela a abouti à la création d'une entité souveraine, l'État. Et pourtant, le système des États nés du contrat social était également anarchique dans la mesure où les États n'avaient pas de direction faisant autorité. Tout comme à l'état de nature, les individus n'étaient guidés que par leur intérêt personnel et l'absence de droits, de sorte que les États agissaient dans leur propre intérêt et se retrouvaient en concurrence avec les autres. Tout comme à l'état de nature, les États étaient donc voués à être en conflit, car il n'y avait aucun souverain au-dessus des États capable d'imposer un même système à tous (comme les lois de contrat social) par la force. C'est sur ces bases que le travail de Hobbes a servi de fondement aux théories réalistes des relations internationales — comme l'expliquent E. H. Carr et Hans Morgenthau — au milieu du XX^e siècle.

Giorgio Agamben — dans son œuvre comme dans son intervention à la table ronde publique organisée pour l'élaboration du présent avis — attire l'attention sur un éventail de graves difficultés liées à l'engagement envers la sécurité. Dans son *Homo sacer, Le pouvoir souverain et la vie nue* et son *État d'exception*, Agamben relie le concept d'«état d'exception» (*Ausnahmezustand*) utilisé par Carl Schmitt (pour qui le «Souverain» est celui qui a le pouvoir de décider de l'état d'exception) aux concepts romains de *justitium* et *auctoritas*. Alors que Schmitt vise à inclure la nécessité de l'état d'urgence dans l'état de droit, Agamben démontre au contraire que toutes les formes de vie ne peuvent être régies par la loi. Agamben examine les pouvoirs accrus auxquels les gouvernements ont recours en temps dits de crise. En ces temps de crise, il qualifie ces élargissements du pouvoir d'*état d'exception*, dans lequel les questions de citoyenneté et les droits de l'individu peuvent être dénigrés voire disqualifiés par le gouvernement, mais toujours au nom de la sécurité. Le pouvoir politique sur les autres acquis grâce à l'état d'exception place le gouvernement (ou un de ses départements) dans une position de toute-puissance, au-dessus des lois. Pendant ces périodes, certaines formes de connaissance sont alors favorisées et acceptées comme vraies et certaines voix sont jugées précieuses, alors que d'autres sont écartées. Cette distinction d'oppression revêt une grande importance en ce qui concerne la production de connaissance. Le processus d'acquisition de certaines connaissances et de refoulement d'autres connaissances est un acte de violence en temps de crise. En outre, Agamben examine la façon dont la suspension des lois dans un état d'exception — d'urgence ou de crise — peut devenir un état de fait permanent.

Giorgio Agamben attire également l'attention sur la façon dont l'économie libérale moderne a contribué au passage de la perspective de la prévention à une approche de «laisser-faire», dans laquelle il convient de gérer les effets (plutôt que les causes) des problèmes, des risques ou des crises (et donc surveiller et contrôler) au nom de la sécurité. La question sous-jacente est de savoir si cela est compatible avec la démocratie.

Après le 11 Septembre et après le 11 Mars

Ces nouvelles configurations géopolitiques peuvent également être observées au niveau de l'évolution des conceptions de la sécurité. Si les approches classiques de la sécurité (approches matérialistes dans les études de sécurité dans les relations internationales) se concentrent sur les dispositions matérielles de la menace, notamment la répartition du pouvoir, les capacités militaires et la polarité, l'approche dite de «sécurisation» se penche quant à elle sur la façon dont une certaine question est transformée par un acteur en une question de sécurité. Une telle manœuvre permet à un acteur d'utiliser des moyens extraordinaires au nom de la sécurité. Le débat sur l'immigration qui fait rage aux États-Unis est un exemple de cette théorie de la sécurisation. Les préoccupations d'infiltration terroriste sont régulièrement citées comme motifs pour un contrôle strict des frontières. Comme il est plus facile de «sécuriser» un problème (c'est-à-dire le faire passer pour une question de sécurité) depuis le 11 Septembre, cette préoccupation pour la sécurité et la sûreté a détourné l'attention des facteurs socio-économiques en jeu en matière de migrations internationales et de la discussion sur les racines de cette immigration.

Des tendances similaires ont été examinées dans le contexte européen, où le fondement du renforcement du contrôle aux frontières et de l'installation de technologies de surveillance aux frontières est lié à la lutte contre les menaces de la criminalité transnationale telles que le terrorisme, le trafic de drogues, la traite des êtres humains et la contrebande. Une sécurisation dynamique a donc été envisagée pour inscrire cette forme indésirable de mobilité humaine connue sous le nom de migration irrégulière dans un cadre européen et la placer dans la même catégorie que d'autres menaces, comme la criminalité organisée et le terrorisme, des menaces pour lesquelles des pratiques de surveillance, de contrôle et de sanctions sont mises en place ou jugées nécessaires et légitimes.

Sur cette toile de fond, le tournant du millénaire ou la fin du XX^e siècle marque également, dans l'imaginaire

CHAPITRE III. | ANALYSE ÉTHIQUE

européen, un jalon sur la voie de la (ré)unification du continent et de son/ses peuple(s), avec la chute du rideau de fer et la sortie prometteuse d'une période non seulement de division, mais aussi de totalitarisme (sous le joug d'un appareil d'État soutenu par des services de renseignement et de sécurité persuasifs), l'abandon des bonnes intentions qui mènent tout droit vers l'enfer, et pas seulement sous le nazisme et le stalinisme. Ce chapitre à peine refermé, les Européens gardent à l'esprit la *Securitate* de Ceaușescu et la *Stasi* (la police secrète *Staatssicherheit*) qui signifie littéralement «Sécurité de l'État».

Recherche de la sécurité, risques et État

La sécurité est non seulement à la base du cadre des droits de l'homme, c'est aussi la pierre angulaire du contrat social. Qu'il s'agisse de Hobbes, de Locke, de Spinoza ou de Rousseau, tous ces théoriciens de la politique ont fait de la sûreté civile et de la sécurité civile, le motif et la fin du contrat social ⁽²⁵⁶⁾, comme discuté ci-dessus. La sécurité civile désigne, dans cette perspective, le droit de chacun d'être préservé des risques de violence. En revanche, elle prépare également la définition d'un État qui détient, selon les termes utilisés par Max Weber (dans *Politics as a vocation*), le monopole de l'usage légitime de la violence ou de la force. En outre, elle trouve une résonance particulière dans le contexte de la «société du risque», comme l'explique Ulrich Beck, dans laquelle — contrairement à la «société industrielle» où la question déterminante était la distribution (in)équitable des biens — la question centrale est celle de la répartition de l'aspect négatif des risques. À quel genre de sécurité d'État les membres de la société du risque aspirent-ils? Que signifie, pour l'État, réussir à revendiquer un monopole sur l'utilisation légitime du risque? Et sur l'assurance légitime de la sécurité? Et si l'État «dissociait» — démantelait ou cédait — ses prérogatives oligopolistiques ou ses revendications, comme l'utilisation légitime de la force?

Les sciences et les technologies sont au cœur de la relation entre le public et l'État par le recours aux notions de légitimité et de sécurité. Cette constatation puissante — qui remonte à Max Weber et même à Aristote — a été rigoureusement documentée dans les travaux de James C. Scott (Scott 1998) et de Yaron Ezrahi

(Ezrahi 1990) ⁽²⁵⁷⁾. Il s'agit d'une caractérisation de l'État démocratique qui cherche en permanence à s'autolégitimer par des performances scientifiques et technologiques (par ex. des projets à grande échelle, «des modernisations», l'institutionnalisation d'avis d'experts scientifiques). La promesse classique de progrès est un marqueur de ces liens qui unissent la science et l'État, qui dépendent tous deux de cette même promesse. Dans le contexte contemporain, cette mobilisation de la recherche, du développement et de l'innovation prend la forme stylisée d'entreprises parallèles, l'une pour déverrouiller la compétitivité, la croissance et l'emploi et l'autre pour relever les principaux défis de la société. Ces entreprises sont en outre censées s'alimenter l'une l'autre, la deuxième en créant de nouveaux débouchés commerciaux pour la première, et la première en générant plus de capital à investir dans la deuxième.

Les effets indésirables et/ou imprévus, qu'ils soient considérés comme des «externalités» ou des «risques», constituent le revers de cet arrangement. D'où également l'importance cruciale et souvent confuse de la répartition des bénéfices, des coûts et des risques de ces efforts de la science et des nouvelles technologies (et bien sûr d'où la nécessité de développer une éthique et des cadres réglementaires pour toutes les tentatives du genre).

La recherche dans le domaine de la sécurité ⁽²⁵⁸⁾ et le développement des technologies de sécurité ont donc pour objet de contrer les inconvénients de cet arrangement. Ils portent en eux — même en tant que projet ou promesse — la résolution des situations énoncées ci-dessus. Ils portent également en eux les ambiguïtés et les tensions constitutives de la notion même de sécurité (et c'est précisément ces tensions constitutives qui ont été examinées dans les sections précédentes de ce chapitre).

⁽²⁵⁷⁾ Scott, James C., *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*, New Haven, CT: Yale University Press, 1998; Ezrahi Y., *The Descent of Icarus: Science and the Transformation of Contemporary Democracy*, Cambridge, MA: Harvard University Press, 1990.

⁽²⁵⁸⁾ Il est intéressant d'examiner ici la notion de la «recherche en tant qu'outil d'élaboration de politiques». En effet, dans certains cas, des politiques de surveillance voient le jour en tant que projets de recherche (EUROSUR étant ici un excellent exemple). Le financement des technologies et des projets de sécurité et de surveillance évite parfois d'ouvrir un débat qui tienne compte du caractère politiquement sensible des problèmes que ces technologies entendent résoudre.

⁽²⁵⁶⁾ Kriegel B., «Le risque de développement», *Philosophie Politique* 11, Paris, PUF, 2000; Guéry F., «Risque, Assurance, Sécurité», *Philosophie Politique* 11, Paris, PUF, 2000.

Développement de la doctrine de sécurité humaine

Les paradigmes traditionnels de la sécurité, sous le couvert de la «sécurité nationale» ou de «la sécurité d'État» se rapportent à la capacité d'un État à se défendre des menaces extérieures. Cela s'inscrit dans la philosophie de la prédominance de la sécurité internationale qui prévaut depuis les traités de Westphalie en 1648 et l'avènement de l'État-nation. Si la théorie des relations internationales englobe classiquement de nombreuses variantes de la sécurité traditionnelle, la caractéristique fondamentale que partagent différentes variantes est leur adhésion à la primauté de l'État-nation.

La sécurité humaine, contrairement à ces approches, soutient que le référent en matière de sécurité doit être l'individu plutôt que l'État. Ce paradigme pour la compréhension des vulnérabilités globales part du principe qu'une vue de la sécurité axée sur le peuple est nécessaire pour la sécurité nationale, régionale et mondiale.

En comblant partiellement les lacunes de la doctrine de la sécurité humaine, la notion de «sécurité sociétale» est un enrichissement intéressant par rapport à d'autres conceptions de la sécurité, qui a permis certains progrès dans le domaine des relations internationales et des études de sécurité (avec la migration comme sous-thème commun). Plutôt que de faire de l'individu le principal référent en matière de sécurité, cette perspective considère la société comme l'objet des menaces de sécurité. La société est ici entendue comme un ensemble de valeurs, de coutumes, d'expériences partagées, d'institutions économiques et de traditions juridiques et artistiques, c'est-à-dire la vie organique et collective de la communauté. La sécurité sociétale a été définie comme «la capacité d'une société à persister dans son caractère essentiel sous des conditions changeantes et des menaces possibles ou réelles» (Buzan, Wæver et De Wilde, 1998) ⁽²⁵⁹⁾. La sécurité sociétale, à l'instar de la sécurité humaine, vise à répondre à l'évolution du contexte des menaces qui ne reflète plus la logique traditionnelle de la sécurité d'État. Elle est moins axée sur la protection contre les menaces externes ou la protection contre les dommages physiques que sur la nécessité de résilience de la société face à l'insécurité. La sécurité sociétale dépasse la notion de sécurité centrée sur l'individu et met l'accent sur les sources sociétales de bien-être.

En ce qui concerne la sécurité humaine en tant que telle, le programme de développement des Nations unies de 1994 intitulé *Rapport mondial sur le développement humain* est une publication-charnière dans le domaine de la sécurité humaine, avec son argument selon lequel la garantie pour tous de la «liberté de choix» et de «l'affranchissement de la peur» est la meilleure façon de s'attaquer au problème de l'insécurité à l'échelle mondiale. Le rapport fait valoir que le champ de la sécurité mondiale devrait être élargi pour inclure les menaces dans sept grandes rubriques: la sécurité économique, la sécurité alimentaire, la sécurité sanitaire, la sécurité de l'environnement, la sécurité personnelle, la sécurité de la communauté, la sécurité politique.

En 2003, l'ONU a créé la *Commission sur la sécurité humaine*, dont la «Doctrine de la sécurité humaine» (DSH) est devenue le point de référence de la plupart des stratégies de sécurité. La DSH plaide pour un changement de paradigme d'une sécurité basée sur des actifs matériels (tels que les frontières, les biens et les propriétés) vers un système basé sur des valeurs humaines immatérielles.

En 2004, le *groupe d'étude sur les capacités européennes de sécurité* convoqué par Javier Solana a présenté la «Doctrine de la sécurité humaine pour l'Europe» en tant que cadre politique de la stratégie européenne de sécurité, basé sur l'approche des Nations unies présentée ci-dessus.

La DSH est véritablement éloquente et intègre visiblement des caractéristiques plus élaborées sur le plan éthique que les doctrines traditionnelles de «sécurité nationale», mais elle repose sur des assimilations et des artifices qui pourraient à la fois dissimuler les tensions inhérentes à la notion de «sécurité» et tomber dans la généralité. Dans cette manœuvre équivoque, qui place également la sécurité comme ultime *telos*, la «sécurisation» prend une nouvelle forme étonnante et l'«état d'exception» (ou l'état d'urgence) trouve une nouvelle justification surprenante.

3.1.2. Les tensions qui structurent la notion de sécurité ou qui s'y rattachent

Ce bref aperçu de la conceptualisation historique et politique de la sécurité montre les tensions qui existent entre d'une part le sens privé et social de la sécurité et d'autre part son sens politique, public et militaire. Au tournant du millénaire, l'espoir était certainement d'élargir le concept politique et public pour embrasser l'approche sociale de la sécurité. C'est ce que recherchaient les objectifs du Millénaire pour le développement en

⁽²⁵⁹⁾ Buzan, Barry, Ole Wæver, and J. de Wilde, eds. *Security: A New Framework for Analysis*, Boulder, CO: Lynne Rienner, 1998.

CHAPITRE III. | ANALYSE ÉTHIQUE

relevant les défis de la pauvreté mondiale et de l'absence de développement. La sécurité dans le sens «social» était considérée comme l'un des moyens, et peut-être le plus important d'entre eux, d'assurer la paix internationale.

Mais il n'a fallu qu'une décennie pour que les «anciens» cadres refassent leur apparition et redéfinissent la notion de la sécurité selon l'acceptation «politique» de sécurisation de la sphère publique. Les individus se sont sentis menacés après plusieurs attaques terroristes et la montée en puissance des groupes terroristes internationaux. Les menaces contre la sécurité sont devenues «le revers» de la mondialisation, et l'idée que la politique devait réagir à ces menaces en augmentant les mesures de surveillance a pris de l'ampleur. Il n'appartient pas à ce rapport de décider de l'opportunité de cette réponse ou de dire si la menace des groupes terroristes a été utilisée pour développer un système de sécurité permettant aux États de surveiller leurs citoyens dans des proportions jamais vues auparavant. Cet aspect sera certainement l'objet d'études historiques. Mais il est clair que l'approche plus sociétale a fini par être reléguée après les attaques du 11 septembre. Comme les technologies de surveillance ne cessaient d'évoluer, il est en effet apparu possible de fournir les moyens de sécuriser le domaine public dans ce sens. Loin des politiques de sécurité du XX^e siècle, la mondialisation a transformé la «sphère publique nationale» en une sphère publique *mondiale*, une sphère publique qui ignore les frontières nationales et/ou les lois nationales.

La philosophie politique dans le monde moderne a toujours fait valoir que, au moins dans les États démocratiques, les représentants élus étaient liés par la «volonté du peuple» et qu'ils étaient par conséquent tenus pour responsables de leurs actes. Cela s'est révélé un véritable défi dans le cadre des nouvelles politiques de sécurité, et les justifications du secret et de la non-transparence ont une nouvelle fois tourné autour de l'argumentation des «circonstances exceptionnelles» ou de «l'état d'exception». Aujourd'hui, la question est de savoir si cette argumentation est en fait devenue l'argumentation déterminante de la politique de sécurité, de connaître le degré de transparence qu'il est possible de maintenir et de décider de la façon d'interpréter deux changements décisifs, à savoir, d'une part, l'intersection des usages politiques et privés des technologies de sécurité et de surveillance et, d'autre part, le développement des pratiques basées sur les TIC dans notre vie sociale. Ces deux développements remettent en question l'idée selon laquelle le «souverain» est celui qui prend toutes les décisions en matière de sécurité. En fait, c'est exactement le rapport entre la souveraineté et

la non-souveraineté des représentants élus (et des États, des sociétés et des individus) qui doit être redéfini.

Un autre changement concerne la nature transnationale des TIC. La sécurité et la surveillance doivent être traitées en premier lieu comme des «affaires intérieures» des États membres de l'Union européenne, puis comme des pratiques transnationales qui dépassent le contrôle démocratique d'un État membre, mais également celui de l'Union européenne, et enfin comme des questions transnationales fondées sur les traités internationaux. Les tensions entre la notion subjective, sociale et politique du concept de sécurité vont se jouer sur chacun de ces trois niveaux.

Le sens global subjectif ou privé du «sentiment de sécurité» dans son environnement, le concept social «d'avoir protégé» ou de «protéger» ses moyens d'existence nécessaires, et la disposition politique de la sécurité publique ne peuvent être dissociés. Le fait même de cet enchevêtrement peut, en particulier au vu des expériences récentes, rendre une approche plus importante que les autres, mais elles doivent être continuellement corrélées et équilibrées les unes avec les autres.

3.2. Préoccupations, considérations et concepts éthiques

3.2.1. Sécurité, surveillance, peur et contrôle

«Peut-être encouragés par les avancées technologiques, le progrès scientifique, les percées miraculeuses dans le domaine de la médecine, ou par une diminution constante de la criminalité, nous serions tellement empreints de rêves d'invulnérabilité ou d'éventuelle immortalité que nous renierions notre nature humaine. La préoccupation obsessionnelle de la sécurité pourrait être perçue comme une tentative de nous détourner d'un aveu terrifiant ou de notre mortalité, un geste apotropaïque destiné à parer ce qui ne pourra jamais être empêché, ou un vain espoir dans l'efficacité parfaite de nos calculs.

Dans son récent mémoire, *Insecure at last*, Eve Ensler associe désespérément la question de la sécurité à un désir de transgresser notre finitude humaine:

«Que sous-entend quelqu'un lorsqu'il parle de sécurité? Pourquoi sommes-nous soudainement une nation et un peuple qui luttent pour la sécurité par-dessus tout? En fait, la sécurité est essentiellement insaisissable, impossible. Nous mourons tous. Nous tombons tous malades. Nous vieillissons tous.

Certains nous quittent. Certains nous surprennent. Certains nous changent. Rien n'est sûr. Et c'est une bonne nouvelle. Mais seulement si vous ne recherchez pas la sécurité comme un but ultime.» ⁽²⁶⁰⁾

Après les révélations du projet «Prism», nombreux sont ceux à avoir été choqués. Choqués par la perte du sentiment de confiance, de dignité et de respect. Choqués parce que les droits de l'homme fondamentaux sont en jeu. Les révélations relatives à la surveillance des chefs d'État de l'UE soulignent d'autant plus l'existence d'une crise éthique sérieuse susceptible d'avoir de graves conséquences politiques. Elles soulignent en outre l'importance pour l'UE de préciser clairement sa position éthique. De sérieuses préoccupations ont été formulées à propos de la surveillance des fonctionnaires européens, comme en témoigne cette déclaration de la commission des affaires étrangères du Parlement européen:

«L'Union européenne et les États-Unis d'Amérique sont des partenaires stratégiques, et ce partenariat est essentiel pour promouvoir nos valeurs communes, notre sécurité et notre leadership commun sur la scène internationale. Or, la confiance dans ce partenariat a été ébranlée et il convient de la rétablir. L'Union européenne, ses États membres et ses citoyens ont exprimé une profonde inquiétude à la suite des révélations sur les programmes américains de collecte de renseignements à grande échelle, notamment en ce qui concerne la protection des données à caractère personnel. Une surveillance généralisée des communications privées, que ce soit de citoyens, d'entreprises ou de dirigeants politiques, est inacceptable ⁽²⁶¹⁾.

Les fonctionnaires européens ont également émis des doutes quant à l'opportunité de poursuivre l'accord actuel *relatif à la sphère de sécurité* pour le transfert de renseignements personnels vers les États-Unis, en vertu duquel les entreprises sont tenues de se conformer aux lois européennes plus strictes en matière de protection

de la vie privée ⁽²⁶²⁾. Bien que les incidences précises sur ces négociations futures ne soient pas claires, de telles déclarations montrent le lien entre les décisions de collecte de renseignements et les négociations commerciales internationales.

Ces révélations et le débat qui les a suivies ont fait prendre conscience à la population que la surveillance imprégnait visiblement toutes les sphères de la vie, de l'espace public, de l'environnement de travail, et même de la vie privée, non seulement des chefs d'État, mais aussi des citoyens ordinaires. Nos relations avec nos voisins, nos amis, nos alliés, nos concitoyens, nos employeurs et nos prestataires de services et nos gouvernements sont en jeu. Des portiques de détection dans les aéroports, des GPS dans les téléphones mobiles pour tracer les déplacements des personnes, des caméras pour surveiller le public dans les centres commerciaux, les musées et les rues, des employeurs qui installent des dispositifs d'enregistrement des saisies clavier, des lunettes Google qui envoient des images sur un ordinateur, la collecte des données sur l'utilisation des cartes de crédit, des cartes de fidélité ou des habitudes d'achat en ligne, des recherches sur les navigateurs, et l'élaboration d'algorithmes visant à analyser ces données, la collecte des empreintes digitales, etc. Les individus sont contrôlés, suivis et évalués. Les technologies modernes permettent à un individu qui suspecte son partenaire de le tromper d'installer des applications pour recueillir des informations à partir de données en masse. Pourquoi les personnes, les entreprises et les gouvernements sont-ils intéressés par ce que font les individus? La raison la plus souvent invoquée est la sécurité et pour pouvoir assurer la sécurité il est nécessaire d'exercer une certaine influence, voire un certain contrôle. Cela modifie fondamentalement le tissu social des sociétés et des alliances. Pour reprendre les mots du professeur canadien de sociologie David Lyon ⁽²⁶³⁾:

«Les processus et les pratiques de surveillance actuelles témoignent d'un monde dans lequel on ne se fait pas vraiment confiance. La surveillance favorise la suspicion et donc menace la cohésion sociale et la solidarité (...) il peut parfois s'agir, me direz-vous, d'une simple mesure de prudence. Mais où cela s'arrêtera-t-il? Les rapports sociaux dépendent de la confiance et nous autoriser à la saper de cette façon ressemble à un lent suicide social.»

⁽²⁶⁰⁾ John T. Hamilton, *Security, Politics, Humanity and the Philosophy of Care*, Princeton UP, 2013, p. 28.

⁽²⁶¹⁾ Commission européenne, Communication de la Commission au Parlement européen et au Conseil. Rétablir la confiance dans les flux de données entre l'Union européenne et les États-Unis d'Amérique, 27 novembre 2013 et http://export.gov/safeharbor/eu/eg_main_018476.asp

⁽²⁶²⁾ Il existe, naturellement, des points de vue différents entre et au sein de ces institutions à cet égard.

⁽²⁶³⁾ D. Lyon, *Surveillance Society*, 2008.

CHAPITRE III. | ANALYSE ÉTHIQUE

Le simulacre de sécurité dans les aéroports

Plus de 1,4 milliard de passagers transitent par les aéroports européens chaque année. Selon les estimations, ce chiffre devrait atteindre 2,7 milliards d'ici 2030 ⁽²⁶⁴⁾. Depuis les événements de septembre 2001, les passagers sont de plus en plus habitués à ne pouvoir transporter que des flacons de liquide de 100 ml maximum dans leur bagage à main, à devoir retirer leurs chaussures, à passer à travers de nouveaux types de scanners corporels et voir leurs mains et leurs bagages contrôlés pour y déceler des traces d'explosifs. Chacune de ces mesures de sécurité a été introduite à la suite d'une menace de sécurité spécifique dans un aéroport. La Commission européenne a présenté la limitation du volume de liquides et de gels pouvant être transporté dans les bagages à main en 2006, après l'échec de la tentative des «liquid bombers» de faire sauter plusieurs avions à l'aéroport d'Heathrow.

La nature réactive de ces mesures, les coûts importants occasionnés par leur introduction et les inconvénients vécus par les passagers ont fait l'objet de nombreuses critiques. Bruce Schneier et d'autres ont fait valoir que plusieurs des mesures de sécurité introduites dans les aéroports à la suite des attentats du 11 septembre n'étaient qu'un «simulacre de sécurité» ⁽²⁶⁵⁾. Le public, choqué et effrayé par les événements, aspirait à de nouvelles mesures pour rétablir son sentiment de sécurité dans l'exercice de ses activités quotidiennes. Les politiciens devaient donc avoir l'air de prendre des mesures à cet égard, indépendamment de la question de savoir si l'action spécifique permettrait effectivement d'améliorer la sécurité de la population.

Il est peu probable que les mesures réactives adoptées permettent de prévenir de futures attaques. Comme l'ont souligné les commentateurs, les terroristes n'auront tout simplement qu'à trouver d'autres moyens ou d'autres lieux où perpétrer leurs actes. En outre, plusieurs exemples réussis de violation de la sécurité aéroportuaire ont été signalés par un certain nombre de journalistes désireux de démontrer qu'un peu d'ingéniosité suffit pour contourner les contrôles de sécurité ⁽²⁶⁶⁾. L'internet regorge d'exemples sur la façon dont les mesures de sécurité peuvent être déjouées.

C'est l'efficacité des mesures de sécurité plutôt que l'évitement de la peur qui doit permettre de gagner la confiance du public. La confiance est cruciale dans presque tous les types de situations dans lesquelles une insécurité existe ou des résultats indésirables sont possibles ⁽²⁶⁷⁾. Comme l'a souligné la baronne Onora O'Neil lors des conférences Reith 2012 sur la confiance ⁽²⁶⁸⁾, «*Confucius explique à son disciple Tzu-kung que trois choses sont nécessaires pour le gouvernement: des armes, de la nourriture et de la confiance. Si un dirigeant est incapable de les rassembler tous les trois, il choisit en premier lieu d'abandonner les armes, ensuite la nourriture. La confiance doit être protégée jusqu'au bout: sans confiance, il est impossible de tenir*».

Bien avant que l'autorité fédérale de l'aviation (Federal Aviation authority FAA) ne lève l'interdiction de l'utilisation des téléphones intelligents, des ordinateurs et des liseuses numériques pendant les phases de décollage et d'atterrissage, les passagers ignoraient cette interdiction doutant de la fiabilité de l'information faisant état de la dangerosité de la pratique. Nick Bilton, dans une série d'articles publiés dans le New York Times, a contesté les régulateurs de cette interdiction en s'appuyant sur des arguments scientifiques ⁽²⁶⁹⁾. Aucun incident en la matière n'a pu être démontré et la FAA a levé l'interdiction en novembre 2013.

Si les gens se voient obligés ou empêchés de faire quelque chose au motif de la sécurité publique, des données scientifiques solides doivent soutenir l'argument, sinon la confiance est ébranlée et les interventions légitimes fondées sur des preuves risquent d'être contournées par un public sceptique.

⁽²⁶⁴⁾ <https://www.aci-europe.org/policy/fast-facts.html> consulté le 9 février 2014.

⁽²⁶⁵⁾ <https://www.schneier.com/essay-292.html> consulté le 9 février 2014.

⁽²⁶⁶⁾ <http://www.theatlantic.com/magazine/archive/2008/11/the-things-he-carried/307057/3/>
<http://www.vanityfair.com/culture/features/2011/12/tsa-insanity-201112> consulté le 10 février 2014.

⁽²⁶⁷⁾ Fukuyama F. 1995. *Trust: the social virtues and the creation of prosperity*. The Free Press, New York.

⁽²⁶⁸⁾ <http://www.bbc.co.uk/radio4/reith2002/lecture1.shtml> consulté le 9 février 2014.

⁽²⁶⁹⁾ <http://bits.blogs.nytimes.com/2011/11/27/disruptions-fliers-must-turn-off-devices-but-its-not-clear-why/> consulté le 9 février 2014.

3.2.2. Contrôle, sécurité, protection

Des scénarios fictionnels dystopiques, tels que le 1984 de George Orwell, avec la crainte orwellienne d'être punis pour des «crimes de pensée», des écrits politiques comme le *Panoptique* de Jeremy Bentham et le débat actuel sur la sécurité se penchent sur le contrôle, les connaissances nécessaires pour assurer le contrôle, le sens d'une vie en étant surveillé en permanence, ainsi que des limites techniques et morales du contrôle. Qu'apporte-t-il aux individus? Ne s'épanouissent-ils pas en étant libres, libres de poursuivre leurs objectifs? Ne s'épanouissent-ils pas en faisant confiance aux gens? Le contraire du contrôle est la confiance. Si l'on fait confiance à ses concitoyens ou à ses employés, la surveillance n'est pas nécessaire et ne doit pas les viser. Être surveillé par une personne ou une entité en qui l'on a confiance est éthiquement beaucoup plus pénible, dans la mesure où l'on est surveillé par une personne ou une entité avec qui l'on croyait partager une relation fondée sur la confiance.

Le comité d'examen du président des États-Unis sur les techniques de renseignement et de communication, dont le rapport intitulé *«La liberté et la sécurité dans un monde en mutation»* a été publié en décembre 2013, commente les mesures visant à accroître la surveillance à la suite des événements dramatiques du 11 septembre:

«La nature humaine étant ce qu'elle est, il y a inévitablement un risque de réaction exagérée lorsque nous

agissons par peur. Dans ces moments-là, ceux qui ont la responsabilité de préserver la sécurité de notre nation, soutenus par une opinion publique inquiète, ont trop souvent été au-delà des programmes et des politiques qui étaient en fait nécessaires et appropriés pour protéger la nation et ont pris des mesures qui ont inutilement et parfois dangereusement mis la liberté individuelle en péril.» ⁽²⁷⁰⁾

Le principal argument mis en avant pour justifier les différentes mesures de surveillance concerne la sécurité des citoyens: «Des terroristes et des criminels attaquent des innocents et la surveillance est nécessaire pour les empêcher de nuire aux personnes qui ont besoin de protection. Il ne s'agit pas de contrôle, mais de protection» — c'est ce que prétend l'argument. L'objectif de la surveillance est d'atteindre l'objectif de la sécurité dans la guerre contre la terreur et le crime. Mais veiller et surveiller sont deux choses bien différentes.

La sécurité, le contrôle et la liberté sont des concepts aussi vieux que les sociétés humaines qui ont, depuis des temps immémoriaux, essayé de maintenir le «troupeau» dans son «enclos» pour sa propre protection, celle de la société tout entière et celles des «autres», dehors. La nécessité d'un contrôle peut également être alimentée par la peur, la panique et la méfiance. Le contrôle est lié au pouvoir et à la façon dont ceux qui surveillent influencent le comportement des surveillés. Comme décrit dans le chapitre 1, les technologies fonctionnent dans un monde globalisé, pas dans une société unique. Il existe une interdépendance des technologies et des questions éthiques qui influencent le débat.

⁽²⁷⁰⁾ Comité d'examen du président sur les techniques de renseignement et de communication «Liberty and Security in a Changing World», 2013, p. 53.

CHAPITRE III. | ANALYSE ÉTHIQUE

Lunettes Google Glass

Les évolutions techniques, comme celles des téléphones intelligents, des systèmes de navigation embarqués et des ordinateurs portables, ont accru la capacité des individus à cheminer efficacement sur le sentier de la vie, à la fois en ligne et hors ligne. Une part importante des habitants des 28 États membres de l'UE utilisent régulièrement ces technologies et leur utilisation continue de croître à mesure qu'elles s'intègrent dans la vie quotidienne. L'une des évolutions les plus récentes est la création de «dispositifs informatiques vestimentaires», comme le projet «Google Glass» (remarquez l'utilisation du singulier). Cette technologie développée par le laboratoire Google[X] Lab, un complexe entouré d'un grand secret qui se concentre sur le développement de produits de consommation futuristes tels que des ascenseurs spatiaux et des voitures sans chauffeur. Bien que certaines de ces technologies soient loin d'être abouties, les lunettes Google Glass devraient être commercialisées avant la fin de l'année 2014 ⁽²⁷¹⁾.

Les lunettes Google Glass sont, fondamentalement, un ordinateur intégré dans la monture d'une paire de lunettes qui reprend les principales fonctions d'un téléphone, d'un ordinateur portable et d'une tablette et qui les place dans la vision périphérique d'un individu. L'affichage de 1,3 cm (un demi-pouce) permet à l'utilisateur de prendre et de partager des photos et des vidéos, de faire du chat vidéo, de traduire, de surfer sur le web et de recevoir des informations en temps réel sur son environnement grâce à une commande vocale. Ce type de lunettes a longtemps nourri l'imaginaire de Hollywood, du «lieutenant commandeur Geordi La Forge» dans Star trek à «Cyclope» dans X-men. Les héros d'action portent des ordinateurs vestimentaires sous la forme d'un casque de réalité virtuelle. Selon Google, les lunettes offrent un aperçu de l'avenir: elles visent à changer l'idée qu'ont les gens des logiciels et la façon dont ils peuvent les intégrer dans leur vie quotidienne. Leur but ultime est de servir de cerveau augmenté.

Les avantages des lunettes Google Glass paraissent évidents: l'affichage de données directement au-dessus du champ de vision d'un utilisateur permet de plus facilement naviguer, prendre des photos, répondre à des messages ou traduire une phrase. Leur potentiel est plus grand encore: imaginer une situation dans laquelle le témoin d'un accident peut aider une victime avant qu'une assistance professionnelle n'arrive sur les lieux grâce à l'affichage sur ses lunettes des techniques de premiers secours et à un contact vidéo direct avec les services d'urgence. Pourtant, le projet est controversé. Outre les fonctions mentionnées ci-dessus qui permettent une utilisation mains libres d'applications technologiques déjà courantes, Google et d'autres développeurs de logiciels sont en train de développer des applications qui permettent à l'utilisateur de scanner une foule pour y trouver ses amis, même si ces amis n'ont pas l'intention d'être trouvés. Certaines personnes soutiennent qu'il n'y a là rien de bien nouveau à une époque où presque tout le monde utilise son téléphone ou sa tablette pour enregistrer et télécharger les différents épisodes de leur vie. Mais il y a une nette différence entre prendre une photo avec des lunettes Google Glass et tout autre dispositif technique: les lunettes ne sont pas dotées d'une grande capacité de stockage. Par défaut, les lunettes téléchargent automatiquement les données vers des serveurs dans les nuages, où Google peut les regrouper et les analyser. Fondamentalement, cela signifie que les données recueillies ne sont pas contrôlées ou détenues par des personnes qui portent les lunettes Google Glass. Google gère les données et pourrait éventuellement les utiliser pour que de la publicité personnalisée s'affiche sur l'écran des lunettes sur la base sur ce que l'utilisateur voit dans son environnement réel, la publicité étant la principale source de revenus de la société. Bien que la surveillance des citoyens par l'État soit devenue une composante normale de la vie moderne, un débat doit être ouvert quant à l'opportunité d'autoriser des sociétés privées à exercer une surveillance. Surtout lorsque l'on pense que les lunettes Google Glass, une fois piratées, pourraient donner à des étrangers l'accès à la plupart de vos informations personnelles. En effet, ce que voit l'utilisateur, le pirate le voit également.

Une autre question est celle du consentement. On peut estimer que les personnes qui utilisent les lunettes Google Glass ont donné leur consentement implicite à Google pour l'utilisation de leurs données. Ils sont prêts à renoncer à certains aspects de leur vie privée pour bénéficier des avantages de cette technologie. Mais si le porteur des

⁽²⁷¹⁾ Sources:

<http://www.google.com/glass/start/> (site web des google glass)

<http://www.techradar.com/news/video/google-glass-what-you-need-to-know-1078114>

<http://www.bbc.co.uk/news/technology-22538854>

<http://www.guardian.co.uk/technology/us-news-blog/2013/may/17/congress-caucus-google-glass-privacy>

<http://www.guardian.co.uk/technology/2013/mar/06/google-glass-threat-to-our-privacy>

lunettes Google Glass a consenti à être en permanence branché au monde numérique de Google, ce n'est pas le cas des personnes saisies ou enregistrées par inadvertance. Ainsi, même si l'utilisateur des lunettes Google Glass a pris une décision en connaissance de cause concernant la conservation et le traitement de ses données, il ne peut donner son consentement pour l'utilisation de données d'autres personnes dont il a collecté des photos, involontairement ou à dessein. Ce que cet exemple sert à illustrer, c'est que les nouvelles technologies telles que les lunettes Google Glass peuvent avoir de lourdes conséquences pour la vie privée des utilisateurs et de ceux qui les entourent.

CHAPITRE III. | ANALYSE ÉTHIQUE

3.2.3. Public et privé

Le débat ne porte pas uniquement sur le contrôle et la protection de l'État et des gouvernements. Des intérêts commerciaux considérables sont également en jeu. Les données en masse permettent de traiter d'énormes quantités de données à caractère personnel, de les lier à d'autres domaines et de les analyser pour produire de nouvelles interférences et conclusions. Le Forum économique mondial qualifie les données à caractère personnel de «nouveau pétrole». Il ne s'agit pas du premier groupe à faire une référence explicite à la pertinence économique des données personnelles et à la dépendance de plus en plus importante de la société à l'égard des données comme outil de croissance économique. Il existe une tension évidente entre d'une part les possibilités économiques offertes par l'augmentation du nombre de données disponibles sur les consommateurs potentiels et, d'autre part, la nécessité de protéger la vie privée. Les fournisseurs de services veulent cibler leurs utilisateurs avec de la publicité et utilisent pour ce faire les connaissances qu'ils recueillent grâce à la surveillance.

La distinction traditionnelle entre la surveillance publique et privée est complexe comme le souligne le professeur de droit de l'université de Harvard: «*Les surveillances gouvernementales et non gouvernementales se soutiennent l'une l'autre de façon complexe et souvent inextricable. Au début, les technologies de surveillance — les logiciels, les puces RFID, les traqueurs GPS, les caméras et d'autres capteurs bon marché — sont utilisées indifféremment par des observateurs gouvernementaux et non gouvernementaux. L'industrie privée vend également de nouvelles technologies de surveillance à l'État.*»⁽²⁷²⁾

Fait intéressant à noter, les fournisseurs commerciaux (Apple, Google, Microsoft) ont récemment écrit aux autorités américaines pour demander de modifier l'accès du gouvernement à leurs données.

«Nous comprenons que les gouvernements ont le devoir de protéger leurs citoyens. Mais les révélations de cet été ont mis en évidence le besoin urgent de réformer les pratiques gouvernementales de surveillance dans le monde. L'équilibre dans de nombreux pays penche beaucoup trop en faveur de l'État, loin des droits de la personne, des droits consacrés dans notre

Constitution. Cela sape les libertés que nous chérissons tous. Il est temps de changer.»⁽²⁷³⁾

3.3. Principes éthiques

L'Union européenne est une communauté de valeurs. Ces valeurs sont intégrées dans la *Convention européenne des Droits de l'homme (CEDH)*, le premier traité juridique international visant à protéger les droits de l'homme à l'aide de mécanismes exécutoires. L'extension de la CEDH, la *charte des droits fondamentaux de l'Union européenne*, qui a été adoptée en 2000 et est entrée en vigueur en 2009, s'articule autour des principes de dignité humaine, de libertés fondamentales, d'égalité, des droits des citoyens et de justice.

Le principe de dignité est sous-jacent à la Convention et à la charte. La *dignité* est au cœur de l'éthique et est également d'une importance cruciale en ce qui concerne le débat sur la sécurité et la surveillance. Il existe un lien étroit entre le principe de dignité et les principes que le Groupe met en avant dans ce chapitre. Les principes éthiques de base qui sous-tendent les recommandations du GEE sur la sécurité et la surveillance sont les suivants:

- La vie privée et la liberté
- L'autonomie et la responsabilité
- Le bien-être et/ou l'épanouissement personnel
- La justice

Outre ces principes de base, il convient d'ajouter deux principes de procédure destinés à générer de la confiance entre les individus, les entreprises et l'État et/ou les États:

- La transparence
- L'efficacité et la proportionnalité

Ces principes contribuent en réalité à la fois à assurer la sécurité et à fixer des limites pour les instruments de sécurité et de surveillance. Sur la base de ces principes, le règlement et la pratique de la protection des droits de l'homme dans le domaine de la sécurité sont décrits et certaines remarques sur la responsabilité sont formulées.

⁽²⁷²⁾ N.M. Richards, the dangers of surveillance — Information Society Project — <http://www.yaleisp.org/sites/default/files/Richards.pdf>

⁽²⁷³⁾ Voir: <https://www.reformgovernmentsurveillance.com> pour plus d'informations sur la lettre ouverte au gouvernement des États-Unis pour une «Réforme globale de la surveillance gouvernementale».

Dignité, respect de la vie privée, liberté et épanouissement personnel

Dignité humaine

La dignité humaine est une valeur universelle. Il existe différentes interprétations philosophiques du concept de dignité humaine dans le débat éthique pluraliste, mais il est universellement reconnu dans les droits de l'homme que la dignité humaine exprime la valeur intrinsèque et l'égalité fondamentale de tous les êtres humains. Cela se reflète dans l'article premier de la charte des droits fondamentaux de l'Union européenne, qui dispose que «la dignité humaine est inviolable. Elle doit être respectée et protégée».

La dignité — appliquée dans le contexte de la sécurité — requiert la protection et le respect de l'intégrité physique et psychologique, l'assurance de la sécurité en tant que condition permettant de poursuivre ses objectifs, et l'intégrité psychologique pour garantir le droit à l'autonomie.

Protection de la vie privée

La vie privée est une notion centrale dans le débat éthique sur la surveillance et la sécurité. Elle est étroitement liée à la protection de la dignité. Les êtres humains ont besoin de leur propre espace, au sens propre comme au sens figuré, pour donner leur pleine mesure et s'épanouir en tant qu'êtres humains. La dignité signifie respecter la nécessité de disposer de son propre espace, de ses propres secrets. Priver une personne de sa vie privée revient à le dépouiller de sa dignité.

Le droit à la vie privée est décrit à l'article 8 de la CEDH:

«Article 8 — Droit au respect de la vie privée et familiale

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

La vie privée provient étymologiquement du latin *privatus*, participe passé de *privo*; «Je prive», «J'ampute». La vie privée se réfère donc au fait d'être séparé, isolé des autres, contrairement au fait d'être public ou commun. Une idée sous-jacente est le droit d'être laissé seul. C'est évidemment une notion importante, mais ce n'est pas de cela qu'il s'agit aujourd'hui. La vie privée a également été conçue comme un «dispositif d'exclusion — un outil permettant de repousser les regards indésirables» ⁽²⁷⁴⁾. Selon *l'Encyclopédie de la vie privée*, elle décrit et impose des «limites sur l'appropriation de l'isolement paisible, des informations personnelles, des choix intimes et des identités d'autrui». Bien que le terme «vie privée» n'existe pas dans toutes les langues, l'expérience de la protection de la vie privée est une «culture universelle», «une part essentielle de l'épanouissement et du bien-être» ⁽²⁷⁵⁾.

La vie privée signifie le droit de protéger les actions et les pensées que les personnes souhaitent garder pour elles-mêmes. Elle est étroitement liée à l'intimité. Observer des personnes dans des situations considérées comme intimes et personnelles, comme dans le cas de caméras enregistrant les activités sexuelles d'une personne ou d'autres comportements intimes, peut être humiliant et dégradant. Les différentes formes de protection de la vie privée et les définitions de l'intimité sont au cœur d'un vaste débat philosophique. Les chercheurs font la distinction entre l'intimité physique (liée à la protection physique), psychologique (liée à l'autonomie personnelle), économique (liée à la propriété), informationnelle (liée à la protection des renseignements personnels) et décisionnelle (liée au pouvoir décisionnel) ⁽²⁷⁶⁾.

Dans le cadre de cet avis, tous ces domaines sont pertinents, par exemple les caméras de vidéosurveillance interfèrent avec l'intimité physique, l'exploration de données porte atteinte à l'intimité *informationnelle*, les technologies de contrôle aux frontières peuvent avoir une incidence sur l'intimité physique et psychologique, et les écoutes téléphoniques ou les enregistrements de courriels touchent l'intimité psychologique et informationnelle.

⁽²⁷⁴⁾ Mireille Hildebrandt, Antoinette Rouvroy (2011) «Law, Human Agency and Autonomic Computing: The Philosophy of Law Meets the Philosophy of Technology», Routledge, 26 août 2011, p. 187.

⁽²⁷⁵⁾ Adam D. Moore (1965) «Privacy Rights: Moral and Legal Foundations» Pennsylvania State University Press, ISBN 978-0-271-03685-4, p. 56.

⁽²⁷⁶⁾ Rapport sur les défis de l'UE.

CHAPITRE III. | ANALYSE ÉTHIQUE

La vie privée a évolué au fil du temps en prenant la forme d'un droit de plus en plus orienté vers la libre construction de la personnalité: la construction autonome de l'identité et la projection des principes démocratiques fondamentaux dans la sphère privée.

La vie privée dans la société moderne

Il n'y a pas d'accord sur le rôle et la signification de la vie privée dans la société moderne. Certains soutiennent une théorie extrême:

«La vie privée n'est plus, il faut l'accepter». Elles mettent en avant l'argument selon lequel la protection de la vie privée est un moyen de contrôler les informations qui devraient généralement être partagées puisqu'il n'est pas possible de la protéger correctement dans l'environnement numérique du web. Ce point de vue, appelé le «mouvement post-vie privée», défend également le fait qu'abandonner activement la vie privée permettrait de déterminer l'épanouissement d'une vertu personnelle et sociale fondée sur la liberté des individus de présenter et de partager les données personnelles qu'ils souhaitent. Toujours selon ce point de vue, une telle approche devrait encourager les gens à cultiver une plus grande tolérance vis-à-vis des attitudes et des comportements d'autrui ⁽²⁷⁷⁾.

Pour le point de vue opposé, l'hypothèse selon laquelle à l'époque actuelle il est difficile de garantir la vie privée n'est pas une raison convaincante pour abandonner la protection nécessaire de la vie privée des individus. La sphère privée est perçue comme un espace où il n'est pas nécessaire de répondre immédiatement aux attentes du public et modes de vie traditionnels ⁽²⁷⁸⁾.

La tendance générale est que la vie privée semble bel et bien vivace. Des changements peuvent cependant intervenir sur ce que l'on souhaite garder privé. «La plupart des gens sont instrumentalisés pour fournir des données personnelles pour acheter en ligne ou utiliser les sites de réseaux sociaux. Mais ils sont tout aussi inquiets de la façon dont ces données seront utilisées

et n'ont pas toujours le sentiment de contrôler les choses.» ⁽²⁷⁹⁾

Rien à cacher?

Un argument souvent mis en avant dans le débat sur la surveillance et la protection de la vie privée est que ceux qui n'ont rien à cacher n'ont rien à craindre. Leur vie privée ne sera pas exposée, ou ils n'ont tout simplement pas à s'inquiéter des mesures intrusives, seuls ceux qui ont quelque chose à cacher risquent de voir leur vie privée menacée. Bien que très populaire, il ne s'agit pas d'un argument convaincant. Chacun a quelque chose à cacher, dans le sens où certaines pensées, images et actes relèvent de l'intime et du privé. Ne faisant rien de mal et n'ayant aucune mauvaise intention ou pensée criminelle, nous n'avons peut-être rien à cacher. Mais certains secrets peuvent être précieux et l'envahissement de certaines technologies et l'exposition qui s'en suit peuvent s'avérer gênants ou humiliants, par exemple parce qu'il s'agit d'un sujet sensible ou que l'on se sent traité comme un criminel. Certaines pensées et certains actes ne sont l'affaire de personne. L'idée de n'avoir «rien à cacher» peut conduire à une certaine naïveté dans la façon dont les gens gèrent eux-mêmes leurs propres données. Certaines personnes peuvent être disposées à partager des données, ne réalisant pas que ce qu'elles pensent être des informations inoffensives contribuent à un système qui n'est plus sans danger.

Consentement

N'est-il cependant pas possible de renoncer à ses droits à la vie privée en consentant à être surveillé, filmé, par exemple dans les programmes de télévision? Le consentement peut-il servir de justification pour limiter la vie privée? Il n'y a pas de réponse simple à cette question. Parfois, un accord signifie qu'il n'y a en effet pas d'invasion de la vie privée, par exemple si l'on autorise une personne à lire ses courriels. Parfois, cependant, ce consentement peut être très fragile, lorsque les gens donnent leur accord de manière superficielle ou naïve. Le fait de cocher une case pour avoir accès à un site web ou à un service en est un bel exemple.

⁽²⁷⁷⁾ Voir, par exemple, http://events.ccc.de/congress/2008/Fahrplan/attachments/1222_postprivacy.pdf intitulé «Embracing Post-Privacy: Optimism for a future where there is nothing to hide»

⁽²⁷⁸⁾ Voir, par exemple, l'Eurobaromètre spécial 359: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf et http://europa.eu/rapid/press-release_IP-11-742_en.htm?locale=en

⁽²⁷⁹⁾ La commissaire Reding citée dans http://europa.eu/rapid/press-release_IP-11-742_en.htm?locale=en

Parfois, les circonstances sont telles que l'on n'a pas vraiment d'autre choix que de donner son «consentement» sous peine d'être privé des moyens de participer à la vie moderne ⁽²⁸⁰⁾.

Face aux données en masse, à la surveillance en masse, à la localisation mondiale, à la vidéosurveillance et à d'autres méthodes de contrôle, les individus peuvent se sentir insignifiants et impuissants. Ils peuvent donc accepter toutes sortes de mesures et les respecter, non pas parce qu'ils ont réellement donné leur accord et donc leur consentement, mais parce qu'ils ont été amenés à croire que c'était ce qu'il fallait faire, parce qu'ils n'ont aucune idée de ce que cela implique, ou parce qu'ils ne peuvent de toute façon rien y faire. On peut avoir l'impression, en tant qu'individu, de n'avoir peu ou rien à dire sur la question de la surveillance. C'est l'une des nombreuses décisions prises par les gouvernements et les acteurs commerciaux que les individus ne peuvent qu'accepter et respecter. Si l'on veut voyager par avion, il faut passer la sécurité. Vous faites des courses: vous êtes filmés et enregistrés sur des caméras de surveillance. Vous voulez profiter de votre carte client: vos habitudes alimentaires n'auront plus de secret pour votre supermarché. Vous avez un téléphone mobile: vous pouvez être tracés. Vous surfez sur l'internet: les sites que vous visitez seront connus de votre fournisseur.

Le débat qui a fait suite aux révélations du programme PRISM a provoqué un sursaut qui peut avoir modifié le comportement complaisant de certains, ainsi que leurs vues sur la vie privée.

⁽²⁸⁰⁾ «Dans la société moderne, les individus, pour des raisons pratiques, utilisent des cartes de crédit, le courrier électronique, le téléphone, l'internet, les services médicaux, et le reste. Leur décision de révéler des informations personnelles à des tierces parties ne traduit pas un manque d'intérêt pour la confidentialité des informations, mais une adaptation nécessaire aux réalités de la vie moderne. Ce qu'ils veulent — et attendent raisonnablement — c'est à la fois la possibilité d'utiliser ces services et le droit de préserver leur vie privée lorsqu'ils les utilisent. S'agissant là d'une politique publique judicieuse dans une société libre, il n'y a aucune raison pour qu'il en aille autrement.»

Comité d'examen du président sur les techniques de renseignement et de communication (2013) Rapport de la NSA intitulé «Liberty and Security in a Changing World». Princeton University Press ISBN 978-0-691-16320-8 et http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

Autonomie, vie privée intellectuelle et responsabilités individuelles

L'autonomie et la liberté sont des principes éthiques centraux dans le débat entourant la sécurité et la surveillance. Une fois encore, ces cas sont étroitement liés à la protection de la vie privée en ce sens qu'une absence de vie privée restreint la liberté et que la liberté de ne pas être surveillé fait partie de la notion de vie privée. L'idée importante est que les individus devraient être libres de penser ce qu'ils veulent, d'exprimer leurs vues, de se déplacer et d'interagir avec qui ils le souhaitent.

Le juriste susmentionné Neill Richards insiste sur la notion de vie privée intellectuelle. Si les gens sont continuellement surveillés et contrôlés, ils se comporteront différemment, ils vont s'adapter pour offrir l'image que l'on attend d'eux et peuvent hésiter à utiliser leur capacité à imaginer de nouvelles idées, dans la mesure où se comporter différemment peut avoir de lourdes conséquences (être considéré comme un paria, se retrouver en prison ou réduit au silence). La surveillance peut être dommageable, *«parce qu'elle peut geler l'exercice des libertés civiles et qu'elle donne au surveillant un pouvoir sur le surveillé (...) Une telle surveillance intellectuelle est particulièrement dangereuse, car elle peut dissuader les individus à expérimenter des idées nouvelles, controversées ou déviantes. Afin de protéger notre liberté intellectuelle de penser sans contrôle ou interférence de l'État, nous avons besoin de... "vie privée intellectuelle"»*. Un argument semblable est avancé par J. Cohen, professeur au Georgetown Law Centre, *«Les environnements qui dissuadent l'indépendance d'esprit et découragent l'expérimentation et la variation de comportement sources d'innovation finiront, avec le temps, par décourager naturellement et systématiquement l'innovation, et les environnements conçus pour favoriser les choix consuméristes et la quête de profit finiront par décourager systématiquement les innovations pour promouvoir d'autres valeurs. La société modulée se consacre à la prédiction, mais pas nécessairement à la compréhension ou à la promotion du bien-être matériel, intellectuel et politique»* ⁽²⁸¹⁾. L'autonomie et la liberté sont de la plus haute importance dans ce débat, car les technologies de surveillance peuvent menacer ces principes.

L'autonomie implique une certaine forme de responsabilité de la part de l'individu. Les citoyens ont la responsabilité d'être conscients, vigilants, critiques et informés,

⁽²⁸¹⁾ J. E. Cohen «What Privacy is For» Harvard Law Review, Vol. 126, n° 7 voir: <http://www.slaw.ca/2013/01/31/thursday-thinkpiece-cohen-on-privacy/>

CHAPITRE III. | ANALYSE ÉTHIQUE

par exemple lorsqu'ils signent une renonciation à la protection de leur vie privée. Ils doivent être conscients des conséquences du partage des données (des leurs ou de celles d'autrui), ils doivent réfléchir à ce qu'ils considèrent être privé et à l'espace qu'ils souhaitent préserver de l'intrusion du gouvernement ou d'acteurs commerciaux, à ce qu'ils veulent conserver en toute sécurité et confidentialité, et à ce qu'ils sont prêts à divulguer. Pour prendre des décisions éclairées, les citoyens doivent disposer d'informations et pouvoir faire leur choix, leur véritable choix. Ils doivent donc bien sûr être informés par les gouvernements et les fournisseurs de services. En la matière, l'éducation relative aux aspects pratiques et moraux, tant sur le plan des connaissances que de la réflexion revêt une importance majeure et doit faire partie de tous les programmes de l'UE.

Il est également important que les citoyens prennent part au débat de société sur les limites de la sécurité et de la surveillance. Quels prix jugent-ils raisonnables quand il s'agit de sécurité, et où et quand la liberté et la vie privée prévalent-elles, même si cela doit se faire au détriment de la sécurité. Il s'agit de problèmes politiques fondamentaux qui ont besoin de la participation du public. Le comité d'examen du président des États-Unis sur les techniques de renseignement et de communication exprime ses préoccupations comme suit:

«L'inquiétude, c'est de voir des citoyens respectueux de la loi, une fois amenés à penser que leur comportement est observé trop étroitement par les organismes gouvernementaux (...) s'empêcher de participer au processus démocratique, s'empêcher de contribuer pleinement à la vie sociale et culturelle de leurs communautés, et même modifier leur comportement pour tant parfaitement privé et légal, de peur que des détails intimes de leur vie ne soit révélés et utilisés contre eux d'une manière ou d'une autre.» (282)

Justice, non-discrimination et suspects habituels

Le principe de justice est interprété de différentes façons dans différents contextes. Dans le contexte de cet avis, l'accent est mis sur la non-discrimination. Les technologies de surveillance et d'analyse des données sont fondées sur la distinction de certaines

caractéristiques ou de certains comportements considérés comme différents, «suspects» ou «mauvais». L'utilisation de certains mots dans un courriel ou une conversation téléphonique, porter un pull à capuche, et avoir une barbe sont stigmatisés à certains moments et à certains endroits. Cela conduit, et les preuves en ce sens abondent, à ce que l'on appelle le tri social: certaines personnes sont «triées», d'autres ne le sont pas. Les «suspects habituels» se distinguent des «innocents» du monde. Cela crée de graves problèmes de justice puisque des individus ou des groupes peuvent être stigmatisés, sur la base de simples préjugés ou de méthodes statistiques (trop) générales, voire défectueuses. Des innocents vont se trouver, probablement maintes et maintes fois, en position de suspect, car il est presque impossible de se défaire d'une telle stigmatisation. Il est véritablement pénible et douloureux de se retrouver dans la peau d'un «faux positif». Cette stigmatisation a de très graves conséquences sociales sur le plan des déplacements, de l'emploi et de la façon dont les gens sont traités dans la vie quotidienne. Elle peut gravement menacer la diversité. Les gens se conforment à certaines habitudes ou à certains codes, non pas parce qu'ils veulent sincèrement les adopter, mais parce qu'ils ne veulent pas être ciblés comme suspects. Elle a aussi des conséquences terribles pour la cohésion sociale et la notion même de citoyenneté. David Lyon dans son dialogue avec Zygmunt Bauman avertit *«si la perte de vie privée peut être la première chose qui nous vient à l'esprit lorsqu'il s'agit de surveillance, la vie privée n'est sans doute pas le problème le plus grave. Les questions de l'anonymat, de la confidentialité et de la vie privée ne doivent pas être ignorées, mais elles sont également liées à celles de l'équité et de la justice, des libertés civiles et des droits de l'homme. En effet, comme nous le verrons, la surveillance est aujourd'hui avant tout une question de tri social, pour le meilleur ou pour le pire. (...) la logique des statistiques et des logiciels qui dirigent la surveillance aujourd'hui produit des résultats qui sont étrangement cohérents. Non seulement, les "Arabes" et les "musulmans" estiment, non sans raison, faire l'objet bien plus que les autres de contrôles "aléatoires" dans les aéroports, mais, comme l'a démontré Oscar Gandy, le tri social réalisé par la surveillance des consommateurs contemporains construit un monde de désavantages cumulés» (283).* Il convient d'adopter une extrême prudence et des exigences élevées vis-à-vis des critères et des statistiques sur la base de laquelle les sélections sont réalisées.

(282) Comité d'examen du président des États-Unis sur les techniques de renseignement et de communication, 2013, p. 112.

(283) Zygmunt Bauman et David Lyon, *Liquid Surveillance*, Polity press 2013, 13-14 ISBN 9780745662824 et en livre numérique (9780745664026).

Transparence

La nécessité de transparence et son importance éthique ont été soulignées dans la dernière décennie, notamment par le GEE. Il s'agit d'un principe essentiel qui met l'accent sur l'importance de la transparence dans l'élaboration et la mise en œuvre de politiques. Que fait-on? Comment les décisions sont-elles prises? Qui fait quoi? La transparence permet d'assurer un contrôle démocratique.

Évidemment, lorsqu'il s'agit de mesures de surveillance, la traduction du principe de transparence en politique peut s'avérer compliquée. Il y a une différence entre, d'une part, la transparence sur la manière dont les décisions sont prises (par ex. la procédure permettant de surveiller certaines personnes suspectées d'activités criminelles) et les principes qui sous-tendent de telles décisions, et la transparence sur des mesures concrètes, comme la surveillance effective de personnes spécifiques, qui ne fonctionneront que si une certaine discrétion est assurée, étant donné que le fait d'être transparent défie l'objectif poursuivi. Bien entendu, l'argument du «besoin de discrétion» peut et a été utilisé de manière abusive, pour ne pas divulguer certaines mesures ou actions. La transparence n'est pas, comme elle le semble parfois, une panacée pour tout ce qui est politiquement complexe ou sensible.

Le GEE souligne la nécessité et l'importance de la transparence, mais formule également deux mises en garde. Être transparent ne suffit pas en soi à justifier la décision ou l'action en question. C'est une condition nécessaire pour permettre le débat sur la justification, pas une condition suffisante pour la justification. La transparence peut parfois conduire les gouvernements ou les fournisseurs de services à soutenir que les citoyens ont effectivement accepté la mesure x, alors que les citoyens estiment ne pas avoir d'autre choix que de subir les conséquences de cette mesure x. Si, par exemple, il existe une obligation d'annoncer l'utilisation d'un système de vidéosurveillance, c'est transparent, mais cela ne répond pas aux questions: l'utilisation de la vidéosurveillance dans ce contexte est-elle justifiée et ceux qui sont filmés estiment-ils avoir un quelconque choix en la matière? Le GEE est d'avis que des conditions matérielles et de procédure sont nécessaires.

Efficacité, proportionnalité et mise en équilibre

Le GEE souligne que, pour développer ou justifier une politique, il faut savoir si les mesures visant à assurer la sécurité permettent d'atteindre en réalité cet objectif

et dans quelle mesure. Des mesures de surveillance ont-elles été prises dans l'espoir qu'elles augmenteraient la sécurité, pour donner au public l'impression qu'il était en sécurité, ou simplement pour montrer que «des mesures étaient prises» alors que rien ne prouve qu'elles aient effectivement accru la sécurité ou que la sécurité était effectivement en jeu. Dans certains scénarios, l'introduction de technologies de sécurité et de systèmes de surveillance se fait en fonction des opportunités, en ne suscitant que peu de débats publics sur la valeur et la nécessité des mesures proposées. La justification des politiques et des mesures présuppose que la façon de définir l'efficacité de la surveillance et de mesurer cette efficacité est clairement établie.

En outre, toute limitation de la vie privée en vue d'accroître la sécurité peut générer de nouvelles formes d'insécurité. La création de banques de données centralisées pour faciliter l'application de la loi peut également exposer les données personnelles à de nouveaux risques liés à une mauvaise utilisation et au vol. Les technologies de fouilles corporelles (par ex. détecteurs de métaux, scanners corporels de dernière génération) qui en théorie devraient empêcher les attentats terroristes peuvent, dans la pratique, accroître le sentiment d'inquiétude dans la population et créer un faux sentiment de sécurité entraînant un relâchement des autres procédures de sécurité.

Si certaines mesures s'avèrent efficaces, alors la question de l'équilibre doit être posée: comment mettre en équilibre la sécurité et la vie privée, l'autonomie et la justice. Aucune formule arithmétique simple ne permet de trouver le bon équilibre. Le comité d'examen du président des États-Unis sur les techniques de renseignement et de communication explique que certains principes ne devraient souffrir d'aucune mise en équilibre:

«Dans une société libre, les fonctionnaires publics ne devraient jamais entreprendre une surveillance visant à punir leurs ennemis politiques, restreindre la liberté d'expression ou la religion, faire taire les critiques légitimes ou les voix dissidentes, favoriser certaines entreprises ou industries, accorder à des entreprises nationales un avantage concurrentiel inéquitable, ou avantager ou pénaliser les membres de certaines communautés religieuses, ethniques, raciales et sexuelles.»⁽²⁸⁴⁾

⁽²⁸⁴⁾ Comité d'examen du président des États-Unis sur les techniques de renseignement et de communication, 2013.

Chapitre IV. Sur la notion de compromis

Dans notre enquête sur l'éthique des technologies de sécurité et de surveillance, nous avons été confrontés à des façons récurrentes et courantes d'approcher, de conceptualiser et de traiter cette question. Cependant, la manière dont les questions éthiques sont formulées revêt une importance considérable, car cela va orienter les approches adoptées et déterminer les réponses possibles dans le cadre choisi, réponses qui pourraient être sensiblement différentes dans un autre cadre.

Comme nous le verrons ci-dessous, la façon la plus courante d'aborder la sécurité et la surveillance est la notion de *compromis* et, en particulier, le compromis entre deux objectifs, la sécurité et la liberté (avec la liberté exprimée, par exemple, sous la forme du droit à la vie privée). Selon certains, la sécurité et la surveillance sont considérées comme des obligations de l'État visant à protéger la vie et les libertés fondamentales de tous les citoyens, et cela, prétendent-ils, exige un certain degré de compromis entre le droit d'être protégé et celui de circuler et/ou agir librement dans une société donnée. Pour d'autres, les nouvelles technologies sont liées à la compétitivité, à l'emploi et à la croissance économique. Elles exigent donc de «renoncer» à certains droits à la liberté, à la fois au niveau du gouvernement, pour supprimer les obstacles qui freinent la réussite de certaines entreprises (qui dépendent de certaines utilisations de données en masse), et au niveau individuel, pour utiliser les possibilités offertes par ces entreprises, en particulier les services en ligne.

Ces approches guident, structurent et contraignent le raisonnement et les réponses politiques apportées aux technologies de sécurité et de surveillance, en les rassemblant autour d'un petit nombre d'options ou de pistes, qui ont une profonde influence sur nos sociétés.

Dans cet avis, une part importante de notre tâche consiste donc à examiner et à faire la lumière sur la «manière de penser actuelle» et sur les approches existantes, à les éclaircir et à dégager ainsi de nouvelles pistes de réflexion, une politique publique, et des actions individuelles et collectives. Notre objectif est de prendre du recul et de réfléchir à ce que montrent ces approches et à ce qu'elles délaissent ou essaient de masquer.

4.1. Équilibrer les droits

Avant de s'aventurer plus loin dans la présentation des types de compromis, il convient de lever ou d'éviter un malentendu important: la dignité de la personne

humaine est le principe fondamental du cadre moral européen et, en tant que tel, ne peut pas faire l'objet d'un «compromis». Bien qu'il y ait de nombreuses significations différentes associées à la notion de dignité humaine, et qu'aucune d'entre elles ne couvre toutes les dimensions, la dignité est intimement liée à la liberté et à la responsabilité. Car c'est précisément cet équilibre entre liberté et responsabilité qui est en jeu dans les interactions contractuelles entre, par exemple, un individu et des entreprises et dans les relations entre l'État et le citoyen.

Les droits que nous évoquons dans le contexte des technologies de sécurité et de surveillance, comme le droit à la vie privée et le droit à la protection des données, ou le droit à l'information et à la transparence, ne sont pas des droits absolus. Ils doivent être mis en équilibre avec d'autres droits et avec les droits d'autres personnes ou groupes de personnes. Dans les théories politiques modernes, cette «mise en équilibre» est laissée à l'autorité de l'État, qui régit les différentes libertés fondamentales pour assurer la justice pour tous. Ainsi, dans cette mise en équilibre, les raisonnements éthique et juridique sont étroitement liés. Les théories (politiques) de la justice ont largement abordé cette question au cours des dernières décennies. Sans recourir à une théorie de la justice en particulier, nous pouvons dire, pour lancer notre réflexion, qu'un agent hiérarchise nécessairement ses valeurs en fonction de ce que la hiérarchie interne a prévu. Dans la tradition des droits de l'homme, on peut faire valoir que certaines valeurs sont exprimées sous la forme de droits et que donc un agent ne peut en faire abstraction pour préserver les conditions de son organisme ou assurer son bien-être ⁽²⁸⁵⁾. Les théories de la justice exigent en outre

⁽²⁸⁵⁾ Cf. par exemple: Alan Gewirth fait valoir dans son ouvrage intitulé *Reason and Morality*, Chicago 1978, que la transition de valeurs en droits est nécessaire du point de vue de l'agent, et qu'elle constitue le présupposé de la «volonté» de l'agent d'accorder à d'autres exactement les mêmes conditions que pour leur organisme. Gewirth les a qualifiés de droits à la liberté et au bien-être, et décrété une hiérarchie (formelle) de droits fondamentaux, de droits inaliénables et de droits supplémentaires. Il existe bien un vaste débat autour du rapport entre la dignité et les droits, et entre les droits «fondamentaux» ou «élémentaires» et d'autres types de droits, tels que le droit (à la liberté) politique ou les droits juridiques, mais cette réflexion est d'ordre philosophique. Il suffit, pour ce qui nous occupe, de reconnaître que toute théorie des droits exige une hiérarchisation entre les types de droits et une application des droits égale pour tous les individus.

CHAPITRE IV. | SUR LA NOTION DE COMPROMIS

qu'un équilibre soit trouvé dans et pour les affaires interpersonnelles. Les droits de la personne sont donc nécessairement mêlés à la question de la justice, si nous comprenons la justice comme la théorie qui traite de la réconciliation interpersonnelle entre les différentes revendications des droits des personnes. Comme la justice exige en même temps une théorie politique, c'est-à-dire une théorie de l'État, cela signifie qu'un État doit s'interroger sur les droits visés et sur le degré de priorité accordé à ces droits, à la fois dans un contexte général et dans des circonstances particulières⁽²⁸⁶⁾. Une sorte de mise en équilibre ou de choix entre plusieurs priorités est, semble-t-il, toujours nécessaire.

À cet égard, en prenant l'exemple significatif du droit fondamental à la protection des données à caractère personnel prévu à l'article 8 de la charte des droits fondamentaux de l'Union européenne, «il ne s'agit pas d'un droit absolu, mais doit être pris en considération par rapport à sa fonction dans la société»⁽²⁸⁷⁾. L'article 52, paragraphe 1, de la charte admet donc que des limitations peuvent être imposées à l'exercice de droits tels que ceux énoncés dans les articles 7 et 8 de la charte. Mais il est essentiel d'examiner les contraintes de ces limitations qui doivent respecter certains critères spécifiques: les limitations doivent être prévues par la loi et respecter le contenu essentiel desdits droits et libertés et, dans le respect du principe de *proportionnalité*, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des *objectifs d'intérêt général reconnus* par l'Union ou au *besoin de protection des droits et libertés d'autrui*⁽²⁸⁸⁾. Une situation analogue prévaut dans le système de la Convention européenne des droits de l'homme⁽²⁸⁹⁾.

En effet, la Cour européenne des droits de l'homme et la Cour de Justice de l'Union européenne (CJUE) ont déclaré à maintes reprises qu'il convenait de mettre l'application et l'interprétation de l'article 8 de la Convention et de l'article 8 de la charte en équilibre avec d'autres droits. Parmi les droits fondamentaux susceptibles d'entrer en conflit avec le droit fondamental à la protection des données à caractère personnel figurent, notamment, les droits à la liberté d'expression et d'information, les droits d'accès aux documents, la liberté des arts et des sciences (article 13 de la charte) et le droit de propriété (article 17 de la charte).

Ces exemples démontrent que nous disposons d'une riche jurisprudence et d'une longue histoire académique sur les questions d'éthique et de philosophie juridique relatives à la mise en équilibre et la hiérarchisation des droits.

Pourquoi alors les questions de compromis auxquelles nous sommes confrontés dans le domaine des technologies de la sécurité et de la surveillance sont-elles d'une nature différente?

4.2. Le compromis entre sécurité et liberté

«Vous ne pouvez pas avoir 100 % de sécurité, et aussi 100 % de respect de la vie privée (...) Nous avons des choix à faire en tant que société. (...) Cela implique certains compromis.»

(Barack Obama, Président des États-Unis, San José, Californie, 7 juin 2013).

Le type classique et dominant de compromis découle de la tâche première de l'État de garantir la vie et les droits des citoyens. C'est cette tâche qui explique en partie pourquoi la souveraineté de l'État est (reste) une valeur aussi forte. Faut-il donc que nous renoncions à une partie de notre vie privée pour préserver notre droit fondamental à la sécurité ou, plus généralement, sommes-nous prêts à renoncer à nos droits à la liberté pour assurer la protection fondamentale de notre vie?

La différence entre ce type de compromis et celui étudié dans la section suivante est que, dans le cas de la sécurité, nous ne choisissons pas de participer ou non. La sécurité relève de la responsabilité des institutions de l'État à trouver un équilibre entre d'une part les droits des personnes et d'autre part les droits entre les personnes. Souvent, la sécurité signifie que la limitation de la liberté d'une personne (ou d'un groupe) sécurise la liberté d'une autre personne, ou inversement. C'est parce que certains individus sont catalogués «positifs»

⁽²⁸⁶⁾ Waldron soutient que la loi et la dignité de la personne sont donc étroitement liées, précisément car la personne qui est capable de raisonnement doit, du moins en principe, être en mesure de comprendre les lois. Les législateurs doivent respecter cette capacité de demander les raisons et respecter la dignité des citoyens qui en font preuve. Refuser aux citoyens de pratiquer la transparence ou d'expliquer les raisons pour lesquelles ils doivent appliquer certaines lois manque donc à ce respect et ne peut être justifié que si le «secret» est lui-même nécessaire pour appliquer une loi donnée. C'est le cas pour certaines activités menées par des «services secrets» au nom de la sécurité ou d'autres intérêts supérieurs de l'État.

⁽²⁸⁷⁾ Voir, par exemple, CJUE, Affaires jointes C-92/09 et C-93/09, Volker et Markus Schecke GbR et Hartmut Eifert/Land Hessen, Recueil 2010, para. 48.

⁽²⁸⁸⁾ *Ibid.*, para. 50.

⁽²⁸⁹⁾ Voir pour cela le Manuel de droit européen en matière de protection des données, FRA, 2014.

(les passeports des citoyens européens sont vérifiés plus rapidement que les autres aux douanes de l'UE, par exemple) ou «négatifs» (dans de nombreux cas, appartenir à un groupe particulier ou être d'une nationalité, d'une origine ethnique ou d'une religion spécifique déclenche un examen minutieux) que d'autres profitent ou subissent les désagréments relatifs aux mesures établies. Dans le cas d'un profilage positif, la ligne entre la préférence raisonnable et le privilège indu est difficile à établir, tout comme il est compliqué dans le cas du profilage négatif de tracer la frontière entre un traitement spécial raisonnable et une discrimination induite. À moins que le législateur (l'État) ne soit en mesure d'articuler face à ses citoyens les raisons — et les critères — déterminant certains choix, il ne respecte pas ses propres relations avec les citoyens. Cette relation entre l'État et ses citoyens, comme nous l'avons dit, est fondée (et doit être fondée) sur le respect de leur dignité, c'est-à-dire leur capacité à comprendre et à respecter les lois qui sont mises en place pour les servir tous autant qu'ils sont. Parfois, ce respect est exprimé sous le terme de confiance. C'est certainement exact, mais ce qui est en jeu est beaucoup plus profond que ce que ce terme pourrait suggérer. Le respect de la compréhensibilité des mesures de l'État devient vite sensible dans le domaine de la sécurité et de la surveillance. Comme Waldron l'explique très justement, les enjeux sont particulièrement importants dans les compromis entre la liberté et la sécurité:

L'objet du compromis, dans ce cas, ce ne sont pas seulement les intérêts économiques ou de banales libertés, comme la liberté de conduire sans ceinture de sécurité. Souvent, l'objet du compromis est ce qui était auparavant considéré comme un droit, et la perte de ce droit peut simplement être imposée aux personnes concernées. Les membres d'une minorité sont détenus sans procès, espionnés, battus ou humiliés au cours d'un interrogatoire, tout cela pour que le reste d'entre nous soit plus en sécurité. Cet exemple est choquant parce que les droits sont censés être des garanties accordées à des individus et à des minorités sur les limites des sacrifices qui peuvent leur être raisonnablement imposées. Les droits sont censés restreindre les compromis et non pas être eux-mêmes l'objet du compromis ⁽²⁹⁰⁾.

Nous devons nous interroger sur la fonction exacte des droits de l'homme dans l'acte de la mise en équilibre. Les droits de qui peuvent faire l'objet d'un compromis? Et

quels droits? Les droits de l'homme ne fonctionnent-ils pas comme des «panneaux de signalisation» restrictifs indiquant exactement dans quelle mesure l'État peut agir sans l'autorisation de ceux dont les droits sont «sacrifiés» pour le bien d'autrui? La vie, la sécurité, la sûreté et la liberté d'une personne peuvent-elles être négociées pour la sécurité d'une autre? Peut-on soutenir qu'il est possible de préserver à la fois la sécurité et la liberté à l'ère des nouvelles technologies de sécurité et de surveillance, si les États sont disposés à réexaminer les politiques qu'ils ont mises en place au début du XXI^e siècle sans prendre l'ensemble des problèmes éthiques en considération? Ces questions sont difficiles, et il n'y aura pas de réponse facile. Mais c'est le principe même du compromis: il sous-estime la difficulté associée à l'équilibre délicat entre liberté et sécurité.

4.3. Le compromis entre «emploi et croissance» et «vie privée et liberté»

Un autre type répandu de «compromis» est celui du cadre économique, où les emplois et la croissance économique sont opposés à certaines libertés, notamment au droit à la vie privée. Qu'est-ce qui prévaut? La compétitivité, la croissance et l'emploi, ou les considérations relatives à la confidentialité, à la protection des données, à l'autodétermination de l'information et aux libertés individuelles?

Ainsi, les voies ouvertes par les nouvelles technologies de l'information et de la communication en général, et l'ensemble des approches reprises sous le concept de «données en masse» en particulier, détiennent un formidable potentiel de compétitivité, d'emplois et de croissance. Le dogme de cette école de pensée transparaît de ces lignes: *Les données en masse sont une grosse entreprise. Elles sont essentielles pour notre prospérité et notre compétitivité, la croissance et l'emploi. Il nous faut choisir entre nous accrocher à des notions désuètes de vie privée ou ouvrir la voie à cette nouvelle aubaine économique pour le plus grand nombre.*

Pour ce qui est des technologies signalées dans le chapitre 1, notamment les technologies de traçabilité et de contrôle, les applications en ligne et mobiles, la communication de machine à machine, l'internet des objets, ainsi que la corrélation croisée des analyses de données, le compromis porte non seulement sur de nouvelles façons de produire de la croissance, mais aussi sur de nouvelles façons de produire des connaissances, c'est-à-dire «du renseignement» (au service de la sécurité), ainsi que des connaissances scientifiques. Il implique à la fois des entreprises privées,

⁽²⁹⁰⁾ J. Waldron: *Is this torture necessary?* New York Review of Books, 2007, Vol. 54/16, p. 40.

CHAPITRE IV. | SUR LA NOTION DE COMPROMIS

potentiellement en situations oligopolistiques, et des autorités publiques, et il ne se limite pas à la corrélation croisée des analyses de données puisqu'il s'étend aux analyses prédictives et aux algorithmes.

Des références sont faites à cet égard au programme PRISM de la NSA, aux tensions qui surgissent des activités de Google et de Facebook notamment, mais aussi aux déclarations précoces et prémonitoires de Scott McNealy, PDG de Sun Microsystems, qui affirmait en 1999 que «vous n'avez plus la moindre vie privée de toute façon. Il faudra vous y faire».

Les tenants de cette perspective sont donc impatients de repousser les entraves de la croissance et de l'innovation qu'ils associent, du moins en partie, aux droits à la vie privée, à la protection des données et à l'auto-détermination en matière d'information.

Il convient de noter que cette approche de «compromis» fonctionne à deux niveaux: au niveau de la politique, pour ce qui est d'éliminer les obstacles à la réussite des entreprises, et au niveau de l'individu, qui souhaite utiliser les possibilités offertes par ces entreprises.

Dans le scénario ci-dessus, le choix porte sur l'action d'un individu envers les entreprises. On peut toujours choisir de s'abstenir de certains services afin de préserver des droits à la vie privée auxquels nous accordons plus de valeur que les libertés que nous tirons de l'utilisation d'internet, de la communication par les médias sociaux, et ainsi de suite. Toutefois, plus ces services sont répandus, moins les individus sont *libres* de participer aux pratiques sociales, et plus il est difficile de choisir librement quel service utiliser. À un certain moment, le désir (ou le besoin) de participer socialement et/ou économiquement surpassera le désir de vie privée. Or, le fait que l'État ou le législateur ferme les yeux sur ce *conflit* sape le droit des particuliers à opter pour des modes de vie qu'ils auraient sans cela toutes les raisons de choisir. L'approche du compromis dissimule le fait que la perte de vie privée que nous subissons tous lorsque nous participons à la nouvelle économie et aux nouveaux moyens de communication n'est en fait pas nécessaire. Elle ne reflète que la réticence à poser des règles qui accorderaient plus d'importance aux droits individuels qu'aux gains des entreprises, sur la base de critères transparents et compréhensibles. L'effort qui a été illustré dans le domaine de la protection des données est un bon exemple de la manière de mettre en place ces critères, et cet effort — quoiqu'insuffisant — est certainement le bienvenu.

Dans les discours sur les technologies de sécurité et de surveillance, il est possible de trouver des alternatives au compromis. Dans ce qui suit, nous allons tout d'abord aborder les concepts de «somme positive» et de «gagnant-gagnant», et ensuite l'approche évolutive fondée sur la notification et le choix (le consentement) lors de la collecte des données (autrement dit les questions soulevées par la sécurité et la surveillance dans les relations avec le marché, ou liées à la sécurité de l'État).

4.4. Des alternatives aux compromis? Les concepts de «somme positive» et de «gagnant-gagnant»

Les développements ci-dessus indiquent la difficulté et la complexité de ces enjeux et de ces priorités inextricables.

Et si nous n'avions pas à nous confronter à ces choix difficiles? Et si nous pouvions gagner des deux côtés?

Telle est précisément la théorie séduisante des défenseurs des concepts de «somme positive» et de «gagnant-gagnant» ⁽²⁹¹⁾. En fait, leur argument est qu'en recourant aux bonnes technologies (des technologies renforçant la protection de la vie privée, des technologies intégrant la vie privée par la conception), il n'est pas nécessaire de faire ces choix difficiles.

Ces approches disposent d'un formidable potentiel, mais elles soulèvent par ailleurs une série de questions sur les failles de ce postulat.

Tout d'abord, peut-on vraiment — comme le préconisent les tenants de ces concepts — se passer de la «mise en équilibre» (éthique/politique/etc.)? Pour le dire autrement, le changement de concept préconisé vers ceux de «somme positive» et de «gagnant-gagnant» peut-il faire l'impasse sur la nécessité d'évaluer ce qui est (ou risque d'être) perdu ou réduit et ce qu'il y a à gagner?

À ce stade, une deuxième question se pose: si l'approche et les discours consistent à nier la nécessité de cette mise en équilibre, là où cet ajustement serait en fait nécessaire, cela ne reviendrait-il pas à tenter de cacher la mise en équilibre? Dans ce cas, cette approche masquerait effectivement la mise en équilibre. Cela

⁽²⁹¹⁾ Une exposition intéressante, complète et très bien faite est proposée dans l'ouvrage d'Ann Cavoukian, *Privacy by Design*, Office of the Information & Privacy Commissioner of Ontario, Canada, 2013.

nous amène à nous demander, d'une part, s'il est souhaitable de refuser une mise en équilibre et, d'autre part, s'il est souhaitable que la mise en équilibre soit masquée. Cela nous amène également à une question plus pratique: est-il souhaitable que la mise en équilibre soit confiée à un seul organe?

Cela nous amène à une troisième piste de réflexion: n'est-il pas plus souhaitable de reconnaître les gains, les pertes, les risques et la répartition des risques? N'est-il pas plus souhaitable que la mise en équilibre soit reconnue et effectuée au vu et au su de tous, avec la participation des parties concernées et/ou une justification explicite du choix opéré?

Sans cela, le risque est de priver le reste de la société et des citoyens de leur capacité de réflexion éthique en ce qui concerne les questions relatives à la sécurité, à la protection de la vie privée, à ce qui compte pour chacun et pour le bien commun (il existe autrement dit un risque de générer des effets de déresponsabilisation). Un tel risque peut en outre apparaître au niveau de la notion même — et des pratiques — de «la vie privée par la conception», en intégrant la capacité de réflexion éthique, la perplexité, la pause de réflexion, le geste critique, l'évaluation et le choix, dans une technologie, un algorithme ou un dispositif. Il existe donc un risque de confiscation et de neutralisation de la capacité de réflexion éthique de tous les individus.

Sans cela, il existe également un risque d'insuffler un faux sentiment de sécurité — même si c'est précisément ce sentiment de sécurité qui est recherché en premier lieu.

4.5. Des alternatives aux compromis? *Les leçons sur la vie privée tirées des notifications et des consentements*

Il existe d'autres alternatives en ce qui concerne l'institutionnalisation des droits concernés et, de fait, elles ont été créées bien avant l'avènement des technologies les plus récentes présentées dans le chapitre 1. Il est important de revoir ces options afin d'évaluer la manière dont elles pourraient être davantage développées dans et pour le contexte actuel.

Cette section examine la situation délicate de la protection des données et de la vie privée, en fait la situation de l'autodétermination en matière d'information, de façon à faire ressortir les idées clés et à développer davantage les principes et les critères requis pour les technologies d'aujourd'hui et de demain.

Les lignes directrices régissant la protection de la vie privée et les flux transfrontaliers de données de caractère personnel adoptées par le Conseil des ministres de l'Organisation de coopération et de développement économiques le 23 septembre 1980 ⁽²⁹²⁾ marquent un jalon important dans l'identification précoce des problèmes de vie privée et de sécurité et les réponses à apporter, et des menaces et des transformations prévisibles à l'époque. Si elles étaient particulièrement judicieuses et opportunes — ou en avance sur leur temps —, les lignes directrices de 1980 fournissent en tant que telles un cadre sur la façon de réfléchir à la protection des données et à la vie privée aujourd'hui et pour l'avenir ⁽²⁹³⁾. Les lignes directrices de l'OCDE définissent huit principes clés:

1. *Principe de la limitation en matière de collecte* — Il conviendrait d'assigner des limites à la collecte des données de caractère personnel et toute donnée de ce type devrait être obtenue par des moyens licites et loyaux et, le cas échéant, après en avoir informé la personne concernée ou avec son consentement.
2. *Principe de la qualité des données* — Les données de caractère personnel devraient être pertinentes par rapport aux finalités en vue desquelles elles doivent être utilisées et, dans la mesure où ces finalités l'exigent, elles devraient être exactes, complètes et tenues à jour.
3. *Principe de la spécification des finalités* — Les finalités en vue desquelles les données de caractère personnel sont collectées devraient être déterminées au plus tard au moment de la collecte des données et lesdites données ne devraient être utilisées par la suite que pour atteindre ces finalités ou d'autres qui ne soient pas incompatibles avec les précédentes et qui seraient déterminées dès lors qu'elles seraient modifiées.
4. *Principe de la limitation de l'utilisation* — Les données de caractère personnel ne devraient pas être divulguées, ni fournies, ni utilisées à des fins

⁽²⁹²⁾ Pour le texte complet des lignes directrices de l'OCDE de 1980 et l'exposé des motifs qui les accompagne, voir: <http://www.oecd.org/fr/sti/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm>

Pour les lignes directrices révisées de 2013, voir: <http://www.oecd.org/ist/ieconomy/2013-OCDE-privacy-directives.pdf>

⁽²⁹³⁾ En 2013, ces lignes directrices ont été révisées sans véritable changement de paradigme.

CHAPITRE IV. | SUR LA NOTION DE COMPROMIS

autres que celles spécifiées conformément au paragraphe 9, si ce n'est:

- a) avec le consentement de la personne concernée; ou
 - b) lorsqu'une règle de droit le permet.
5. *Principe des garanties de sécurité* — Il conviendrait de protéger les données de caractère personnel, grâce à des garanties de sécurité raisonnables, contre des risques tels que la perte des données ou leur accès, destruction, utilisation, ou divulgation non autorisés.
6. *Principe de transparence* — Il conviendrait d'assurer, d'une façon générale, la transparence des progrès, pratiques et politiques, ayant trait aux données de caractère personnel. Il devrait être possible de se procurer aisément les moyens de déterminer l'existence et la nature des données de caractère personnel, et les finalités principales de leur utilisation, de même que l'identité du maître du fichier et le siège habituel de ses activités.
7. *Principe de la participation individuelle* — Toute personne physique devrait avoir le droit:
- a) d'obtenir du maître d'un fichier, ou par d'autres voies, confirmation du fait que le maître du fichier détient ou non des données la concernant;
 - b) de se faire communiquer les données la concernant; dans un délai raisonnable; moyennant, éventuellement, une redevance modérée; selon des modalités raisonnables; et sous une forme qui lui soit aisément intelligible;
 - c) d'être informée des raisons pour lesquelles une demande qu'elle aurait présentée conformément aux alinéas a) et b) est rejetée et de pouvoir contester un tel rejet; et
 - d) de contester les données la concernant et, si la contestation est fondée, de les faire effacer, rectifier, compléter ou corriger.
8. *Principe de la responsabilité* — Tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus.

Les lignes directrices sont un témoignage de l'intérêt, déjà bien présent dès les années 1970 et qui n'a cessé d'augmenter jusqu'au début du XXI^e siècle, accordé

à l'autorité exercée par un individu sur ses données, fondée sur le principe de la liberté et de l'autodétermination. Cela se traduit par l'accent mis *sur la notification et le choix (le consentement) au moment de la collecte de données* et par l'exigence imposée à ceux qui récupèrent les données de respecter plusieurs normes visant à protéger les droits à la liberté des utilisateurs. Les cadres pour la protection des données et de la vie privée ont été construits sur cette pierre angulaire dans de nombreuses régions du monde (notamment dans l'UE et aux États-Unis), sur la base de la notion de transaction selon laquelle une entité fournit à un individu une notification à propos de son intention de collecter des données, cet individu exerce son droit à faire un choix en connaissance de cause quant à l'opportunité d'autoriser cette collecte, après quoi l'utilisation subséquente des données est limitée par les conditions de cette notification (avec le rôle important joué à cet égard, et dans le contexte des principes indiqués ci-dessus, par le principe de limitation de la finalité).

Ce cadre a notamment eu pour résultat, d'un point de vue pratique, de faire apparaître ces longues notifications déroulantes que l'on fait défiler sans y réfléchir pour donner son consentement, c'est-à-dire atteindre le bouton «J'accepte» en bas de l'écran et cliquer dessus.

Les limitations de ce modèle sauteront aux yeux de la plupart des lecteurs, mais seulement à un niveau intuitif ⁽²⁹⁴⁾.

Une autre lacune concerne *l'exercice* de ce droit.

D'une part, cette question porte sur la notion de «choix» qui, comme discuté ci-dessus, doit reposer sur de véritables options.

D'un autre côté, il est tout à fait remarquable que — notamment en ce qui concerne un recours — ce droit ne soit en fait pas exercé (il y a même un renversement de la charge de la preuve, dans l'UE notamment, de sorte que dans la transaction indiquée ci-dessus il n'appartient pas aux personnes de prouver la violation). Les commissaires à la protection de la vie privée ne reçoivent pour ainsi dire aucune plainte. La majorité des atteintes à la vie privée restent inconnues, non réglementées, non contestées. En tout état de cause,

⁽²⁹⁴⁾ En outre, très concrètement, la lecture est souvent délibérément rendue compliquée par l'utilisation de lettres capitales. Cela a pour effet de décourager les consommateurs outre la terminologie juridique bien souvent jargonneuse.

le fait de mettre l'accent sur la notification et le consentement au moment de la collecte — ou, de manière plus large, sur la conformité à la réglementation — est insoutenable en tant que modèle exclusif pour assurer l'avenir de la vie privée.

Quelles sont les options?

L'une des voies explorées concerne les solutions technologiques, qui intègrent la vie privée dans la conception des produits et des services, par exemple par l'intermédiaire de la désidentification/anonymisation/pseudonymisation des données personnelles.

Une autre voie consiste à faire passer l'accent de la «collecte» à l'«utilisation» des données, c'est-à-dire de la notification et du consentement au moment de la collecte à l'utilisation des données. Il faut noter les effets que ce passage pourrait avoir sur les principes et les pratiques de la *spécification et de la limitation de la finalité* constituent un enjeu essentiel dans ce contexte.

Un premier aspect lié, mais distinct — en ce qui concerne le passage de la collecte à l'utilisation — consiste à modifier l'équilibre des responsabilités, qui pèsent actuellement lourdement sur les personnes concernées vers une plus grande responsabilisation des utilisateurs de données — notamment en mettant l'accent sur la responsabilité institutionnelle de la «gestion des données» plutôt que sur la simple conformité à la réglementation.

Un deuxième aspect lié, mais distinct, consiste à évoluer vers un système d'analyse de risque. Cela peut être perçu comme un projet d'amélioration ou comme une façon de faire accepter l'abandon de la spécification et de la limitation de la finalité ⁽²⁹⁵⁾. Un élément à cet égard est le développement possible d'un processus d'évaluation des risques visant à mesurer les différentes utilisations proposées, ainsi que des ensembles de mesures destinées à réduire les risques.

Il convient de bien garder à l'esprit l'apprentissage lié à l'analyse des risques et celui lié à l'évaluation des effets (concernant l'évaluation de l'incidence sur la vie privée), comme discuté dans la section suivante.

4.6. Au-delà du compromis

Un peuple prêt à sacrifier un peu de liberté pour un peu de sécurité ne mérite ni l'un ni l'autre.

(Benjamin Franklin)

Comprendre les conditions du compromis

Lors de l'analyse du compromis en tant que type, scénario ou métaphore ou en tant que vision du monde guidant les choix politiques et l'évolution des institutions, il est important de le considérer sérieusement, afin de définir et finalement de dépasser ses limites.

Qu'est-ce donc qu'un «compromis» et qu'est-ce que cela implique? À la base, cela signifie que l'on abandonne quelque chose pour en gagner une autre. Et en effet, cela signifie que quelque chose est cédé en échange d'autre chose. Il s'agit donc d'un échange.

«Si nous voulons davantage de sécurité, alors il nous faut renoncer à une partie de notre vie privée et à d'autres libertés.» «Pour plus d'emplois et plus de croissance, il nous faut renoncer à certains de nos droits de l'homme.»

Mais qu'est-ce qui est acquis et qu'est-ce qui est cédé? Très précisément, en ce qui concerne les choix relatifs à l'adoption et au déploiement des nouvelles technologies de sécurité et de surveillance, que signifie exactement «davantage de sécurité» et quel bénéfice en tire-t-on?

Il nous incombe de poser la question de savoir si, en fait, la notion même de gain ne doit pas être considérée comme problématique en l'absence d'évaluation rigoureuse, d'appréciation ou d'estimation. D'où la nécessité de remettre en question au moins le coût et l'efficacité de ces efforts et, en définitive, la formulation de ces efforts lorsque des *choix* ou des *alternatives* semblent écartés.

Un autre aspect important auquel il convient de prêter attention est le «nous» dans les propositions en italique ci-dessus. Qui est ce «nous»? C'est-à-dire, comment ces décisions (celles relatives à l'adoption et au déploiement des nouvelles technologies de sécurité et de surveillance) ont été prises, ou, pour le dire plus simplement, par qui ces décisions ont été prises. Ce point mérite d'être creusé: dans les conditions de l'échange, le «nous» qui concède est-il le même «nous» qui en tire profit? Claiement: qui gagne, qui perd, qui décide, qui *sait*?

⁽²⁹⁵⁾ Notamment dans les travaux financés par Microsoft Corporation, voir Fred H. Cate et Viktor Mayer-Schönberger, Notice and Consent in a World of Big Data: Microsoft Global Privacy Summit Summary Report and Outcomes, novembre 2012.

CHAPITRE IV. | SUR LA NOTION DE COMPROMIS

La simplicité et les risques

Cet exemple donné par Bruce Schneier est un cas d'espèce: ⁽²⁹⁶⁾

«Vous pouvez avoir autant de sécurité que vous voulez, tant que vous êtes disposé à accepter des compromis. Peu de temps après le 11 Septembre, un journaliste m'a demandé: «Comment pouvons-nous empêcher que cela ne se produise plus jamais?» «C'est facile», j'ai répondu. «Il suffit de clouer tous les avions au sol.» C'est une idée ridicule, mais nous pourrions faire en sorte que ce type d'attaque n'ait plus jamais lieu si nous sommes disposés à accepter le compromis.»

Cela illustre, même sans le vouloir, les terribles limites de la vision mondiale du compromis. Car, outre le côté ridicule de la situation exposée ici, l'idée que cette mesure extrême («clouer tous les avions au sol») permettrait en fait «d'assurer que l'attaque ne puisse jamais se répéter», est elle-même particulièrement incongrue ou manque de perspective. Si les avions étaient maintenus au sol, des attaques pourraient malheureusement encore être menées par d'autres moyens.

«Facile. Tout simplement violer la vie privée et les libertés individuelles de chacun.» Personne n'ose proposer cette solution. Au contraire, cette sombre perspective souligne la simplicité de certains discours, ainsi que la fragilité de la frontière entre le possible et le concret et le contraste entre une telle simplicité et la difficulté de traiter efficacement des besoins en matière de sécurité.

Il est également intéressant de noter que l'expérience et l'expertise de Bruce Schneier l'ont finalement conduit à élaborer un processus qu'il décrit comme parfaitement en phase avec le cadre d'évaluation et de gestion des risques. Plus généralement, le système d'analyse de risque est en effet la référence dominante dans le domaine de la sécurité de l'information, des systèmes et des infrastructures de sécurité. Le système d'analyse de risque possède sa propre histoire, sa propre institutionnalisation et ses propres contraintes. Ce que l'on peut

en retenir, c'est que la face cachée de ce système est en fait une combinaison de compromis bien plus complexe que ce que les dichotomies et les régimes unilatéraux ne prévoient, avec, d'une part, les compromis entre les différents risques ou entre les risques et les coûts, ou ceux entre les coûts, les risques et les bénéfices, et la répartition des risques, et, d'autre part, les divisions notables et insoutenables entre l'évaluation du risque et la gestion du risque, entre la science et la politique, et entre la connaissance et la décision.

La mesure de toutes choses

Comme indiqué ci-dessus, il nous incombe de nous demander si la notion même de gain (qui est au cœur du compromis) ne doit pas être considérée comme problématique en l'absence d'évaluation rigoureuse, d'appréciation ou d'estimation.

Au-delà de l'exigence minimale d'examiner le coût et l'efficacité de ces efforts (c'est-à-dire le choix d'adopter et de déployer de nouvelles technologies de sécurité et de surveillance — une exigence minimale qui n'est bien souvent même pas respectée) les questions se rapportant à l'évaluation sont les suivantes: que gagne-t-on, que perd-on, par qui, comment cela est-il encadré, mesuré et partagé, par qui, et comment cela s'articule-t-il avec les processus de prise de décisions.

Le cadre d'évaluation doit nécessairement comprendre l'évaluation des *avantages* et des *inconvénients* (et des tenants et aboutissants, des implications, des limites et des contraintes, des FFPM, c'est-à-dire des forces, des faiblesses, des possibilités et des menaces) de certains investissements dans la sécurité. Ce n'est cependant pas suffisant, dans la mesure où ce qui est nécessaire, de disposer d'évaluations comparatives qui ne se concentrent pas sur une technologie spécifique ou sur un investissement en particulier dans la sécurité, qui ne se concentrent pas sur une «solution technologique» ou une «solution de sécurité» lorsque la question pourrait être formulée différemment et donc traitée différemment.

Il est également important que ces évaluations ex ante des investissements dans la sécurité offrent une authentique aide à la prise de décision plutôt que de légitimer un ensemble d'options politiques prédéfinies. En effet, toute formulation du type «il n'y a pas de choix, il n'y a pas d'alternative, il n'y a pas de place pour le débat et la justification, nous devons tout simplement le faire» ne peut être tolérée.

⁽²⁹⁶⁾ Bruce Schneier, le célèbre cryptographe et directeur technique de Counterpane Internet Security, auteur de l'ouvrage *Applied Cryptography* et du best-seller intitulé *Secrets & Lies*, a été interviewé, après la publication de *Beyond Fear*, par Lawrence M. Walsh, directeur de la rédaction de *Information Security*. Article daté de novembre 2013 consulté le 16 décembre 2013 à l'adresse: <http://searchsecurity.techtarget.com/feature/Bruce-Schneier-Beyond-Fear-Searching-for-rational-security>

Cela nous ramène à la dialectique des fins et des moyens dans laquelle s'inscrivent la surveillance et la sécurité. Alors que la sécurité est d'abord présentée comme un moyen pour permettre ou assurer l'épanouissement individuel et collectif (avec la surveillance comme moyen de parvenir à la sécurité), on observe souvent — ou on occulte souvent — une dérive subtile de la sécurité qui devient une fin en soi. La sécurité est donc erronément considérée comme un synonyme ou un substitut du bien commun.

Au cœur des difficultés décrites ci-dessus figure précisément la question de l'intérêt général et du bien commun, sachant que la question de l'allocation des ressources est également une question de justice et de solidarité. Ces difficultés sont aggravées par l'absence de débat public sur la sécurité en tant que moyen, sur le choix des moyens (y compris les technologies de surveillance) visant à renforcer la sécurité, et sur les finalités poursuivies. En fait, le débat public (en tant que tel et en tant que déclencheur de la mobilisation des autres constituants de l'appareil démocratique) est un élément nécessaire du cadre d'évaluation décrit ci-dessus.

Le présent avis participe également à ce débat réflexif et informé pour lequel il plaide. Après avoir étudié le riche tissu conceptuel de la sécurité et de la surveillance, avec ses tenants et aboutissants et ses diverses facettes (relatives à la vigilance, à la vulnérabilité, au secret, au contrôle, la réalisation, etc. — cf. chapitre 3), il est important dans ce contexte d'attirer l'attention sur une autre dimension de la question des **causes profondes**. Il est important de contrecarrer l'effet Matthieu qui existe dans (et entre) les sociétés en examinant les disparités socio-économiques — en fait la grave question des inégalités au sens large — en tant que déterminant essentiel de la surenchère dans laquelle s'inscrivent la sécurité et la surveillance. Cela doit être considéré au niveau individuel (avec la notion de propriété et l'importance attachée à la protection de la propriété privée), ainsi qu'à l'égard de la sécurité d'État, en l'élargissant au niveau supranational, européen notamment.

Qu'est-ce que l'Europe a, en définitive, à protéger? À sécuriser? De Kiev à Lampedusa, et d'Athènes à Sidi Bouzid, ce sont des questions cruciales à aborder.

Formulation de recommandations en matière de technologies de sécurité et de surveillance

La surveillance par l'État, la sécurité nationale, la loi et le maintien de l'ordre, la collecte de renseignements, la surveillance des entreprises et le prélèvement de données partagées à titre privé sont souvent interdépendants et fonctionnent comme des «assemblages de sécurité et surveillance». S'il y a lieu de reconnaître cette sombre réalité, il ne faut pas y succomber en termes analytiques et prescriptifs. Autrement dit, les différents volets de ces assemblages doivent être séparés et traités spécifiquement, en fonction des utilisations qui en sont faites. Étant donné que des agents différents ont des responsabilités différentes, les principes doivent être traduits en critères plus sensibles au contexte, afin de répondre aux besoins des entreprises, d'une part, et de l'État, d'autre part.

Mais c'est aussi à ce stade que le scénario du compromis constitue un cadre trompeur: l'équilibre trouvé dans un contexte, c'est-à-dire de l'utilisation des données et le partage des données, peut ne pas être applicables dans d'autres, c'est-à-dire la sécurité de l'État, précisément parce que l'individu ne peut pas choisir d'y adhérer ou non. La question qui se pose alors est de savoir comment l'individu peut être respecté dans son ou ses droits à la vie privée et à la sécurité lorsque les mesures de protection de ces droits exigent leur violation — ce qui semble être un processus «normal» de hiérarchisation se transforme facilement en une contradiction et c'est pour *cette* raison que les droits ne doivent pas être «échangés» mais qu'il faut bien, au contraire, restreindre le compromis.

Les recommandations du GEE visent à recenser les critères de responsabilité et de surveillance afin de protéger la liberté des individus et leur sécurité. Reste à savoir s'il est possible de dépasser la métaphore du «compromis» et de revenir à la traditionnelle métaphore de la hiérarchisation des droits — une métaphore qui ne cède aucun droit, même si elle reconnaît que les priorités peuvent varier non seulement selon les individus, mais également dans différents contextes. Dans la mesure où la confiance reflète le sens d'une acceptation générale ou, autrement dit, de l'affirmation sociétale qu'un bon équilibre a été trouvé entre la liberté individuelle et la vie privée, et entre la justice et la sécurité sociétale, la méfiance reflète exactement l'inverse: le sentiment d'un malaise général et la renonciation potentielle ou, autrement dit, l'objection sociétale du déséquilibre entre la liberté et la protection de la vie privée, et entre la justice et la sécurité sociétale.

Recommandations

Le Groupe européen d'éthique des sciences et des nouvelles technologies (GEE) a été invité à émettre un avis sur les aspects éthiques des technologies de sécurité et de surveillance. Il s'agit là d'une tâche certes d'actualité, mais difficile, étant donné que ces technologies représentent des objectifs très divers, sont mises en œuvre par différents acteurs, entraînent différents degrés et formes d'atteintes aux droits de l'homme, et débouchent sur différentes utilisations.

La disponibilité croissante de volumes importants d'informations et l'expansion des réseaux de communication ont joué un rôle déterminant dans la mondialisation qui s'est produite au XX^e siècle. Cette évolution s'est par ailleurs accompagnée d'un sentiment accru d'insécurité, d'un manque de confiance et d'un faible niveau de tolérance à l'égard du risque. Les tueries perpétrées dans les écoles, les cinémas et les centres commerciaux, les attentats aux explosifs commis dans le métro, les trains et les avions, les enlèvements d'enfants et les sévices et vols visant les personnes âgées ont contribué à renforcer le sentiment d'insécurité que nous éprouvons au sein même de nos communautés. Cette perception persiste, alors même que, objectivement, tout indique que le monde n'a jamais été aussi sûr qu'aujourd'hui. Il ne fait aucun doute que les stratégies de sécurisation adoptées en Europe et dans d'autres parties du monde résultent de la volonté des pouvoirs publics de répondre à ce sentiment d'insécurité éprouvé par les populations.

Selon une acception assez étroite, la sécurité désigne la protection des personnes contre les préjudices physiques ou la menace de tels préjudices, et constitue un élément essentiel du bien-être. En vertu du contrat social, les États se sont engagés à garantir la sécurité de leurs citoyens en échange du pouvoir de restreindre les libertés individuelles. Cela ne représente toutefois qu'un aspect de la problématique de la sécurité. En effet, si la protection de l'intégrité physique est nécessaire, elle n'est pas suffisante. La sécurité doit être envisagée dans un contexte plus large englobant à la fois la sécurité des individus et celle de la société dans son ensemble. Il nous faut dès lors élargir notre réflexion au-delà du seul rôle de l'État et nous pencher sur celui des individus, des communautés et des entités commerciales. L'Europe est une communauté de valeurs partagées au sein de laquelle nous nous efforçons de préserver la dignité, l'autonomie, la liberté et la justice en nous appuyant sur le cadre des droits de l'homme. L'environnement ainsi créé permet

à l'individu de s'épanouir en laissant libre cours à sa créativité et à son esprit d'innovation, en nouant des relations personnelles solides et en participant à la vie de sa communauté. L'éducation, la santé, la démocratie, l'environnement et l'égalité sont autant d'éléments essentiels pour atteindre l'objectif d'une Europe sûre.

L'approche plutôt restrictive adoptée jusqu'ici en matière de sécurité, notamment dans le contexte de l'interprétation étroite de la sécurité de l'État, a consisté à se concentrer sur la théorie selon laquelle il faudrait nécessairement accepter des compromis, un exemple classique étant le compromis entre la liberté, souvent représentée sous l'angle de la vie privée, et la sécurité. S'il est certes nécessaire de trouver un bon équilibre entre des principes ou valeurs concurrents lorsqu'ils sont incompatibles, le respect de certains principes fondamentaux, comme celui de la dignité humaine, n'est tout simplement pas négociable. Aussi devons-nous dépasser la rhétorique des compromis pour nous engager dans une approche plus nuancée dans laquelle les technologies et les mesures de sécurité sont évaluées à l'aune de leur proportionnalité et de leur efficacité et dans laquelle les droits, au lieu de faire l'objet de marchandage, sont considérés comme prioritaires.

Le GEE reconnaît que, dans une société démocratique, il est parfaitement légitime que le pouvoir de l'État se manifeste par la mise en place d'agences qui, sous réserve de restrictions légales strictes, sont autorisées à recourir à des technologies de surveillance pour préserver la sécurité des citoyens. Le GEE considère également que la **dignité** de la vie humaine suppose un certain degré de confidentialité et de discrétion. Lorsque les pouvoirs publics portent atteinte au droit à la vie privée d'un individu, ces atteintes doivent être **justifiées** et devraient faire l'objet d'un contrôle de l'autorité judiciaire. La surveillance doit être **nécessaire** et **proportionnée** afin qu'il existe un lien approprié entre les mesures prises et les objectifs atteints. L'**efficacité** de l'intervention est un élément essentiel pour évaluer sa proportionnalité, et cette efficacité doit être réexaminée à intervalles réguliers. Les compétences en matière de surveillance devraient être accordées pour des buts spécifiques et une durée déterminée. Il convient d'examiner et de documenter les **solutions alternatives** permettant d'atteindre les mêmes objectifs, et d'opter pour la méthode la moins intrusive. L'**obligation de rendre compte** étant un préalable indispensable à la surveillance publique, il doit apparaître clairement que les activités de surveillance sont menées pour des motifs valables et dans le

RECOMMANDATIONS

respect des codes de bonnes pratiques accessibles au public. La mise en œuvre des technologies de sécurité et de surveillance doit être aussi **transparente** que possible et les exceptions légitimes doivent être prévues expressément dans l'ordre juridique. Il convient que les organisations privées et/ou commerciales menant des activités de surveillance soient elles aussi tenues de respecter les critères susmentionnés.

La discrimination est un grave sujet de préoccupation à cet égard. Nous devons être conscients des effets imprévus que pourrait avoir une surveillance omniprésente. En effet, ce type de surveillance pousse les individus à se conformer à une certaine normalité (en tant que normativité), et donc à modifier leurs comportements et à renforcer davantage encore cette norme. Il en résulte une société appauvrie — voire totalement uniformisée — privée de toute diversité, créativité, et même cohésion. La discrimination peut consister à cibler et/ou surveiller plus spécifiquement certaines minorités: le GEE demande que des mesures soient prises lorsqu'une telle situation est constatée dans un État membre de l'Union. Elle concerne également la question du profilage et celle de la stigmatisation. Il faut reconnaître que, dans le cas du profilage, les formes sont multiples, allant des programmes de type «opt in/out» (comme le programme «Global Entry») au profilage de populations entières au moyen de techniques sophistiquées de surveillance de masse, en passant par les «délits de faciès» et la reconnaissance des visages (ou d'autres systèmes biométriques). Pour ce qui est de la stigmatisation, si elle doit de toute évidence être évitée (de même que son corollaire, l'humiliation), le rôle joué par l'utilisation de plus en plus généralisée des algorithmes dans les dispositifs de sécurité et de surveillance est particulièrement préoccupant à cet égard. Ces algorithmes peuvent en effet brouiller ou confisquer la réflexivité éthique et la justification des choix, avec pour résultat le profilage intégré ou la «stigmatisation par conception». Ils sont également susceptibles de renforcer encore la normalité et la conformité mentionnées ci-dessus, en occultant les processus de sélection et en les dissociant de toute intervention et de tout raisonnement humains. Le GEE n'ignore en rien le risque d'instrumentalisation des conseils d'éthique et des organismes apparentés dans ces processus de normalisation liés aux nouvelles technologies. Il est en effet parfaitement conscient de la difficulté qu'il y a à se pencher sur les aspects éthiques des technologies de sécurité et de surveillance sans que cela soit perçu comme une sorte de cautionnement global. Il a choisi de ne pas reculer devant cette difficulté, mais de l'attaquer de front dans cet avis.

Au vu des considérations qui précèdent, le GEE convient des recommandations suivantes dans le domaine des technologies de surveillance et de sécurité:

I. Le recours aux technologies qui sont susceptibles de porter atteinte à la vie privée des individus et que ces derniers n'ont pas la possibilité d'accepter ou de refuser nécessite une justification particulière. Le GEE demande qu'une *justification au cas par cas* soit exigée pour ces mesures.

1. **Obligation de rendre compte**

Les États membres doivent veiller à ce que les organismes habilités à surveiller la sphère privée des individus agissent dans l'intérêt général et soient tenus de rendre compte de leurs actes. Lorsque l'État délègue des tâches de sécurité et/ou de surveillance à des entreprises privées, ces entreprises sont soumises aux mêmes obligations légales et éthiques; il convient, par ailleurs, que les États membres mettent en place des mécanismes permettant de vérifier que ces obligations sont respectées.

2. **Contrôle effectué par les juges**

Les États membres doivent disposer d'un système de contrôle sous l'autorité des juges pour les activités de surveillance menées par les pouvoirs publics dans le cadre d'enquêtes pénales. Il convient que les individus soient informés a posteriori de la surveillance dont ils ont fait l'objet, pour autant que cela ne compromette pas le déroulement d'une enquête. Tout individu ayant fait l'objet d'une surveillance illicite devrait avoir la possibilité d'exercer son droit de recours.

3. **Vers une conception commune de la sécurité nationale**

Les valeurs européennes communes inscrites dans la charte des droits fondamentaux de l'Union européenne constituent le cadre normatif qui pourrait servir de base à une conception éthique commune de la sécurité nationale.

a) Tout en reconnaissant que la sécurité nationale figure, à juste titre, au cœur des intérêts nationaux et relève de la compétence des États membres, le GEE recommande que les institutions de l'Union, en concertation avec les États membres, trouvent les moyens de parvenir à une conception commune de la sécurité nationale.

- b) Le GEE recommande également que les États membres mettent en place des procédures leur permettant de tenir les autres États membres dûment informés de leurs activités de renseignement extraterritoriales afin de préserver la confiance entre les différents partenaires.
- c) Il convient que les États membres s'abstiennent de surveiller d'autres États membres sous couvert de sécurité nationale dans le but d'en retirer un avantage commercial, cette activité étant contraire à l'objectif de l'Union de mettre en place un marché européen unique.

4. Drones

Le développement rapide des drones et leur déploiement accru par les États membres dans des contextes militaires, civils et commerciaux n'ont pas été accompagnés par des mesures de gouvernance et de contrôle, de sorte que les dispositions en vigueur demeurent pour le moins fragmentaires. Pour les usages civils et commerciaux, l'Union doit se doter d'un cadre juridique détaillé régissant le développement, l'achat, l'utilisation et l'exportation des drones. Le GEE se félicite des mesures déjà adoptées par la Commission dans le domaine de l'intégration des systèmes d'aéronefs télépilotés (Remotely Piloted Aircraft Systems ou RPAS) dans le système aéronautique européen (incluant l'organisation d'une vaste consultation et la publication d'une feuille de route). Et le fait qu'il ait d'emblée été prévu de prendre en considération les conséquences du déploiement des drones sur la société dans son ensemble doit être salué.

- a) Compte tenu de l'engagement pris récemment par l'Union d'améliorer la coordination entre les États membres dans le domaine du développement et de l'achat des drones, le GEE préconise d'étendre cette coopération à l'établissement de normes communes et d'un cadre réglementaire régissant les usages civils et commerciaux des drones dans l'Union. Il conviendra en particulier d'évaluer les cadres mis en place par l'Union en matière de protection des données et de la vie privée afin de déterminer si le régime réglementaire en vigueur est approprié dans le contexte de l'intégration des systèmes d'aéronefs télépilotés dans l'espace aérien européen.
- b) Les États membres doivent veiller à ce que leurs politiques en matière d'usage des drones dans la sphère publique domestique (c'est-à-dire à l'intérieur des frontières nationales) ne portent

pas atteinte aux droits humains des personnes visées par les opérations impliquant des drones. Cet usage des drones dans la sphère publique domestique doit être soumis à autorisation et faire l'objet d'un contrôle approprié afin de garantir la sécurité et de prévenir les abus. En outre, les personnes ou entités sollicitant l'autorisation d'utiliser des drones de surveillance doivent démontrer que l'usage envisagé est justifié, nécessaire et proportionné. Le GEE recommande également que les politiques et procédures régissant l'usage des drones dans la sphère publique domestique à des fins de surveillance soient mises à la disposition du public afin de garantir la transparence, sans laquelle il est impossible d'obtenir la confiance du public.

- c) Le GEE attire l'attention sur les graves problèmes éthiques que soulèvent l'usage militaire des drones et la guerre robotisée, et prend note de la résolution du Parlement européen du 25 février 2014 sur l'utilisation des drones armés. Le GEE appelle les États membres qui utilisent des drones à des fins militaires à faire preuve d'une plus grande transparence et à veiller à respecter leur obligation d'en rendre compte. À cette fin, ils doivent divulguer la base juridique, la portée et les limites de toute frappe mortelle réalisée au moyen de drones et contrôler le respect des cadres juridiques existants applicables aux conflits armés traditionnels. Les informations concernant le nombre de civils et d'autres personnes tués au cours de frappes de drones devraient également être mises à la disposition du public. Le GEE préconise par ailleurs vivement la réalisation de travaux de recherche portant sur les aspects éthiques des frappes mortelles par des drones armés et sur leur compatibilité avec la théorie de la guerre juste. Il importe en outre d'effectuer des recherches sur l'implication de l'agir moral lorsque les opérateurs de drones se trouvent à distance, et que se développent des drones autonomes.

II. En ce qui concerne les technologies de surveillance, la charge de la preuve devrait revenir aux États et/ou aux entreprises, lesquels, avant d'introduire des systèmes de surveillance, doivent démontrer *de manière publique et transparente*:

- que ces systèmes sont **nécessaires**;
- que ces systèmes sont **efficaces**;

RECOMMANDATIONS

- que ces systèmes respectent le principe de proportionnalité (limitation de la finalité, par exemple);
- qu'il n'existe aucune **solution de remplacement** meilleure pouvant se substituer à ces technologies de surveillance.

Ces critères doivent également être soumis par la suite à une évaluation **post factum**, soit dans le cadre des analyses politiques normales, soit dans le cadre des politiques des États membres.

En outre:

- l'**obligation de rendre des comptes** implique que les individus sont en droit d'être informés des technologies de surveillance mises en œuvre – même si, dans certains cas, ces informations ne peuvent être communiquées qu'a posteriori;
- la **transparence** en ce qui concerne les intérêts économiques doit être respectée à tout moment.

5. Données à caractère personnel

Le GEE estime que, dans le domaine des données à caractère personnel, les organisations publiques comme les organisations privées doivent se fonder sur le principe de limitation de la finalité. Autrement dit, les données à caractère personnel ne devraient être recueillies que dans un objectif spécifique et légitime. Les données ainsi recueillies devraient, si possible, être anonymisées et le cryptage devrait être plus largement utilisé, étant donné qu'il peut contribuer à améliorer à la fois la protection de la vie privée et la sécurité. Il convient d'éviter le partage des données par défaut, et de permettre aux utilisateurs de contrôler (par exemple au moyen de paramètres de confidentialité) et de modifier les informations les concernant et détenues par les organisations. Le profilage d'individus à des fins commerciales devrait être subordonné au consentement explicite des personnes concernées. Les organisations commerciales devraient indiquer la *nature des données* qu'il est prévu de recueillir, *par qui* la collecte sera effectuée, *dans quel objectif*, pendant *combien de temps*, et s'il est prévu de relier les données recueillies à d'autres sources de données.

6. Sensibilisation du public aux politiques en matière de données

Le GEE réaffirme qu'il est, selon lui, nécessaire de mieux informer les membres du public sur les modalités, les raisons et les objectifs de la collecte, du

partage et de la protection des données à caractère personnel les concernant. Les pouvoirs publics comme les entreprises doivent, à cet égard, rendre accessibles au public leurs politiques. Il convient que l'Union et les États membres s'efforcent de promouvoir la connaissance, la sensibilisation et le débat quant aux conséquences du recours aux technologies de sécurité et de surveillance sur les individus et la société dans son ensemble. Dès l'école primaire, des programmes d'éducation devraient fournir des informations et des instruments qui permettront aux individus de protéger leurs données personnelles dans l'environnement numérique.

7. Données en masse («Big data»)

Le GEE constate une évolution vers la collecte et la corrélation d'ensembles volumineux de données, appelés «données en masse» («big data»). Bien que le GEE reconnaisse la valeur potentielle que revêtent ces ensembles de données, il craint que, si l'on n'y prend pas garde, le principe de limitation de la finalité, qui est au cœur de la protection des données, soit mis à mal. C'est pourquoi il exhorte les pouvoirs publics et les organisations privées à entreprendre une réflexion éthique poussée qui éclairera leurs actions et leur permettra de les aligner sur les valeurs européennes communes que sont la dignité, le respect de la vie privée et l'autonomie. Le GEE recommande que l'Union élabore un code de conduite pour l'analyse des données en masse qui guiderait les organisations dans ce processus.

8. Algorithmes

Dans le contexte des technologies de sécurité et de surveillance, il importe d'observer que les algorithmes sont, par définition, sélectifs et que leur impartialité est tout aussi sujette à caution que celle des personnes qui les programment. Les algorithmes sous-jacents et leurs paramètres sont des hypothèses éthiques qu'il devrait être obligatoire d'explicitier. En outre, les algorithmes ne sont pas infaillibles et les données produites dépendent des données d'entrée utilisées et de la qualité de celles-ci, qu'il conviendrait, selon le GEE, d'examiner et de valider en permanence. Il convient par ailleurs de prévoir, dans le cadre de la formation des personnes chargées de l'établissement des algorithmes, d'aborder les aspects éthiques de cette activité.

9. Protection de la vie privée dans les communications électroniques

Le GEE recommande que la Commission européenne envisage de réviser la directive sur la vie privée et

les communications électroniques, dont le champ d'application actuel couvre uniquement les communications électroniques. Compte tenu de l'explosion des interfaces numériques qui s'est produite depuis l'entrée en vigueur de la directive, le GEE juge opportun de réviser cette directive en élargissant son champ d'application aux produits relevant de la téléphonie par internet (voice over Internet Protocole — VOIP — les communications sur IP et à haut débit), ainsi qu'aux réseaux privés d'entreprise.

10. Évaluation de l'impact sur la vie privée

Les procédures d'évaluation de l'impact sur la vie privée doivent faire partie intégrante de la pratique réglementaire des États membres lorsque des systèmes d'information nouveaux ou modifiés sont introduits sur le marché. L'évaluation devrait porter sur les conséquences potentielles de la technologie proposée sur les données à caractère personnel et, si des risques sont répertoriés, des mesures devraient être prises pour trouver des processus permettant de réduire ces risques, voire mettre au point des solutions de remplacement.

11. Migrations et contrôle aux frontières

Le contrôle aux frontières est un domaine dans lequel les technologies de sécurité et de surveillance sont largement utilisées. Cette utilisation soulève plusieurs préoccupations ayant trait aux incidences sur les droits de l'homme et au principe de solidarité, tant au niveau mondial qu'entre les États membres. Le GEE recommande d'évaluer les systèmes de contrôles aux frontières au regard des critères définis dans le présent avis, à savoir la dignité et les droits de l'homme, la justice, la nécessité, la proportionnalité, l'efficacité, les solutions de remplacement et l'obligation de rendre des comptes.

Conformément aux conclusions du groupe de travail «Article 29», le GEE craint que le régime d'enregistrement des entrées et des sorties (Entry/Exit System — EES) proposé dans le cadre de l'initiative «Frontières intelligentes» n'entraîne des atteintes disproportionnées à la vie privée des individus. Le programme de Stockholm indique qu'avant de créer de nouveaux systèmes, une évaluation de ceux-ci et d'autres programmes existants doit être menée. Le GEE n'est pas convaincu que ce critère soit rempli dans le cas du programme d'enregistrement des entrées et des sorties avec une réflexion d'ensemble prenant en compte les coûts pour la vie privée et la protection des données ainsi que l'effectivité pour le contrôle des frontières et la sécurité publique. Il recommande

donc un moratoire sur l'introduction de l'EES, ce qui permettra, dans l'intervalle, d'évaluer les systèmes existants, comme le système d'information sur les visas, afin de déterminer si les objectifs de l'EES peuvent être atteints de manière proportionnée.

Dans la mesure où les bases de données UE à grande échelle utilisées dans le cadre du contrôle aux frontières peuvent porter atteinte aux droits des ressortissants de l'Union et des pays tiers, dont une proportion non négligeable est particulièrement vulnérable, il convient que leur mise en œuvre soit soumise à une évaluation rigoureuse sur le plan, notamment, de leur impact sur les droits fondamentaux et de leur conformité au principe de limitation de la finalité.

III. Les critères d'évaluation éthiques vont de pair avec les critères d'évaluation juridiques. Ce n'est que si ces deux catégories de critères sont remplies que la **confiance** peut être (ré)instaurée. C'est pourquoi le GEE préconise l'adoption de diverses mesures destinées plus concrètement à renforcer la confiance des citoyens et à représenter l'intérêt qu'ils ont à retrouver/conservé le contrôle de leurs affaires personnelles. Ces mesures ont notamment trait au contrôle, à la répression, à la dénonciation des abus, à l'information du public, à l'éducation, à la formation et à la recherche.

12. Un dispositif de contrôle digne de confiance

Le GEE reconnaît que, pour les questions touchant à la sécurité nationale, il n'est pas toujours possible de garantir la transparence des activités de surveillance. La confiance du public n'en constitue pas moins un élément essentiel de la légitimité des actions menées par l'État pour garantir la sécurité. Le GEE préconise que, sans préjudice du contrôle sous l'autorité d'un juge, les États membres mettent en place des mécanismes à cet effet (ou étendent les mécanismes existants) en chargeant un organisme ou une personne disposant de compétences de contrôle de remplir le rôle de tiers de confiance au nom du public. Ce rôle consisterait notamment à étudier les répercussions de la surveillance publique et privée sur les droits et obligations des citoyens. Dans un souci de transparence et de respect de l'obligation de rendre des comptes, les États membres devraient publier des données agrégées sur le nombre de demandes introduites en vue d'obtenir des compétences de contrôle, sur l'identité des demandeurs et sur les objectifs poursuivis. Les États membres devraient consulter la personne ou l'organisme concernés avant d'introduire des dispositions législatives ayant trait à la surveillance. D'après le GEE, le tiers

RECOMMANDATIONS

de confiance jouerait un rôle décisif en sensibilisant le public et en favorisant le débat concernant les risques et les avantages de la surveillance.

13. Contrôle du respect de la réglementation en matière de protection des données

Le GEE estime que la protection des données prévue par la législation de l'Union est solide, mais qu'elle doit être mise en œuvre au niveau national. Aussi convient-il que les États membres veillent à ce que les autorités chargées de la protection des données jouissent de compétences juridiques suffisantes et disposent de l'expertise technique et des ressources requises pour assurer des niveaux d'application efficaces dans l'ensemble de l'Union.

14. Dénonciation des abus

Il convient que la Commission européenne et les États membres fassent en sorte qu'un mécanisme efficace et complet de protection des lanceurs d'alerte soit mis en place dans les secteurs public et privé. Conformément aux principes formulés par l'organisation Transparency International dans son rapport de 2013 intitulé *Whistleblowing in Europe*, il importe que, dans les situations touchant à la sécurité nationale, des réglementations et des procédures concernant les lanceurs d'alerte existent et soient claires, qu'elles garantissent la confidentialité ou l'anonymat, qu'elles permettent la réalisation, en temps voulu, d'une enquête approfondie et indépendante sur les révélations des lanceurs d'alerte, et qu'elles prévoient des mécanismes transparents et contraignants permettant de donner suite en temps voulu aux plaintes des lanceurs d'alerte victimes de représailles. Lorsque les informations divulguées ont trait à des questions touchant à la sécurité nationale, à des secrets officiels ou militaires, ou à des informations classifiées, il convient d'adopter pour leur communication des procédures et des garanties spéciales tenant compte du caractère sensible de la question en cause, de manière à favoriser un suivi et une résolution au niveau interne et à éviter que des informations ne soient inutilement divulguées à l'extérieur. Ces procédures devraient permettre la divulgation interne, la divulgation à un organe de contrôle autonome et indépendant du point de vue institutionnel et opérationnel, du secteur de la sécurité, ou la divulgation à des autorités disposant d'une habilitation

de sécurité appropriée. La divulgation externe (c'est-à-dire la divulgation aux médias ou à des organisations de la société civile) serait justifiée en dernier recours.

15. Protection intégrée de la vie privée

Les organisations publiques et privées devraient adopter, pour la mise au point des technologies de sécurité et de surveillance, des principes de protection de la vie privée par ou dans la conception (*privacy by/in design*). Les valeurs européennes que sont la dignité, la liberté et la justice doivent être prises en compte avant, pendant et après le processus de conception, de développement et de mise à disposition de ces technologies. Les technologies favorisant la protection de la vie privée devraient être intégrées dès le début du processus, et non rajoutées après la mise en œuvre. Le GEE estime qu'il serait possible, si les ingénieurs, les développeurs et les experts du domaine de la réflexion philosophique et éthique collaboraient dans un cadre interdisciplinaire, de diffuser au sein des organisations une culture dans laquelle le concept de respect de la vie privée serait compris et mis en pratique. L'introduction, dans le cursus des étudiants et des diplômés en ingénierie et en informatique, mais aussi au niveau de l'éducation et de la formation professionnelles, de cours et de formations aussi bien théoriques que pratiques sur les aspects éthiques pourrait contribuer à une meilleure compréhension des approches fondées sur la protection de la vie privée par ou dans la conception dans le domaine des technologies de sécurité et de surveillance.

16. Comprendre le concept de respect de la vie privée et en apprécier la valeur

Le respect de la vie privée n'est pas un concept statique, et il faudra, pour adopter des mesures appropriées garantissant la protection de l'intimité physique des individus et des renseignements personnels les concernant, parvenir à mieux comprendre la signification et la valeur que les Européens attachent à ce concept. À cette fin, il convient que l'Union dégage des fonds en vue de la réalisation de travaux de recherche qui permettront d'examiner et d'analyser comment les Européens appréhendent les questions ayant trait à la sécurité et à la surveillance et quel rôle ils entendent jouer dans ce cadre.

Recommendations

The EGE has been asked to formulate an opinion on the ethical implications of security and surveillance technologies. This is a timely but difficult task, as these technologies represent very different purposes, are performed by different actors, entail different stages and forms of intrusion on human rights and lead to different uses.

The increasing availability of large amounts of information and the growth of communication networks have been major factors in the globalisation of the 20th century. Another feature of a globalised world is the feeling of insecurity, a lack of trust and a low tolerance of risk. Shootings in schools, cinemas and shopping centres, explosives on the underground, trains and aeroplanes, abduction of children, beatings and robberies of older people have served to increase our sense of feeling unsafe in our own communities. This perception persists despite the fact that all objective measures tell us that there has never been a safer time to live. The desire of Governments to respond to the perception of a feeling of insecurity amongst its citizens has undoubtedly driven securitization approaches adopted in Europe and elsewhere.

Security, employed in the rather narrow sense, involves protection from physical harm or the threat of harm and is a fundamental component of well-being. Through the social contract, States have committed to provide security for the citizenry in exchange for the power to curtail individual liberty. This is however, but one aspect of the security paradigm. Protecting physical integrity is necessary but not sufficient. Security needs to be viewed in the broader context which encompasses both human and societal security. This requires us to expand our considerations from the role of the State to that of individuals, communities and commercial entities. Europe is a community of shared values where we strive to safeguard dignity, autonomy, freedom and justice through our Human Rights Framework. This provides an environment in which the person can flourish through creativity, innovation, development of strong personal relationship with others and their contribution to their communities. Education, health, democracy, environment and equality are all essential elements in realising the goal of a secure Europe.

The rather limited approach to achieving security, most especially when it comes to the narrow interpretation of state security, has been to engage in the narrative of trade-offs, the classic example being the trade-off between freedom, often embodied as privacy, and

security. While a proper balance needs to be struck between competing principles or values when they come into conflict, there are some core principles such as human dignity which simply cannot be traded away. This requires us to move beyond the rhetoric of trade-offs and into a more nuanced approach where security technologies and measures are assessed on the basis of proportionality and effectiveness and rights are prioritised rather than traded.

The EGE recognises that an entirely legitimate manifestation of state power in a democratic society is to have agencies that according to strict legal limitations are permitted to use surveillance as a means of safeguarding the security of its citizens. The EGE would also assert that elements of secrecy and discretion are an intrinsic aspect of the **dignity** of human life. Infringement by a public authority of a person's right to privacy must be **justified** and should be subject to judicial oversight. Surveillance must be **necessary** and **proportionate** in order to ensure an appropriate connection between the actions taken and the objectives achieved. A key element in assessing proportionality is the **effectiveness** of the intervention and effectiveness must be reviewed regularly. Powers to surveil should be granted for a defined purpose and for a defined period of time. **Alternatives** capable of achieving the same goal should be examined and documented and the least intrusive method should be selected. **Accountability** is a necessary pre-requisite for public surveillance thus, it should be clear that surveillance is being undertaken for appropriate reasons and in conformance with publicly available codes of practice. Security and surveillance technologies must be applied with as great a degree of **transparency** as possible, with legitimate exceptions explicitly determined in the legal system. Private and or commercial organisations involved in surveillance should also be bound by the aforementioned criteria.

In these regards, discrimination is an important area of concern. We need to be mindful of the possible unanticipated effects of ubiquitous surveillance. It corrals individuals towards conforming to forms of normality (as normativity), thus behaving differently and further strengthening that norm, and thus in turn giving rise to an impoverished — if not neutered — society (where diversity, creativity and even cohesiveness have been rooted out). Discrimination may concern the specific targeting and/or surveillance of minorities, and the EGE calls for action where and when this is the case in EU Member States. Furthermore, discrimination relates to

RECOMMENDATIONS

issues of profiling as well as of stigmatization. Concerning profiling, it should be recognized that it takes many forms, from opt in/out programs (such as Global Entry) to ‘face crime’ and face recognition (and other biometrical systems), through to the profiling of all through advanced mass surveillance. Concerning stigmatization, while it is clear that it (and its correlate, humiliation) must be avoided, the role played by the increasingly pervasive use of algorithms as part of security and surveillance assemblages is particularly alarming in that regard. These algorithms can obfuscate or confiscate ethical reflexivity and justification of choices, resulting in in-built profiling or ‘stigmatization by design’. In doing so they also risk perfecting the normality and compliance alerted to above, by black-boxing selection processes, removing them from human intervention and understanding. In this regard the EGE is fully aware of the risk of instrumentalisation of ethics councils and cognate bodies in these processes of normalisation pertaining to new technologies. Indeed the EGE is fully aware of the difficulties inherent to the embracing from an ethical perspective of the topic of security and surveillance technologies without this being understood as a form of overall condoning. It has chosen not to shy away from those difficulties but to confront them head-on in this Opinion.

Based on these considerations the EGE agrees on the following recommendations in the field of security and surveillance technologies:

I. Technologies with the potential to intrude into the privacy of individuals *and* to which they cannot consent (or cannot opt out), require specific justification. The EGE calls for a *case by case justification* for these measures.

1. Accountability

Member States need to ensure that those granted with powers to surveil the private sphere of citizens are acting in the public interest and are accountable for their actions. Where the State delegates security and/or surveillance tasks to private companies, they are bound by the same legal and ethical obligations and Member States should put in place mechanisms to monitor compliance with such obligations.

2. Judicial oversight

Member States must have a system of judicial oversight for surveillance carried out by public authorities in order to investigate crime. The individual should be informed post-hoc that they have been the subject of surveillance provided that no investigation is prejudiced as a result. An individual should have the opportunity to seek redress from

the Courts if they have been the subject of unlawful surveillance.

3. Towards a common understanding of national security

The shared European values enshrined in the EU Charter of Fundamental Rights represent the normative framework on which a common ethical understanding of national security could be built.

- a) While recognising that national security is legitimately placed at the heart of national interests and is a competence of Member States, the EGE recommends that EU institutions in conjunction with Member States should find ways to establish such a common understanding of national security.
- b) The EGE also recommends that Member States should establish procedural means to keep other Member States appropriately informed of extra jurisdictional intelligence activities in order to preserve trust between partners.
- c) Member States should not in the name of national security surveil other Member States for commercial advantage, because it conflicts with the EU objective of achieving a single European market.

4. Drones

The rapid development and increased deployment of drones by Member States in military, civilian and commercial contexts has not been accompanied by the necessary governance and oversight arrangements, which remain fragmented at best. For civilian and commercial uses, the EU lacks a comprehensive legal framework for the development, acquisition, use and export of drones. The EGE welcomes actions already taken by the European Commission in the area of Remotely Piloted Aircraft Systems (RPAS) integration in the EU aviation system (including wide ranging consultation and the publication of a roadmap). The inclusion from the outset, of a consideration of societal implications of drone deployment is to be commended.

- a) Given the recent EU commitment for improved coordination amongst Member States in the development and acquisition of drones, the EGE recommends that this cooperation be extended to the generation of common standards and a regulatory framework governing the civilian

and commercial use of drones within the EU. Particular attention should be paid to an evaluation of existing EU data protection and privacy frameworks, in order to assess if the current regulatory regime is fit for purpose in the context of Remotely Piloted Aircraft Systems integration in European airspace.

- b) Member States must ensure that national policies regarding use of drones domestically (i.e. within national borders), in the public sphere, do not violate the human rights of those subject to drone operations. Domestic use of drones should be subject to an authorisation and proper oversight to ensure safety and prevent misuse. Further, those seeking authorisation for the use of surveillance drones must demonstrate that the proposed use is justified, necessary and proportionate. The EGE also recommends that policies and procedures governing the domestic use of drones for the purpose of surveillance should be publically available in the interests of transparency, a prerequisite of public trust.
- c) The EGE draws attention to the grave ethical implications of the military use of drones as well as of automated warfare, and acknowledges the European Parliament resolution on the use of armed drones of 25 February 2014. The EGE calls for greater transparency and accountability on the part of Member States that operate drones for military purposes. To that end, Member States must disclose the legal basis, scope, and limits of any lethal drone strikes and there must be scrutiny that existing legal frameworks that apply to traditional armed conflicts are not being violated. Information on the number of civilians and non-civilians killed in drone strikes should also be publicly available. Further, the EGE strongly advocates research to address the ethical implications of lethal drone strikes and their compatibility or otherwise with just war theory. Moreover, research is required on the role of moral agency where drone operators are situated remotely as well as in relation to the development of autonomous drones.

II. Regarding surveillance technologies, the burden of proof should lie with states and/or companies, who have to demonstrate *publicly and transparently*, before introducing surveillance options,

- that they are **necessary**

- that they are **effective**
- that they respect **proportionality** (e.g. purpose limitation)
- that there are no better **alternatives** that could replace these surveillance technologies

These criteria must then also be subjected to **post factum assessment**, either on the level of normal political analyses, or through Member States policies to do so.

Furthermore:

Accountability means that individuals have the right to be informed about surveillance technologies — even though in some cases this information may only be provided ex post;

Transparency with respect to economic interests must be ensured at all times.

5. Personal data

The EGE affirms that the purpose limitation principle as regards personal data be the standard for both public and private organisations. Personal data should only be collected for a specific and legitimate purpose. As far as possible data should be anonymised and greater use should be made of encryption which can serve to enhance both privacy and security. Data sharing by default is to be avoided and users should be allowed to control (e.g. through access to privacy settings) and change information held by organisations about them. Profiling of individuals for commercial purposes should be subject to the individual's explicit consent. Information should be available by commercial organisations in relation to *what data* are going to be collected, *by whom*, *for what purpose*, *for how long* and if data collected will be linked with other data sources.

6. Public awareness of data policies

The EGE reaffirms its view that there needs to be greater clarity for the public in relation to how, why and for what purpose their personal information is managed, shared and protected. Public authorities as well as corporate actors must make their policies in that regard publicly available. The EU and Member States should seek to foster public knowledge, awareness and debate on the implications for individuals and wider society of the use of security and surveillance technologies. Education programs should start at school level and should provide

RECOMMENDATIONS

information and tools for citizens to safeguard their data in the digital environment.

7. Big data

The EGE notes the shift towards collection and correlation of large datasets, so called “big data”. While the EGE recognises the potential value of such datasets, we are concerned that without proper attention, the principle of purpose limitation at the core of data protection will be undermined. Thus, the EGE urges public authorities and private organisations to engage in purposeful ethical inquiry to inform and align their actions with shared European values of dignity, privacy and autonomy. The EGE recommends that the EU develop a code of conduct for big data analytics that would guide organisations with the process.

8. Algorithms

In the context of security and surveillance technologies, it is important to note that algorithms are necessarily selective in their design and are as subject to bias as the humans which program them. Underlying algorithms and their parameters are ethical assumptions and these should be made explicit as a mandatory requirement. Moreover, algorithms are not infallible and the data generated are contingent on the choice and quality of data input, which in the view of the EGE should be continually examined and validated. Furthermore, education on the ethical aspects in the design of algorithms should be included in the training of developers.

9. e-Privacy

The EGE recommends that the EC give consideration to revising the e-Privacy Directive, the scope of which currently encompasses electronic communications. Given the explosion of digital interfaces since the introduction of the Directive, the EGE considers it appropriate that VoIP — Voice over Internet Protocol, indeed IP communications, broadband communications — products and also corporate private networks would be included in the remit of any revised Directive.

10. Privacy Impact Assessment

Privacy Impact Assessment procedures must form part of regulatory practice in Member States when new or modified information systems which process personal data are being introduced to the market. The assessment should address the potential implications of the proposed technology for personal data and if risks are identified, measures should be

taken to identify processes to mitigate the risk or indeed alternatives to that which is proposed.

11. Migration and border control

Border control is one area where security and surveillance technologies are broadly applied. This raises several concerns as regards the impact on human rights and the solidarity principle, both globally and among EU Member States. The EGE recommends to evaluate the Border Control Systems in view of the criteria set up in this Opinion, namely dignity and human rights, justice, necessity, proportionality, effectiveness, alternatives, and accountability.

In line with the findings of the Article 29 working party, the EGE is concerned that the Entry/Exit System (EES) proposed under the Smart Borders Initiative involves a disproportionate intrusion into individual’s privacy. The Stockholm programme notes that before creating new systems, an evaluation of these and other existing systems should be made. The EGE is not convinced that this criterion has been met in the case of the Entry Exit System with a thorough reflection taking into account the costs for privacy and data protection and the effectiveness for border control and public security. It therefore recommends a moratorium on the introduction of the EES, while existing systems such as the Visa Information System are evaluated to see if the objectives of the EES can be met in a proportionate manner.

Acknowledging that large-scale EU databases used for border control purposes can pose risks to the rights of EU and non-EU nationals, a proportion of whom are particularly vulnerable, the implementation of these databases should be subject to a rigorous evaluation with particular attention paid to their impact on fundamental rights and adherence to the principle of purpose limitation.

III. Ethical and legal assessment criteria go hand in hand. They can (re-)build **trust** only together, and therefore the EGE recommends several different measures intended more concretely to build up trust and represent citizens’ interests in having/maintaining control over their personal affairs. These include issues of oversight, enforcement, whistleblowing, public information, education, training and research.

12. Trustworthy oversight

The EGE recognises that in matters of national security it is not always possible to be transparent regarding surveillance activities. Nonetheless, public

trust is crucial to the legitimacy of States actions in the pursuit of security. To that end, the EGE recommends that, without prejudice to judicial oversight, Member States establish or expand existing mechanisms in the form of a body or person vested with powers of oversight to act as a trusted third party on behalf of the public. The role of such an entity would include monitoring the effects of both public and private surveillance on the rights and duties of citizens. Aggregate information on the number of requests made for surveillance powers, by whom and for what purpose should be published by Member States thereby ensuring transparency and accountability. Member States should consult such a body or person in advance of introducing legislation pertaining to surveillance. The EGE envisages that the trusted third party would have a key role in raising public awareness and stimulating debate with regard to the risks and benefits of surveillance.

13. Data protection enforcement

The EGE is of the view that the protection of data enshrined in EU law is robust but requires to be enforced at the national level. Member States should therefore ensure that data protection authorities have sufficient legal powers, technical expertise and resources to ensure effective levels of enforcement across the European Union.

14. Whistleblowing

The European Commission and Member States should ensure that an effective and comprehensive whistle-blower protection mechanism is established in the public and private sectors. In line with the Transparency International principles as articulated in the 2013 *Whistleblowing in Europe* Report, in situations where national security is involved, whistle-blower regulations and procedures should be present and clear; maintain confidentiality or anonymity; ensure thorough, timely and independent investigations of whistleblowers' disclosures; and have transparent, enforceable and timely mechanisms to follow up on a complaint of a whistleblower in relation to retaliation. Where a disclosure concerns matters of national security, official or military secrets, or classified

information, special procedures and safeguards for reporting that take into account the sensitive nature of the subject matter should be adopted in order to promote successful internal follow-up and resolution and to prevent unnecessary external exposure. These procedures should permit internal disclosures, disclosure to an autonomous oversight body that is institutionally and operationally independent from the security sector, or disclosures to authorities with the appropriate security clearance. External disclosure (that is, to the media or civil society organisations) would be justified as a last resort.

15. Designing privacy

Public and private organisations should adopt privacy-by and privacy-in design principles for development of security and surveillance technologies. The European values of dignity, freedom and justice must be taken into account before, during and after the process of design, development and delivery of such technologies. Privacy enhancing technologies should be integrated from the outset and not bolted on following implementation. In the view of the EGE, instilling a culture in organisations, where privacy is understood and reflected in practice, can be achieved through engineers, developers and experts in philosophical and ethical reflection working together in an interdisciplinary way. The introduction of ethical courses and training both on a theoretical and practical level in engineering and informatics for undergraduate and post-graduate students, but also during vocational education and training could improve the grasp of privacy by and in design approaches in the field of security and surveillance technologies.

16. Understanding and valuing privacy

Privacy is not a static concept and a fuller understanding of how European citizens conceptualise and value privacy is required, if appropriate steps are to be taken to safeguard physical and informational privacy. To this end, the EU should make funds available for research to examine and analyse how citizens consider, and cultivate their involvement in, issues related to security and surveillance.

Empfehlungen

Die EGE wurde gebeten, eine Stellungnahme zu den ethischen Implikationen der Sicherheits- und Überwachungstechnologien zu formulieren. Dies ist eine zeitgemäße, aber schwierige Aufgabe, da diese Technologien sehr unterschiedliche Zwecke haben, von unterschiedlichen Akteuren verwendet werden, verschiedene Stufen und Formen von Gefährdungen der Menschenrechte mit sich bringen und zu unterschiedlichen Nutzungsformen führen.

Die zunehmende Verfügbarkeit von großen Informationsmengen und die steigende Anzahl von Kommunikationsnetzen sind wichtige Faktoren, die die Globalisierung des 20. Jahrhunderts mit sich gebracht hat. Weitere Merkmale einer globalisierten Welt sind das Unsicherheitsgefühl, mangelndes Vertrauen und eine geringe Risikotoleranz. Schießereien in Schulen, Kinos und Einkaufszentren, Sprengstoffanschläge in U-Bahnen, Zügen und Flugzeugen, Kindesentführungen, Prügelattacken und Raubüberfälle auf ältere Menschen haben dazu beigetragen, dass unser Unsicherheitsgefühl auch in unserem eigenen Umfeld stärker geworden ist. Auch wenn alle objektiven Bewertungen zeigen, dass es nie eine Zeit gab, in der das Leben sicherer war als heute, bleibt dieses Unsicherheitsgefühl bestehen. Der Wunsch der Regierungen, auf dieses von den Bürgern wahrgenommene Unsicherheitsgefühl zu reagieren, hat zweifellos zu einer Ausweitung sicherheitspolitischer Maßnahmen in Europa und anderswo geführt.

Sicherheit, im eher engen Wortsinn verwendet, beinhaltet den Schutz vor körperlichen Schäden oder der Androhung von Schaden und ist ein wesentlicher Bestandteil des Wohlbefindens. Durch den Gesellschaftsvertrag haben sich Staaten verpflichtet, im Austausch für das Zugeständnis, die Freiheit des Einzelnen zu beschneiden, für die Sicherheit der Bürger zu sorgen. Dies ist jedoch nur ein Aspekt des Sicherheitsparadigmas. Der Schutz der körperlichen Unversehrtheit ist notwendig, aber nicht ausreichend. Sicherheit muss in einem breiteren Kontext betrachtet werden, der sowohl menschliche als auch gesellschaftliche Sicherheit umfasst. Dies erfordert, dass wir unsere Überlegungen von der Rolle des Staates zu der von Einzelpersonen, Gesellschaftsgruppen und Wirtschaftsunternehmen erweitern. Europa ist eine Wertegemeinschaft, in der wir uns bemühen, Würde, Autonomie, Freiheit und Gerechtigkeit durch Menschenrechte zu schützen. Diese schaffen ein Umfeld, in dem sich der Einzelne durch Kreativität, Innovation, Entwicklung von starken persönlichen Beziehungen zu anderen und ihrem Beitrag

zur Gesellschaft entfalten kann. Bildung, Gesundheit, Demokratie, Umwelt und Gleichheit sind wesentliche Bausteine eines sicheren Europas.

Ein eher begrenzter Ansatz zur Verwirklichung von Sicherheit, ganz besonders, wenn es um die enge Auslegung dieses Begriffs als Staatssicherheit geht, ist es, Kompromisse zu schließen. Das klassische Beispiel dafür ist der Kompromiss zwischen Freiheit, oft als Datenschutz bzw. Privatsphäre bezeichnet, und Sicherheit. Eine ausgewogene Balance zwischen konkurrierenden Prinzipien oder Werten muss hergestellt werden, wenn diese in Konflikt geraten. Es gibt aber einige Grundprinzipien wie die Menschenwürde, die in keinem Fall geopfert werden dürfen. Dies erfordert, dass wir über die Rhetorik von Kompromissen hinausgehen und eine differenziertere Vorgehensweise anstreben, bei der Sicherheitstechnologien und Maßnahmen auf der Grundlage der Verhältnismäßigkeit und Wirksamkeit geprüft und Rechte priorisiert und nicht geopfert werden.

Die EGE erkennt an, dass die Staatsgewalt in einer demokratischen Gesellschaft in völlig legitimer Weise Einrichtungen dazu einsetzt, nach strengen gesetzlichen Vorschriften die Überwachung als Mittel zur Wahrung der Sicherheit ihrer Bürger zu nutzen. Die EGE vertritt auch die Auffassung, dass Geheimhaltung und Diskretion ein wesentlicher Teil der **Würde** des menschlichen Lebens sind. Die Verletzung des Rechts einer Person auf Privatsphäre durch eine Behörde muss **begründet** werden und gerichtlicher Aufsicht unterliegen. Die Überwachung muss **notwendig** und **verhältnismäßig** sein, um eine entsprechende Beziehung zwischen den ergriffenen Maßnahmen und den erreichten Zielen zu gewährleisten. Ein Schlüsselement für die Beurteilung der Verhältnismäßigkeit ist die **Wirksamkeit** des jeweiligen Eingriffs. Diese Wirksamkeit muss regelmäßig überprüft werden. Die Befugnis zur Überwachung muss für einen bestimmten Zweck und für einen bestimmten Zeitraum gewährt werden. **Alternativen**, die das gleiche Ziel erreichen können, müssen geprüft und dokumentiert werden, um die am wenigsten intrusive Methode zu wählen. **Rechenschaftspflicht** ist eine notwendige Voraussetzung für die öffentliche Überwachung. Folglich muss die Überwachung offensichtlich aus angemessenen Gründen und in Übereinstimmung mit öffentlich zugänglichen Verfahrensregeln erfolgen. Sicherheits- und Überwachungstechnologien müssen so **transparent** wie möglich angewendet werden, wobei legitime Ausnahmen ausdrücklich im Rechtssystem bestimmt werden. An der Überwachung beteiligte private oder

EMPFEHLUNGEN

gewerbliche Organisationen müssen ebenfalls an die oben genannten Kriterien gebunden sein.

In dieser Hinsicht ist die Diskriminierungsgefahr ein wichtiger und problematischer Aspekt. Wir müssen uns über die möglichen unerwarteten Auswirkungen der allgegenwärtigen Überwachung bewusst sein. Sie zwingt den Einzelnen dazu, sich mit entsprechenden Formen der Normalität (wie Normativität) abzufinden, sich folglich anders zu verhalten und diese Norm weiter zu stärken, was wiederum zu einer verarmten — wenn nicht sogar kastrierten — Gesellschaft führt (in der Vielfalt, Kreativität und sogar Zusammenhalt ausgemerzt wurden). Die Diskriminierung kann in Form eines speziellen Abzielens auf bestimmte Minderheiten oder ihre Überwachung auftreten, und die EGE fordert Abhilfemaßnahmen, wenn es in den EU-Mitgliedstaaten zu solchen Fällen kommt. Weiterhin kann Diskriminierung Profiling und Stigmatisierung betreffen. Es muss anerkannt werden, dass Profiling vielfältige Formen annehmen kann, von Programmen, bei denen man sich selbst für die Teilnahme entscheiden kann (wie das Global-Entry-Programm), bis hin zu „Facecrime“ und Gesichtserkennung (sowie anderen biometrischen Systemen) und zur Profiling aller Bürger durch Massenüberwachung. Stigmatisierung (und ihre Entsprechung, die Demütigung) müssen selbstverständlich vermieden werden, doch die Rolle, die die zunehmend allgemeine Verwendung der Algorithmen als Teil der Ansammlung von Sicherheits- und Überwachungsdaten spielt, ist in dieser Hinsicht besonders alarmierend. Diese Algorithmen können die ethische Reflexivität und Rechtfertigung von Entscheidungen verschleiern oder für sich einnehmen, was zu „In-built-Profiling“ oder „Stigmatisierung by Design“ führt. Dabei riskieren sie auch die Perfektionierung der Normalität und Compliance, auf die oben hingewiesen wurde, durch unübersichtliche Auswahlprozesse, damit menschliche Eingriffe und Verständnis ferngehalten werden. Die EGE ist sich in dieser Hinsicht der Gefahr der Instrumentalisierung von Ethikräten und verwandten Einrichtungen bei diesen Prozessen der Normalisierung in Bezug auf neue Technologien vollständig bewusst. Denn die EGE ist sich auch der Schwierigkeiten, die darin liegen, die Sicherheits- und Überwachungstechnologien aus ethischer Sicht zu betrachten, ohne dass dies als eine Form des stillschweigenden Duldens verstanden wird, vollumfänglich bewusst. Die EGE ist entschlossen, diese Schwierigkeiten nicht zu scheuen, sondern sie in dieser Stellungnahme direkt anzugehen.

Die EGE stimmt, basierend auf diesen Überlegungen, den folgenden Empfehlungen auf dem Gebiet der Sicherheits- und Überwachungstechnologien zu:

I. Technologien, die möglicherweise die Privatsphäre von Personen verletzen könnten, die nicht die Möglichkeit haben, ihr Einverständnis zu erklären (oder die nicht ablehnen können), erfordern eine spezifische Rechtfertigung. Die EGE fordert jeweils Begründungen für jeden Einzelfall für diese Maßnahmen.

1. Rechenschaftspflicht

Die Mitgliedstaaten müssen sicherstellen, dass Personen oder Einrichtungen, die berechtigt sind, die Privatsphäre der Bürger zu überwachen, im öffentlichen Interesse handeln und Rechenschaft über ihr Handeln ablegen müssen. Wenn der Staat Sicherheits- und/oder Überwachungsaufgaben an private Unternehmen delegiert, sind diese an die gleichen rechtlichen und ethischen Verpflichtungen gebunden. Die Mitgliedstaaten müssen gewährleisten, dass die Einhaltung dieser Verpflichtungen überwacht wird.

2. Gerichtliche Kontrolle

Die Mitgliedstaaten müssen über ein System der gerichtlichen Kontrolle von behördlichen Überwachungsmaßnahmen bei strafrechtlichen Ermittlungen verfügen. Der Einzelne muss nachträglich informiert werden, dass er überwacht wurde, vorausgesetzt, dass dadurch die Ermittlung nicht beeinträchtigt wird. Der Einzelne muss die Möglichkeit haben, auf dem Gerichtsweg Entschädigung zu beantragen, wenn er Objekt einer rechtswidrigen Überwachung wurde.

3. Entwicklung eines gemeinsamen Verständnisses von nationaler Sicherheit

Die in der Charta der Grundrechte verankerten gemeinsamen europäischen Werte stellen den normativen Rahmen dar, auf dem ein gemeinsames ethisches Verständnis der nationalen Sicherheit aufgebaut werden kann.

- a) Es wird anerkannt, dass die nationale Sicherheit legitim im Mittelpunkt der nationalen Interessen steht und in die Zuständigkeit der Mitgliedstaaten fällt. Die EGE empfiehlt jedoch, dass die EU-Organe in Zusammenarbeit mit den Mitgliedstaaten auf ein gemeinsames Verständnis für die nationale Sicherheit hinwirken.
- b) Die EGE empfiehlt auch, dass die Mitgliedstaaten Verfahren einrichten, um andere Mitgliedstaaten entsprechend über nachrichtendienstliche Tätigkeiten außerhalb ihres Hoheitsgebiets zu informieren, um das Vertrauen zwischen den Partnern zu bewahren.

- c) Die Mitgliedstaaten dürfen nicht im Namen der nationalen Sicherheit andere Mitgliedstaaten überwachen, um kommerzielle Vorteile zu erzielen, weil dies im Widerspruch zu dem Ziel der EU steht, einen einheitlichen europäischen Markt zu schaffen.

4. Drohnen

Die rasante Entwicklung und der vermehrte Einsatz von Drohnen in militärischen, zivilen und wirtschaftlichen Zusammenhängen durch die Mitgliedstaaten wurden nicht von den notwendigen Entscheidungsstrukturen und Kontrollregelungen begleitet, die derzeit bestenfalls fragmentarisch sind. Der EU fehlt ein umfassender Rechtsrahmen für die Entwicklung, den Erwerb, den Einsatz und den Export von Drohnen für den zivilen und wirtschaftlichen Einsatz. Die EGE begrüßt die bereits von der Europäischen Kommission getroffenen Maßnahmen hinsichtlich der Integration ferngesteuerter Luftfahrzeuge (Remotely Piloted Aircraft Systems, RPAS) in das EU-Luftverkehrssystem (einschließlich umfassende Konsultation und Veröffentlichung eines Fahrplans). Die Einbeziehung der Betrachtung der gesellschaftlichen Auswirkungen auf den Drohneneinsatz von Anfang an ist zu loben.

- a) Angesichts des jüngsten Engagements der EU für eine verbesserte Koordinierung zwischen den Mitgliedstaaten bei der Entwicklung und Beschaffung von Drohnen empfiehlt die EGE, dass diese Zusammenarbeit auf die Erzeugung von gemeinsamen Normen und rechtlichen Rahmenbedingungen für die zivile und kommerzielle Nutzung von Drohnen in der EU ausgedehnt wird. Besonderes Augenmerk muss auf eine Bewertung der bestehenden EU-Datenschutzregelungen gerichtet werden, um beurteilen zu können, ob die derzeitigen Rechtsvorschriften im Hinblick auf die Integration ferngesteuerter Luftfahrzeuge (Remotely Piloted Aircraft Systems, RPAS) in den europäischen Luftraum ihren Zweck erfüllen.
- b) Die Mitgliedstaaten müssen dafür sorgen, dass die nationale Politik in Bezug auf den Einsatz von Drohnen im Inland (d. h. innerhalb der nationalen Grenzen), im öffentlichen Raum, nicht die Menschenrechte der Personen verletzen, die von den Drohneneinsätzen betroffen sind. Die Nutzung von Drohnen auf dem eigenen Staatsgebiet muss einer Zulassung und geeigneten Aufsicht unterliegen, um die Sicherheit zu

gewährleisten und Missbrauch zu verhindern. Außerdem müssen Personen, die Genehmigungen für den Einsatz von Aufklärungsdrohnen beantragen, nachweisen, dass die beabsichtigte Nutzung gerechtfertigt, notwendig und verhältnismäßig ist. Die EGE empfiehlt auch, dass die Regelungen und Verfahren für den Einsatz von Drohnen im Inland für Überwachungszwecke im Interesse der Transparenz, einer Voraussetzung für das Vertrauen der Öffentlichkeit, öffentlich zugänglich sein müssen.

- c) Die EGE lenkt die Aufmerksamkeit auf die gravierenden ethischen Auswirkungen der militärischen Nutzung von Drohnen sowie der automatisierten Kriegsführung und begrüßt die Entschließung des Europäischen Parlaments zum Einsatz von bewaffneten Drohnen vom 25. Februar 2014. Die EGE fordert mehr Transparenz und Verantwortlichkeit auf Seiten der Mitgliedstaaten, die Drohnen für militärische Zwecke einsetzen. Zu diesem Zweck müssen die Mitgliedstaaten die rechtliche Grundlage, den Umfang und Grenzen aller tödlichen Drohnenangriffe offenlegen, und es muss eine Untersuchung stattfinden, dass die bestehenden für traditionelle bewaffnete Konflikte geltenden rechtlichen Rahmenregeln nicht verletzt werden. Informationen über die Anzahl von Zivilisten und Nicht-Zivilisten, die bei Drohnenangriffen getötet werden, müssen ebenfalls öffentlich zugänglich gemacht werden. Ferner befürwortet die EGE ausdrücklich Untersuchungen, um die ethischen Implikationen der tödlichen Drohnenangriffe und deren Kompatibilität oder anderweitige Aspekte mit der Theorie des gerechten Krieges zu prüfen. Darüber hinaus sind Studien zur Rolle des moralischen Handelns erforderlich, wenn Drohnen ferngesteuert betrieben werden. Dasselbe gilt auch für die Entwicklung von Drohnen mit Selbststeuerung.

II. In Bezug auf Überwachungstechnologien muss die Beweislast bei den Staaten und/oder Unternehmen liegen, die *öffentlich und transparent* Nachweise erbringen müssen, bevor sie Überwachungsaktionen durchführen,

- dass diese **notwendig** sind,
- dass diese **wirksam** sind,

EMPFEHLUNGEN

- dass diese **verhältnismäßig** sind (z. B. Zweckbindung),
- dass es keine besseren **Alternativen** gibt, die diese Überwachungstechnologien ersetzen könnten.

Die Einhaltung dieser Kriterien ist einer **nachträglichen Beurteilung** zu unterziehen. Dies muss entweder auf der Ebene der normalen politischen Analysen oder durch die diesbezüglichen Regelungen der Mitgliedstaaten geschehen.

Außerdem:

Rechenschaftspflicht bedeutet, dass alle Menschen das Recht haben, über Überwachungstechnologien informiert zu werden — auch wenn diese Information in einigen Fällen erst nachträglich zur Verfügung gestellt wird.

Transparenz in Bezug auf die wirtschaftlichen Interessen muss jederzeit gewährleistet werden.

5. Personenbezogene Daten

Die EGE betont, dass die Zweckbindung hinsichtlich der personenbezogenen Daten die Norm für öffentliche wie private Organisationen zu sein hat. Personenbezogene Daten sollten nur für einen spezifischen und rechtmäßigen Zweck gesammelt werden. So weit wie möglich sollten Daten anonymisiert und die Verschlüsselung stärker genutzt werden, um sowohl den Datenschutz als auch die Sicherheit zu erhöhen. Standardmäßige Datenfreigabe ist zu vermeiden, und Nutzer sollten die Möglichkeit haben (z. B. durch den Zugang zu Datenschutzeinstellungen), Informationen, die Organisationen über sie besitzen, zu kontrollieren und zu berichtigen. Das Profiling von Personen für kommerzielle Zwecke muss der ausdrücklichen Zustimmung der Betroffenen unterliegen. Informationen von kommerziellen Unternehmen sollten im Hinblick darauf zur Verfügung stehen, wofür Daten gesammelt werden, von wem, zu welchem Zweck, wie lange und ob die Daten, die gesammelt werden, mit anderen Datenquellen verknüpft werden.

6. Das öffentliche Bewusstsein für Datenrichtlinien

Die EGE bekräftigt ihre Auffassung, dass die Öffentlichkeit besser darüber aufgeklärt werden muss, wofür, wie, warum und zu welchem Zweck personenbezogene Daten verarbeitet, weitergegeben und geschützt werden. Behörden und

Unternehmen müssen ihre Regelungen in diesem Zusammenhang öffentlich zugänglich machen. Die EU und die Mitgliedstaaten müssen sich bemühen, die Öffentlichkeit über die Folgen der Verwendung von Sicherheits- und Überwachungstechnologien für den Einzelnen und die Gesellschaft aufzuklären, das Bewusstsein für diese Problematik zu schärfen und die Debatte zu diesem Thema zu fördern. Aufklärungsprogramme müssen bereits in der Schule beginnen und Informationen und Instrumente für die Bürger bereitstellen, damit diese ihre Daten in der digitalen Umwelt schützen können.

7. Big Data

Die EGE hat festgestellt, dass mehr und mehr dazu übergegangen wird, große Datenmengen, sogenannte „Big Data“, zu sammeln und miteinander in Beziehung zu setzen. Während die EGE den potenziellen Wert solcher Datensätze anerkennt, sind wir besorgt, dass ohne angemessene Sorgfalt im Umgang mit diesen Daten der Grundsatz der Zweckbindung als Mittelpunkt des Datenschutzes untergraben wird. So fordert die EGE Behörden und private Organisationen dringend auf, aussagekräftige ethische Untersuchungen anzustellen, um ihr Handeln mit den gemeinsamen europäischen Werten der Würde, Privatsphäre und Autonomie zu durchdringen und in Einklang zu bringen. Die EGE empfiehlt, dass die EU einen Verhaltenskodex für die Big-Data-Analyse entwickelt, der Unternehmen bei diesem Prozess unterstützen würde.

8. Algorithmen

Im Kontext der Sicherheits- und Überwachungstechnik muss beachtet werden, dass Algorithmen in ihrer Konstruktion notwendigerweise selektiv sind und von den Menschen, die sie programmieren, beeinflusst werden können. Algorithmen und ihren Parametern liegen ethische Annahmen zugrunde, die obligatorisch explizit gemacht werden sollten. Außerdem sind Algorithmen nicht unfehlbar, und die generierten Daten hängen von der Auswahl und Qualität der Dateneingabe ab, die nach Ansicht der EGE ständig geprüft und validiert werden sollte. Darüber hinaus sollte die Aufklärung über die ethischen Aspekte bei der Gestaltung von Algorithmen in die Ausbildung von Entwicklern aufgenommen werden.

9. Datenschutz im Bereich der elektronischen Kommunikation (e-Privacy)

Die EGE empfiehlt der Kommission, in Erwägung zu ziehen, die E-Privacy-Richtlinie zu überarbeiten, die derzeit den Rechtsrahmen für den Umgang

mit elektronischer Kommunikation darstellt. Angesichts des rapiden Anstiegens der Zahl der digitalen Schnittstellen seit der Einführung der Richtlinie hält es die EGE für angemessen, dass Produkte, die VoIP (Voice over Internet Protocol), IP-Kommunikation oder Breitbandkommunikation verwenden, und auch private Unternehmensnetze in den Geltungsbereich einer überarbeiteten Richtlinie einbezogen werden.

10. Datenschutz-Folgenabschätzung

Die Mitgliedstaaten müssen in ihre Prüfungs- und Regulierungstätigkeit Verfahren zur Datenschutz-Folgenabschätzung einbeziehen, wenn neue oder geänderte Informationssysteme, die personenbezogene Daten verarbeiten, auf den Markt kommen. Die Bewertung muss die möglichen Auswirkungen der vorgeschlagenen Technologie für personenbezogene Daten angehen. Werden Risiken ermittelt, müssen Maßnahmen ergriffen werden, um Prozesse zur Senkung dieser Risiken zu identifizieren oder Alternativen zu dem zu finden, was vorgeschlagen wird.

11. Migration und Grenzkontrolle

Grenzkontrollen sind ein Bereich, in dem Sicherheits- und Überwachungstechnologien sehr verbreitet sind. Dies wirft sowohl global als auch in den EU-Mitgliedstaaten einige Bedenken hinsichtlich der Auswirkungen auf die Menschenrechte und das Solidaritätsprinzip auf. Die EGE empfiehlt, die Grenzkontrollsysteme im Hinblick auf die in dieser Stellungnahme aufgestellten Kriterien, nämlich Menschenwürde und Menschenrechte, Gerechtigkeit, Notwendigkeit, Verhältnismäßigkeit, Wirksamkeit, Alternativen und Rechenschaftspflicht zu beurteilen.

Im Einklang mit den Ergebnissen der Artikel-29-Arbeitsgruppe ist die EGE besorgt, dass das Einreise-/Ausreisensystem (Entry-Exit-System — EES), das im Rahmen der Grenzinitiative „Smart Borders“ vorgeschlagen wird, einen unverhältnismäßigen Eingriff in die individuelle Privatsphäre darstellt. Laut dem Stockholmer Programm sollten neue Systeme nur dann entwickelt werden, wenn sie und andere existierende Systeme zuvor begutachtet worden sind. Die EGE ist nicht davon überzeugt, dass dieses Kriterium beim Einreise-/Ausreisensystem hinreichend erfüllt ist. Dazu hätte es einer umfassenden Betrachtung bedurft, welche sowohl die Beeinträchtigungen von Privatsphäre und Datenschutz als auch die Wirksamkeit für Grenzkontrolle und öffentliche Sicherheit einschließt. Daher empfiehlt die EGE ein Moratorium für die Einführung des EES, während bestehende

Systeme wie das Visa-Informationssystem ausgewertet werden, um zu prüfen, ob die Ziele der EES in angemessener Weise erfüllt werden können.

Da EU-Großdatenbanken, die für Grenzkontrollzwecke verwendet werden, die Rechte von EU- und Nicht-EU-Bürgern in Gefahr bringen, von denen ein Teil besonders gefährdet ist, muss die Einführung solcher Datenbanken einer strengen Bewertung unter besonderer Berücksichtigung ihrer Auswirkungen auf die Grundrechte und die Einhaltung des Grundsatzes der Zweckbindung unterzogen werden.

III. Ethische und rechtliche Bewertungskriterien gehen Hand in Hand. **Vertrauen** kann nur durch ein Zusammenwirken beider (wieder) aufgebaut werden. Daher empfiehlt die EGE verschiedene Maßnahmen, um konkreter Vertrauen aufzubauen und die Interessen der Bürger an der Kontrolle über ihre persönlichen Angelegenheiten zu wahren. Diese Maßnahmen fallen in die Bereiche Aufsicht, Durchsetzung, Whistleblowing, Information der Öffentlichkeit, Bildung, Ausbildung und Forschung.

12. Vertrauenswürdige Aufsicht

Die EGE erkennt an, dass es in Fragen der nationalen Sicherheit nicht immer möglich ist, im Hinblick auf Überwachungsmaßnahmen transparent zu sein. Dennoch ist das Vertrauen der Öffentlichkeit von entscheidender Bedeutung für die Legitimität staatlicher Sicherheitsmaßnahmen. Zu diesem Zweck empfiehlt die EGE, dass unbeschadet jeglicher gerichtlicher Aufsicht die Mitgliedstaaten eine Stelle oder Person mit Aufsichtsbefugnis einrichten oder bestehende Gremien erweitern, damit eine vertrauenswürdige dritte Partei zur Verfügung steht, die im Namen der Öffentlichkeit handeln kann. Eine solche Stelle würde auch die Auswirkungen der öffentlichen und privaten Überwachung auf die Rechte und Pflichten der Bürger beobachten. Zusammengefasste Informationen über die Anzahl der Anträge auf Überwachungsbefugnisse, unabhängig von wem und zu welchem Zweck diese eingereicht wurden, müssen von den Mitgliedstaaten veröffentlicht werden, damit Transparenz und Rechenschaftspflicht gewährleistet sind. Die Mitgliedstaaten sollten eine solche Stelle oder Person im Vorfeld der Einführung von Rechtsvorschriften auf dem Gebiet der Überwachung konsultieren. Die EGE sieht vor, dass die vertrauenswürdige dritte Partei eine wichtige Rolle bei der Sensibilisierung der Öffentlichkeit und der Anregung von Debatten über Risiken und Nutzen der Überwachung spielt.

13. Durchsetzung des Datenschutzes

Die EGE ist der Ansicht, dass der im EU-Recht verankerte Datenschutz robust ist, aber auf nationaler Ebene durchgesetzt werden muss. Die Mitgliedstaaten müssen daher sicherstellen, dass die Datenschutzbehörden über ausreichende rechtliche Befugnisse, technisches Know-how und Ressourcen verfügen, um eine effektive Rechtsdurchsetzung in der gesamten Europäischen Union zu gewährleisten.

14. Whistleblowing

Die Europäische Kommission und die Mitgliedstaaten müssen sicherstellen, dass ein effektiver und umfassender Schutzmechanismus für Whistleblower (Hinweisgeber bzw. Informanten) im öffentlichen wie im privaten Sektor etabliert wird. Im Einklang mit den Grundsätzen von Transparency International, wie im Bericht von 2013 über „Whistleblowing in Europa“ angegeben ist, muss es Vorschriften und Verfahren für Fälle geben, in denen es um die nationale Sicherheit geht, und diese müssen klar sein. Die Vertraulichkeit oder Anonymität muss gewährleistet sein, und es muss für gründliche, zeitnahe und unabhängige Untersuchungen der Angaben von Informanten gesorgt werden. Außerdem muss es transparente, durchsetzbare und zeitnahe Mechanismen geben, um rechtzeitig eine Beschwerde eines Informanten wegen etwaiger Vergeltungsmaßnahmen zu verfolgen. Wenn eine Offenlegung Fragen der nationalen Sicherheit, Amts- oder Militärgeheimnisse oder Verschlussachen betrifft, sind spezielle Verfahren und Garantien für die Berichterstattung einzuführen, die die Sensibilität der Thematik berücksichtigen, um erfolgreich eine interne Verfolgung zu erreichen und eine unnötige externe Exposition zu verhindern. Diese Verfahren sollten eine interne Offenlegung, die Weitergabe an ein autonomes Aufsichtsgremium, das institutionell und operativ unabhängig vom Sicherheitssektor ist, oder die Weitergabe an Behörden mit der entsprechenden Sicherheitsüberprüfung vorsehen. Externe Weitergabe (das heißt, an die Medien und Organisationen

der Zivilgesellschaft) würde als letztes Mittel gerechtfertigt werden.

15. Planung von Datenschutz

Behörden und private Unternehmen müssen Planungsprinzipien für den „Datenschutz durch“ und den „Datenschutz in“ bei der Entwicklung von Sicherheits- und Überwachungstechnologien verabschieden. Die europäischen Werte Würde, Freiheit und Gerechtigkeit müssen vor, während und nach der Gestaltung, Entwicklung und Bereitstellung solcher Technologien berücksichtigt werden. Datenschutzfreundliche Technologien müssen von Anfang an integriert werden; es reicht nicht aus, auf eine spätere Implementierung zu verweisen. Nach Ansicht der EGE ist es möglich, durch die interdisziplinäre Zusammenarbeit von Ingenieuren, Entwicklern und Experten in philosophischer und ethischer Reflexion eine Organisationskultur zu schaffen, in der der Datenschutz verankert ist und in der Praxis reflektiert wird. Kurse und Schulungen zu ethischen Aspekten auf theoretischer und praktischer Ebene sowohl für Studenten und Hochschulabsolventen in den Fachbereichen Ingenieurwissenschaften und Informatik als auch in der beruflichen Bildung könnten die Berücksichtigung von Datenschutzaspekten bei der Entwicklung von Sicherheits- und Überwachungstechnologien verbessern.

16. Das Verständnis für und die Wertschätzung der Privatsphäre

Privatsphäre und Datenschutz sind kein statisches Konzept, und ein vollständigeres Verständnis darüber, wie europäische Bürger diese Aspekte verstehen und bewerten, ist unbedingt erforderlich, wenn geeignete Maßnahmen ergriffen werden müssen, um die informationelle Selbstbestimmung und den Datenschutz sicherzustellen. Zu diesem Zweck muss die EU Mittel für die Forschung zur Verfügung stellen, um zu untersuchen und zu analysieren, wie Bürgerinnen und Bürger ihre Mitwirkung in Fragen der Sicherheit und Überwachung sehen und pflegen.

Le groupe européen d'éthique des sciences et des nouvelles technologies

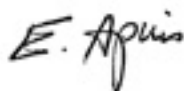
Le président

Julian Kinderlerer



Les membres

Emmanuel Agius



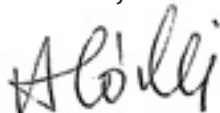
Peter Dabrock



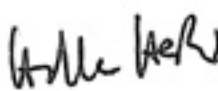
Inez de Beaufort



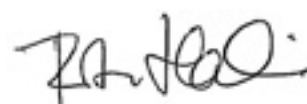
Andrzej Gorski



Hille Hacker



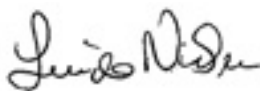
Ritva Halila



Paula Martinho da Silva



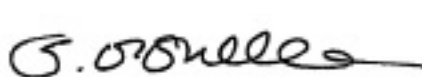
Linda Nielsen



Herman Nys



Siobhán O'Sullivan



Laura Palazzani



Pere Puigdomenech



Marie-Jo Thiel



Günter Virt



Secrétariat GEE

Adresse

Commission européenne
Berl 8/362
1049 Bruxelles
BELGIQUE
Fax +32 22994565
E-mail: BEPA-ETHICS-GROUP@ec.europa.eu



Jim DRATWA

Commission européenne
Membre, Bureau des conseillers de politique européenne
Secrétaire général du DIB
Chef du secrétariat GEE
Berl 8/358
1049 Bruxelles
BELGIQUE
Tél. +32 22958253
E-mail: jim.dratwa@ec.europa.eu



Joanna PARKIN

Commission européenne
Chargée de mission, Bureau des conseillers de politique européenne
1049 Bruxelles
BELGIQUE
Tél. +32 22954262
E-mail: joanna.parkin@ec.europa.eu



Kim Hoang LE

Commission européenne
Secrétariat GEE
Berl 8/362
1049 Bruxelles
BELGIQUE
Tél. +32 22999228
E-mail: kim-hoang.le@ec.europa.eu



Adriana Sorina OLTEAN

Commission européenne
Secrétariat GEE
Berl 8/362
1049 Bruxelles
BELGIQUE
Tél. +32 22993016
E-mail: adriana-sorina.oltean@ec.europa.eu

Site web:

http://ec.europa.eu/european_group_ethics/index_en.htm

COMMENT VOUS PROCURER LES PUBLICATIONS DE L'UNION EUROPÉENNE?

Publications gratuites:

- un seul exemplaire:
sur le site EU Bookshop (<http://bookshop.europa.eu>);
 - exemplaires multiples/posters/cartes:
auprès des représentations de l'Union européenne (http://ec.europa.eu/represent_fr.htm),
des délégations dans les pays hors UE (http://eeas.europa.eu/delegations/index_fr.htm),
en contactant le réseau Europe Direct (http://europa.eu/europedirect/index_fr.htm)
ou le numéro 00 800 6 7 8 9 10 11 (gratuit dans toute l'UE) (*).
- (*) Les informations sont fournies à titre gracieux et les appels sont généralement gratuits (sauf certains opérateurs, hôtels ou cabines téléphoniques).

Publications payantes:

- sur le site EU Bookshop (<http://bookshop.europa.eu>).

Abonnements:

- auprès des bureaux de vente de l'Office des publications de l'Union européenne (http://publications.europa.eu/others/agents/index_fr.htm).



Office des publications

ISBN 978-92-79-37943-7
doi:10.2796/2409