ONU et CdE

Janvier

19 février – La Cour européenne des droits de l'homme (CouEDH) déclare irrecevable une requête présentée par deux co-fondateurs de The Pirate Bay, l'un des plus grand sites de partage de fichiers. L'affaire *Neij et Sunde Kolmisoppi c. Suède* porte sur la violation de leur liberté d'expression, du fait de leur condamnation pour infraction à la loi sur le droit d'auteur (*Copyright Act*). Le partage de fichiers en ligne relève du droit de « recevoir et de communiquer des informations » inscrit à l'article 10 de la Convention européenne des droits de l'homme (CEDH), mais les tribunaux nationaux avaient, à juste titre, pesé le droit des demandeurs contre la nécessité de protéger le droit d'auteur

25-27 février – Dans les recommandations de la première réunion d'examen du SMSI+10 (Sommet mondial sur la société de l'information), l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO) réaffirme que les droits de l'homme doivent être appliqués de la même façon en ligne comme hors ligne

Février

Mars

17 avril – Le rapporteur spécial de l'Organisation des Nations Unies (ONU) sur la promotion et la protection du droit à la liberté d'opinion et d'expression publie son rapport annuel indiquant que la surveillance des communications par l'État ébranle les droits humains en matière de respect de la vie privée et de liberté d'expression

18 avril – Dans l'affaire *M.K. c. France*, la CouEDH décide que, les garanties relatives à la collecte, la conservation et l'effacement des empreintes digitales d'une personne suspectée mais non condamnée de vol étant insuffisantes, les autorités avaient de fait violé le droit au respect de la vie privée de cette personne

Avril

Mai

4 juin – Dans l'affaire *Peruzzo et Martens c. Allemagne,* la CouEDH déclare la requête irrecevable. L'ordonnance du Tribunal stipulant la collecte d'échantillons cellulaires de personnes condamnées pour des délits graves et de les conserver dans des bases de données sous la forme de profils ADN était nécessaire et proportionnée

11 juin – Le Comité des Ministres du Conseil de l'Europe adopte une déclaration sur les risques présentés par le suivi numérique et les autres technologies de surveillance pour les droits fondamentaux

20–21 juin – Les acteurs européens se rencontrent lors du forum régional « Dialogue européen sur la gouvernance d'internet » (EuroDIG) pour discuter de la manière d'utiliser un internet ouvert et sécurisé au service de l'intérêt public

24 juin – La Commission des questions juridiques et des droits de l'homme de l'Assemblée parlementaire du Conseil de l'Europe (APCE) adopte un rapport sur la *sécurité nationale et l'accès à l'information* et encourage les gouvernements à aligner leur législation en relation avec les lanceurs d'alerte sur un ensemble de principes reconnus mondialement

25 juin 2013 – La CouEDH considère dans l'affaire *Initiative des jeunes pour les droits de l'Homme c. Serbie* que le refus opposé par l'agence serbe de renseignements de fournir des informations sur le nombre de personnes qu'elle avait soumises à une surveillance électronique viole le droit de l'organisation non-gouvernementale (ONG) à recevoir des informations

Juin

16 juillet – La CouEDH considère dans l'affaire *Nagla c. Lettonie* que la saisie de dispositifs de stockage de données, conservés à son domicile par une journaliste, a violé le droit à la liberté d'expression ainsi que le droit des journalistes à protéger leurs sources

Juillet

Août

Septembre

10 octobre – Dans l'affaire *Delfi AS c. Estonie,* la CouEDH décide qu'établir la responsabilité d'un portail web quant aux commentaires offensants publiés par ses lecteurs est une restriction justifiée et proportionnée de la liberté d'expression du portail

22–25 octobre – La première session sur les droits de l'homme en ligne, tenue dans le cadre du Forum sur la gouvernance d'internet, se conclut par un appel à intensifier le rôle du Forum dans le domaine de la protection des droits de l'homme pour les utilisateurs d'internet, ainsi que, pour les États, à consulter les parties prenantes pendant toute procédure législative

Octobre

8 novembre – Les ministres responsables des médias et de la société de l'information des États membres du Conseil de l'Europe adoptent une déclaration politique et trois résolutions sur la liberté de l'internet, le rôle des médias à l'âge du numérique et la sécurité des journalistes lors de la Conférence ministérielle du Conseil de l'Europe à Belgrade

Novembre

18 décembre – L'Assemblée générale des Nations Unies adopte une résolution sur le droit à la vie privée à l'ère du numérique

Décembre

UE

11 janvier – Ouverture officielle du Centre européen de lutte contre la cybercriminalité (EC3) près l'Office européen de police (Europol)

Janvier

7 février – La Commission européenne publie une *Communication conjointe sur la stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé*

7 février – La Commission européenne adopte une proposition de directive concernant les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'UE

Février

19 mars – La Cour de justice de l'Union européenne (CJUE) rend son arrêt dans l'affaire *Sophie in't Veld MEP c. Commission européenne* sur la transparence des documents de l'accord commercial anti-contrefaçon (ACTA) en annulant la décision de la Commission du 4 mai 2010, qui refusait l'accès aux documents

27 mars – La Commission européenne propose un nouveau règlement relatif à Europol, qui suggère de modifier les garanties en matière de protection des données

Mars

24 avril – La Commission européenne adopte le livre vert *Se préparer à un monde audiovisuel totalement convergent : croissance, création et valeurs*

24 avril – La Commission libertés civiles, justice et affaires intérieures (LIBE) du Parlement européen rejette la proposition de directive européenne sur l'utilisation des données des passagers aériens (PNR)

Avril

13 mai – La Commission européenne présente un programme visant à mettre en place l'Observatoire mondial de la politique d'Internet, destiné à surveiller les développements politiques, législatifs et technologiques liées à internet de par le monde

30 mai – Dans l'affaire *Commission c. Suède*, la CJUE ordonne à la Suède de payer une somme forfaitaire de 3 000 000 EUR pour son retard à transposer dans la législation nationale la directive sur la conservation des données

Mai

10 juin – La Vice-présidente Viviane Reding écrit au procureur général des Etats-Unis afin d'obtenir des informations quant aux programmes de surveillance tel que le programme PRISM

13 juin – Dans l'affaire *Michael Schwarz c. Stadt Bochum*, la CJUE conclut que les dispositifs de sécurité et de biométrie dans les passeports et les documents de voyage des ressortissants des États membres de l'UE constituent une ingérence proportionnée avec la protection des données à caractère personnel

25 juin – Le Conseil de l'Union européenne approuve le texte sur la mise en œuvre de la stratégie de cybersécurité de l'Union européenne remis par le groupe des Amis de la présidence chargé des questions inhérentes au cyberespace

Juin

4 juillet – Le Parlement européen adopte une résolution enjoignant la Commission LIBE de mettre sur pieds une commission d'enquête sur les programmes de surveillance américains

Juillet

12 août – La directive relative aux attaques visant les systèmes d'information est adoptée. Elle renforcera la protection des données à caractère personnel en réduisant la capacité des cybercriminels à abuser des droits des victimes en toute impunité

Août

11 septembre – La Commission européenne présente une proposition de règlement établissant des mesures relatives à un marché unique européen des communications électroniques et visant à faire de l'Europe un continent connecté

Septembre

21 octobre – La Commission LIBE adopte son rapport sur la proposition de règlement relatif à la protection des données et la proposition de directive concernant le secteur de l'application de la loi

Octobre

Novembre

10 décembre – L'avocat général de la CJUE présente ses conclusions dans l'affaire *Commission c. Hongrie*, suggérant une violation de l'indépendance de l'autorité chargée de la protection des données

12 décembre – Dans ses conclusions, l'avocat général de la CJUE estime que la directive sur la conservation des données est incompatible avec la Charte des droits fondamentaux de l'Union européenne

18 décembre – Le rapporteur de la commission d'enquête LIBE sur la surveillance de masse suggère, dans ses conclusions préliminaires, de suspendre l'accord sphère de sécurité ou *Safe Harbour* et le programme de surveillance du financement du terrorisme (TFTP), en créant une offre européenne d'informatique en nuage et en garantissant des voies de recours judiciaires aux citoyens de l'UE dont les données à caractère personnel sont transférées aux États-Unis (USA)

Décembre

3 Société de l'information, respect de la vie privée et protection des données à caractère personnel

Des révélations sans précédent sur la surveillance de masse par les États-Unis et le Royaume-Uni des flux de données et des télécommunications mondiales ont fait la une de la presse internationale pendant des semaines en 2013. La question de la vie privée s'est ainsi trouvée placée sous les feux de l'actualité et le fossé existant entre des technologies à l'évolution rapide et les lois actuelles protégeant le droit à la vie privée a été mis en évidence. Ces révélations se sont produites alors que l'UE travaillait sur la réforme la plus importante de la législation européenne dans le domaine de la protection des données depuis ces 20 dernières années. En soulignant avec éclat la nécessité d'un cadre fort de protection des données, celles-ci ont marqué un tournant dans le débat. Déconcertés par ces révélations, les décideurs de l'UE et des États membres ont immédiatement pris des mesures pour consolider les règles de protection des données, tandis que la société civile poussait pour une plus grande transparence et des voies de recours plus efficaces devant les tribunaux et les autorités chargées de la protection des données. Face à ces révélations, le législateur de l'UE a introduit avec succès des réformes significatives dans le paquet concernant la réforme de la protection des données. En dépit de certains progrès, cette réforme n'était pas finalisée à la fin 2013.

3.1. Les révélations sur la surveillance de masse suscitent un intérêt mondial

A partir de juin 2013, Edward Snowden, un consultant de l'Agence nationale de sécurité américaine (NSA) a divulgué à plusieurs médias des documents révélant les détails du fonctionnement d'un programme de surveillance mondial par la NSA, ainsi que ceux d'un programme mené par le Quartier général des communications du gouvernement (GCHQ) du Royaume-Uni. D'un intérêt particulier pour l'Union, ces programmes mondiaux comportaient aussi des cibles au sein de l'UE telles que les institutions européennes ou les ambassades des États membres[1].

Quelques semaines à peine avant que ces révélations ne se propagent dans toute l'Union européenne et dans le monde entier, le rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, remarquant cette lacune existant

Développements clés dans le domaine de la société de l'information, du respect de la vie privée et de la protection des données

- Les révélations d'une surveillance massive se répercutent dans les domaines de la société de l'information, du respect de la vie privée et de la protection des données. Ces révélations poussent les organisations de la société civile à protester et à réclamer une meilleure protection ; elles incitent aussi les décideurs et les législateurs de l'Union européenne et des États membres à adopter des mesures plus énergiques, à renforcer la protection législative et à proposer de plus grandes garanties pour la protection des données.
- Réagissant à ces révélations, l'Assemblée générale des Nations Unies adopte un texte sans précédent sur la protection de la vie privée.
- Ces révélations – qui touchent l'UE alors que celle-ci travaille sur la réforme la plus importante de la législation de l'Union en matière de protection des données depuis ces 20 dernières années – mettent en évidence le fait que la protection des droits fondamentaux dans le monde virtuel requiert une plus grande attention.
- Le Parlement européen adopte son rapport sur le paquet relatif à la réforme de la protection des données mais celui-ci est retardée au Conseil de l'Union européenne.

entre les évolutions technologiques rapides et les lois actuelles garantissant le droit au respect de la vie privée, attirait l'attention sur certaines failles spécifiques, tel que le manque de supervision judiciaire des mesures de surveillance (voir également le Chapitre 10 concernant les États membres et les obligations internationales)[2]. L'Assemblée générale des Nations Unies, faisant écho aux appels du rapporteur spécial des Nations Unies, a demandé aux États membres de revoir leur législation sur ce type de surveillance et de s'assurer que celle-ci respecte les obligations internationales en matière de droits de l'homme. Elle a adopté en décembre 2013 une résolution sur le *Droit à la vie privée à l'ère numérique*[3].

Lorsque les médias ont publié les premières révélations, le Comité des Ministres du Conseil de l'Europe a adopté une déclaration sur les risques présentés par le suivi numérique et les autres technologies de surveillance pour les droits fondamentaux. Dans cette déclaration, il indiquait : « une législation qui permet de surveiller largement les citoyens peut être jugée contraire au droit au respect de la vie privée. De telles possibilités et pratiques peuvent dissuader les citoyens de participer à la vie sociale, culturelle et politique et à plus long terme, avoir des effets dommageables sur la démocratie »[4]. Le Commissaire aux droits de l'homme du Conseil de l'Europe a publié le 24 octobre 2013 un texte[5] soulignant les menaces contre les droits de l'homme et le droit à la vie privée lorsque la surveillance secrète gagne du terrain. En outre, les ministres responsables des médias et de la société de l'information ont adopté une déclaration politique en novembre 2013, en soulignant que « toute [...] surveillance visant à la protection de la sécurité nationale doit être conforme aux normes existantes en matière de droits de l'homme ainsi que de l'État de droit »[6].

Le Tableau 3.1 énumère les programmes de surveillance les plus connus mais, selon des révélations ultérieures, ceux-ci ne seraient en réalité que « la partie émergée de l'iceberg »[7].

3.1.1. L'Union européenne prend des mesures face à la nouvelle d'une surveillance de masse

> *« Le scandale de la surveillance de masse a été un coup de tonnerre et l'Europe répond. »*
>
> *Viviane Reding, Vice-présidente, « Un pacte pour l'Europe en matière de protection des données », 28 janvier 2014, Discours/14/62, http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm*

Le Parlement européen, la Commission européenne et le Conseil de l'Union européenne ont rapidement réagi aux révélations de l'affaire Snowden, prenant un

Tableau 3.1 : Principaux programmes de surveillance

Nom du programme	Description des programmes allégués
Prism	Fournit à la NSA un accès direct aux serveurs centraux des neuf principales sociétés du numérique aux États-Unis, lui permettant de collecter des données sur leurs clients, ainsi que d'examiner leur historique, le contenu des courriels, les transferts de fichiers et les discussions en ligne.
Xkeyscore	Permet aux analystes de la NSA d'examiner, sans y être préalablement autorisés, de vastes bases de données contenant des courriels, des discussions en ligne et l'historique de navigation de millions d'utilisateurs d'internet ainsi que leurs métadonnées.
Upstream	Programmes de collecte gérés par la NSA qui consistent à mettre sur écoute sans autorisation des connexions internet câblées.
Bullrun	Programme de décryptage géré par la NSA pour tenter de pénétrer des technologies de cryptage largement utilisées, lui permettant de contourner le cryptage de données utilisé par des millions de personnes dans leurs transactions en ligne et leurs courriels.
Muscular	Programme conjoint utilisé par la NSA et le GCHQ visant à intercepter, à partir de liens privés, la circulation de données entre les principales plateformes telles que Yahoo, Google, Microsoft Hotmail et Windows Live Messenger.
Tempora	Activité de surveillance en amont permettant au GCHQ d'avoir accès aux câbles de fibre optique transportant d'énormes quantités de communications privées entre utilisateurs d'internet et de les partager avec la NSA.
Edgehill	Programme de décryptage géré par le GCHQ visant à décoder le trafic crypté utilisé par les sociétés pour fournir un accès à distance à leur système.

Sources: Moraes, C. (2013), document de travail n° 1, sur les programmes de surveillance US/UE et leur impact sur les droits fondamentaux des citoyens européens, *PE524.799v01-00, Bruxelles, 11 décembre 2013; Bowden, C. (2013),* Les programmes américains de surveillance et leur impact sur les droits fondamentaux des citoyens européens, *Étude réalisée pour le Parlement européen, PE 474.405, Bruxelles, septembre 2013*

certain nombre de mesures qui exprimaient leur vive préoccupation quant au programme de surveillance de masse, ont demandé des éclaircissements et se sont efforcés de restaurer la confiance, par exemple, dans les flux de données. Le Tableau 3.2 résume ces mesures. Le Parlement européen a chargé la Commission libertés civiles, justice et affaires intérieures (LIBE) de mener une enquête[8]. Son projet de rapport, finalisé en janvier 2014, lance l'idée d'un «habeas corpus numérique européen de règles relatives à la protection de la vie privée» basé sur huit actions concrètes. Parmi celles-ci se trouve l'adoption du paquet relatif à la réforme sur la protection des données de l'UE d'ici 2014 (pour plus d'informations sur le paquet relatif à la réforme sur la protection des données, voir la Section 3.2), la protection accrue des lanceurs d'alerte, le développement d'une stratégie européenne pour une plus grande indépendance des technologies de l'information ainsi que la suspension des accords spécifiques US-UE.

Le projet de rapport de 2013, adopté au printemps 2014[9], est axé sur la décision 2000/520/CE, appelée décision relative à la sphère de sécurité[10], et qui assure la base légale pour le transfert des données à caractère personnel depuis l'UE aux sociétés américaines. Ces transferts reposent sur les Principes de la « sphère de sécurité » visant à la protection de la vie privée et sur le Programme de surveillance du financement du terrorisme (TFTP), cette « sphère de sécurité » garantissant que les sociétés américaines enregistrées offrent le niveau de protection de la vie privée « adéquat » requis par la législation de l'UE.

Le Conseil de l'Union européenne a mis en place un groupe de travail UE-US *ad hoc* pour établir les faits en ce qui concerne les programmes de surveillance américains et leur impact sur les droits fondamentaux dans l'UE et sur les données à caractère personnel des citoyens de l'Union. Le 27 novembre 2013, le groupe de travail a publié ses conclusions[11]. Tout en présentant les garanties en place en matière de protection des données, le rapport souligne les différences entre les régimes juridiques américain et européen de protection des données.

Le 27 novembre 2013, s'appuyant sur le rapport de ce groupe de travail, la Commission européenne a publié deux communications relatives aux conséquences des révélations[12].

La première, la communication relative au *fonctionnement de la sphère de sécurité*, évalue la mise en

Tableau 3.2: documents clés de l'UE adoptés à la suite des révélations sur la surveillance de masse

Institution	Titre	Référence
Commission européenne	10 juin 2013 – La Vice-présidente Viviane Reding demande des explications et des éclaircissements sur le programme PRISM.	
Commission européenne	19 juin 2013 – La Vice-présidente Viviane Reding et la Commissaire Cecilia Malmström envoient une lettre aux autorités américaines exprimant leur préoccupation concernant les conséquences des programmes de surveillance américains sur la protection des droits fondamentaux des Européens.	
Parlement européen	Résolution du 4 juillet 2013 relative au programme de surveillance américain de la NSA, aux organismes de surveillance dans divers États membres et aux incidences sur les droits fondamentaux des citoyens européens.	P7_TA(2013)0322
Parlement européen	Résolution du 23 octobre 2013 relative à la suspension de l'accord TFTP du fait de la surveillance exercée par l'agence nationale de sécurité américaine (NSA)	P7_TA(2013)0449
Conseil de l'Union européenne	Rapport du 27 novembre 2013 sur les conclusions des co-présidents de l'Union européenne du groupe de travail ad hoc UE-États-Unis sur la protection des données	16987/13
Commission européenne	Communication de la Commission au Parlement européen et au Conseil – Restaurer la confiance dans les flux de données UE-États-Unis	COM(2013) 846 final du 27 novembre 2013
Commission européenne	Communication de la Commission au Parlement européen et au Conseil sur le fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union européenne et des sociétés établies sur son territoire	COM(2013) 847 final du 27 novembre 2013
Commission européenne	Communication de la Commission au Parlement européen et au Conseil relative au rapport conjoint de la Commission et du département du Trésor des États-Unis concernant la valeur des données fournies dans le cadre du programme de surveillance du financement du terrorisme (TFTP)	COM(2013) 843 final du 27 novembre 2013
Parlement européen	Projet de rapport du 8 janvier 2014 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	PE526.085v02-00

Source: FRA, 2013

œuvre de la décision 2000/520/CE et recommande un certain nombre d'améliorations[13]. Cette communication suggère, par exemple, que les sociétés informent leurs clients lorsque les autorités américaines sont autorisées à collecter et à traiter des données pour des raisons de sécurité nationales, dans l'intérêt général ou en application de la loi.

La deuxième, la communication intitulée *Restaurer la confiance dans les flux de données UE-États-Unis*[14], évalue l'impact d'une surveillance à une grande échelle sur différents accords UE-États-Unis. Elle met en cause le caractère nécessaire et proportionné du programme de surveillance américain dans le contexte de la sécurité nationale. Cette communication souligne la pertinence du paquet de la réforme de la protection des données dans ce cadre. Une fois adoptée, la réforme augmentera les garanties concernant la protection des données à caractère personnel des citoyens de l'UE (pour de plus amples informations sur la réforme relative à la protection des données, voir la Section 3.2). Elle suggère aussi d'améliorer la décision relative à la sphère de sécurité et d'accroître les garanties dans le contexte de l'application de la loi. Elle prône le renforcement de la protection de la vie privée sur internet, ce qui ne doit pas ébranler la liberté, l'ouverture et la sécurité du cyberespace (pour plus de renseignements sur la société de l'information, voir la Section 3.3).

3.1.2. Les États membres de l'UE réagissent à la surveillance de masse

Parmi les États membres de l'UE, les réactions aux révélations se sont échelonnées de l'absence totale de réaction jusqu'à la protestation populaire. En **Finlande**, par exemple, les citoyens ont présenté une initiative pour réformer la législation sur la protection des données. Intitulée « Oui, nous le pouvons – La loi pour la sauvegarde de la liberté d'expression et de la vie privée dans le monde » a été présentée le 8 juillet 2013 au service en ligne du ministère de la justice mais elle n'a pour le moment conduit à aucune modification législative concrète[15]. Cette initiative propose de criminaliser la surveillance disproportionnée des citoyens en en faisant un délit universel dont les auteurs pourraient être poursuivis en Finlande même si l'acte est commis dans un autre pays. Elle élargit aussi la responsabilité des autorités et des opérateurs de télécommunications pour signaler la collecte, la conservation et l'utilisation en masse de données à caractère personnel. Pour le moment, le ministère finlandais de l'intérieur rend seul compte à la Commission européenne des pratiques de conservation des données ; les entreprises sont dépourvues de toute obligation de rendre compte de leurs pratiques en matière de protection des données. Cette initiative comprend aussi des dispositions visant à protéger le statut juridique des lanceurs d'alerte, en interdisant leur extradition ou le rejet de leur demande de permis d'entrée ou de séjour.

En **Allemagne**, la Conférence des commissaires à la protection des données a vivement critiqué le manque d'explications de la part des autorités américaines sur le but des programmes de surveillance de masse et a appelé les gouvernements de la fédération et des États (*Länder*) à protéger les droits fondamentaux, à renforcer la supervision des services secrets ainsi qu'à arrêter et à empêcher la coopération non constitutionnelle des services de renseignements, là où celle-ci a été mise en place[16]. La société civile a vivement réagi. Le 7 septembre 2013, plusieurs milliers de personnes ont protesté à Berlin contre la surveillance. La manifestation, organisée et encouragée par une large coalition de 85 organisations pour les libertés civiles, groupes de défense de la vie privée, fédérations de journalistes, partis politiques et leurs organisations pour la jeunesse[17], a rassemblé près de 15 000 manifestants[18]. Sous la bannière de « Liberté oui, peur non – Stop à la manie de la surveillance ! » (*Freiheit statt Angst. Stoppt den Überwachungswahn!*), les manifestants ont protesté contre la surveillance des télécommunications par les services secrets, la conservation des données, les scanners corporels, la biométrie, l'enregistrement des dossiers passagers et la vidéo surveillance. Ils ont demandé que soit mis en place un régime européen fort de protection des données, une évaluation indépendante des pouvoirs existants en matière de surveillance et un moratoire sur des mesures de surveillance planifiées[19]. En outre, de nouveaux types de manifestations de groupe ont fleuri : des « walk-ins » à proximité des sites des agences de renseignements nationales et américaines ont attiré l'attention des médias[20] ; lors de crypto-parties, des experts en technologie de l'information ont formé des personnes du public non-initiées à la manière de se protéger et de crypter leurs données et leurs communications électroniques[21].

Certains États membres de l'UE ont envisagé une réforme en matière de services de renseignements à la lumière des révélations de l'affaire Snowden. En **France**[22] et en **Hongrie**,[23] par exemple, des amendements réglementant l'accès des services de renseignements aux données à caractère personnel ont suscité les critiques d'organisations de la société civile, d'hommes politiques[24] et d'institutions spécialisées telles que, respectivement, le Conseil national du numérique en France[25] et l'Autorité pour la protection des données en Hongrie[26]. En novembre 2013, la Cour constitutionnelle hongroise a validé la constitutionnalité de la loi correspondante. La Cour a estimé qu'une organisation antiterroriste qui s'appuie sur une autorisation ministérielle plutôt que sur un mandat du tribunal pour collecter des informations cachées sur des citoyens ne violait pas le droit à la vie privée[27].

Le 19 juillet 2013, le gouvernement fédéral **allemand** a présenté un programme en huit points pour contribuer à éclairer les faits sur la surveillance de masse et pour assurer une protection plus solide du droit au respect de la vie privée et de la protection des données. Intitulé « l'Allemagne est un pays de liberté », ce programme propose les mesures suivantes :

1) suspendre au plus vite les accords administratifs sur la surveillance des communications avec la France, le Royaume-Uni et les États-Unis ;

2) organiser des discussions d'experts avec les États-Unis pour examiner ce sujet ;

3) réclamer un accord international pour la protection des données (sous forme de protocole additionnel de l'article 17 du pacte international relatif aux droits civils et politiques) ;

4) promouvoir les travaux du règlement européen sur la protection des données, avec l'obligation pour les sociétés privées de signaler les transferts de données vers les pays tiers (voir la Section 3.2) ;

5) développer des normes permettant aux agences de renseignement des États membres de l'Union de coopérer ;

6) élaborer et mettre en œuvre une stratégie européenne en matière de technologie de l'information en collaboration avec la Commission européenne ;

7) établir une table ronde pour une discussion sur la « technologie de la sécurité pour la technologie de l'information », en partenariat public-privé avec des instituts de recherche et des sociétés privées ;

8) renforcer l'éducation des citoyens en matière de sécurité des technologies de l'information grâce à l'initiative « l'Allemagne en sécurité sur l'internet » (*Deutschland sicher im Netz*)[28].

Le gouvernement allemand a suspendu en août les accords administratifs avec les États-Unis. Il a aussi organisé plusieurs discussions avec la France et le Royaume-Uni. De nombreuses questions restent sans réponse, cependant, et il est impossible de savoir quelle direction prendront les discussions portant sur un accord de non-espionnage.

Aux **Pays-Bas**, les révélations ont suscité des questions parlementaires. Le 2 décembre 2013, le gouvernement a aussi institué une commission destinée à évaluer la loi sur les agences d'information et de sécurité de 2002 (*Wet op de Inlichtingen- en Veiligheidsdiensten 2002*). Elle a conclu que les pouvoirs des agences devaient être étendus, en raison des nouvelles menaces pesant sur la sécurité nationale du fait de cyber attaques et de l'espionnage numérique[29].

En **Slovénie**, les révélations ont aussi conduit à une question parlementaire. Le gouvernement a répondu le 28 novembre 2013, en indiquant qu'une surveillance globale à grande échelle n'est pas acceptable, en raison des standards en matière de droits de l'homme, telles que le droit au respect de la vie privée et l'État de droit[30].

3.1.3. Demandes d'information et recours judiciaires

Les révélations de l'affaire Snowden ont aussi suscité des appels à plus de transparence et poussé certains à rechercher, dans le cas de violations alléguées, des recours devant les autorités de protection des données et la Cour européenne des droits de l'homme (CouEDH).

En octobre 2013, des ONG polonaises ont demandé des informations sur les programmes de surveillance[31] à plusieurs agences et institutions gouvernementales. Certaines ont donné des réponses détaillées sur leur activité liée au programme PRISM, telle l'Autorité pour la protection des données. D'autres ont répondu en partie seulement et en termes généraux. La commission des services secrets du Parlement polonais a confirmé, par exemple, qu'aucune réunion sur le programme PRISM n'avait eu lieu et qu'aucun membre de la commission n'avait souhaité discuter de ce programme de surveillance de masse. Enfin, certaines entités, comme les services de renseignement, ont répondu qu'elles ne pouvaient répondre à aucune des questions pour des raisons de sécurité nationale ou d'autres motifs d'ordre confidentiel[32]. Toutes les réponses sont publiées en ligne[33].

Le Défenseur polonais des droits de l'homme a appelé à l'ouverture d'une enquête sur le programme PRISM[34]. Le 19 novembre 2013, le procureur général a informé le Défenseur des droits de l'homme qu'il n'avait pas de motif d'ouvrir une telle enquête[35].

L'Autorité irlandaise pour la protection des données a examiné la conformité de Facebook avec la loi sur la protection des données à la lumière des révélations de l'affaire Snowden. Celle-ci a rejeté la plainte d'Europe-v-Facebook.org comme étant futile et tracassière dès lors que Facebook avait agi dans le cadre des termes de l'accord de partage des données UE-États-Unis de la sphère de sécurité[36]. Le 21 octobre 2013, la Haute Cour a accepté l'appel contre la décision du commissaire à la protection des données. Il est probable qu'une audience dans cette affaire se tienne en 2014.

La Commission nationale luxembourgeoise pour la protection des données a déclaré à l'été 2013 qu'elle examinait les transferts de données vers la NSA effectués par Skype, le service de VoIP (« Voix sur IP ») et de messagerie instantanée appartenant à la société de technologie de l'information Microsoft, qui est installée aux États-Unis. En novembre 2013, la

Commission a annoncé que « le transfert de certaines catégories de données vers des sociétés affiliées aux États-Unis, tel qu'il est établi dans les politiques de confidentialité des deux entreprises, s'opère légalement, conformément aux règles applicables de la décision d'adéquation 2000/520/CE de la Commission européenne mettant en œuvre l'accord sur la sphère de sécurité ». L'autorité de protection des données n'a donc découvert aucune violation des dispositions législatives sur la protection des données par Skype ou Microsoft. Elle a souligné que sa décision ne devait pas être considérée comme confirmant ou infirmant l'existence de programmes de surveillance tel PRISM, dès lors que sa compétence est limitée aux activités des deux entreprises au Luxembourg[37].

En septembre 2013, trois organisations de la société civile et un particulier ont déposé une plainte devant la Cour européenne des droits de l'homme (CouEDH) selon laquelle les programmes de surveillance du GCHQ au Royaume-Uni violaient leur droit à la vie privée aux termes de l'article 8 de la Convention européenne des droits de l'homme. La CouEDH a transmis la plainte au gouvernement du Royaume-Uni.[38]

3.2. L'UE reconnaît la nécessité d'un régime fort pour la protection des données

Les révélations de l'affaire Snowden au printemps 2013 ont marqué un tournant dans les discussions sur la réforme de la protection des données de l'UE – en soulignant avec fermeté la nécessité d'un cadre fort pour la protection des données.

La Vice-présidente de la Commission européenne, M^me^ Viviane Reding, qui a qualifié les révélations sur la surveillance de masse de coup de tonnerre pour le législateur de l'UE, a souligné la nécessité d'un cadre fort, clair et applicable en matière de protection des données pour assurer la protection des droits fondamentaux des citoyen de l'Union.

> *« Un cadre législatif solide avec des règles claires s'appliquant aussi dans des situations où les données sont transférées et traitées à l'étranger est, plus que jamais, une nécessité. Il fournirait une certitude juridique et une protection pour les personnes et les entreprises concernées. »*
>
> *Viviane Reding, Vice-présidente, « la surveillance de masse est inacceptable – une action des États-Unis pour restaurer la confiance est maintenant nécessaire », 9 décembre 2013, Discours/13/1048, http://europa.eu/rapid/press-release_SPEECH-13-1048_en.htm*

3.2.1. Réforme du régime de protection des données dans l'UE

La mondialisation et la croissance rapide de la technologie de l'information ont modifié de manière radicale la manière dont les données à caractère personnel sont collectées et traitées depuis l'adoption en 1995 de la directive 95/46/EC[39]. Même sans les révélations de l'affaire Snowden, la nécessité de renforcer les droits fondamentaux des personnes en matière de protection des données et de stimuler l'économie du numérique dans l'Union, ce qui a conduit la Commission européenne à proposer en janvier 2012 une réforme complète de cette directive.

Le nouveau règlement général sur la protection des données[40] vise à créer un ensemble unique de règles contraignantes sur la protection des données dans l'UE. Lorsqu'il sera adopté, il remplacera la directive 95/46/CE.

Tableau 3.3 : Propositions du paquet de la réforme sur la protection des données

Instrument de l'UE	Titre	Référence	Rapport du Parlement européen
Projet de règlement	Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)	COM(2012) 11 final, Bruxelles, 25 janvier 2012	Projet de rapport du Parlement européen voté dans la commission d'enquête LIBE le 21 octobre 2013 : C7-0025/2012 – 2012/0011(COD)
Projet de directive	Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données	COM(2012) 10 final, Bruxelles, 25 janvier 2012	Projet de rapport du Parlement européen voté dans la commission d'enquête LIBE le 21 octobre 2013 : C7-0024/2012 – 2012/0010(COD)

Source : FRA, 2013

La directive sur la protection des données[41], qui remplacerait la décision sur le cadre de protection des données[42], couvre le traitement des données à caractère personnel par les autorités chargées de l'application de la loi.

En 2013, le Contrôleur européen de la protection des données (CEPD) a publié des commentaires supplémentaires[43] sur la réforme pour assurer que le nouveau régime de protection des données serait effectif en pratique. Ses commentaires venaient en réponse aux amendements proposés par différentes commissions du Parlement européen. Le groupe de travail « Article 29 » a également discuté de la réforme, celui-ci a ensuite émis un avis[44] sur le projet de directive et un document de travail[45] sur les actions de mise en œuvre du projet de règlement.

Un lobbying sans précédent de la part des entreprises américaines partisanes et des organisations de la société civile ont poursuivi le législateur européen alors que le Parlement élaborait les détails du nouveau paquet de la réforme relative aux données à caractère personnel. Le président du groupe de travail « Article 29 » n'a pas mâché ses mots lorsqu'il a résumé l'intense pression : « Les législateurs européens en avaient assez du lobbying des États-Unis »[46]. Tandis que les groupes de pression soutenaient en général les règles uniques de protection des données que le règlement établirait dans l'Union, ils s'opposaient à ce qu'ils considéraient comme une charge administrative, une responsabilité accrue, et des amendes plus élevées – pour ne citer que quelques-uns des éléments contestés.

« Ce scandale a un impact. Mais les membres du Parlement européen ont conscience que nous discutons aussi d'une question plus large : les droits fondamentaux et le respect de la vie privée en général, particulièrement lorsqu'il s'agit de la question des services secrets de l'État. [...] Un autre impact important sur le débat est que tous les membres du Parlement, hommes politiques mais aussi personnes physiques, voient maintenant l'importance d'avoir un cadre juridique commun à l'Union. Cela protège nos droits personnels, y compris sur internet. »

Jan Philipp Albrecht, Député européen, rapporteur LIBE pour le projet de règlement, Bruxelles, 26 septembre 2013

En janvier, les rapporteurs LIBE ont adopté leurs projets de rapports sur le règlement[47] et la directive[48] proposés. Quatre autres commissions du Parlement européen ont également publié des avis proposant des amendements. Après des mois de négociations sur les amendements proposés, la Commission LIBE a voté le 21 octobre 2013 par une majorité écrasante en faveur de plusieurs amendements de compromis qui, dans les grandes lignes, renforceraient les garde-fous en matière de protection des données du paquet de réforme. La séance plénière devrait adopter le paquet au printemps 2014.

Les amendements LIBE intégrés dans le projet renforcent diverses protections. Ils comprennent, par exemple, le renforcement du rôle que doit jouer le futur Comité européen pour la protection des données. Ils durcissent aussi la définition du consentement nécessaire avant le traitement des données d'une personne. Ils fusionnent le droit à la portabilité des données avec le droit à l'accès aux données, permettant ainsi aux personnes de demander que leurs données personnelles soient déplacées d'un fournisseur d'accès à un autre. Ils intègrent également le « droit à l'oubli et à l'effacement » sous le « droit à l'effacement », qui, ensemble, permettent aux personnes de demander que leurs données personnelles soient effacées d'un site internet. Les amendements de la Commission LIBE rendent aussi obligatoire maintenant la nomination d'un responsable de la protection des données pour toute entreprise traitant les données de 5 000 personnes concernées sur une période de 12 mois. Ils restreignent également les raisons rendant possible le transfert de données personnelles vers des pays situés en dehors de la zone économique européenne.

Les amendements de la Commission LIBE sont particulièrement axés sur le renforcement des Autorités nationales chargées de la protection des données (APD) qui sont requises par le droit de l'Union et fonctionnent comme la première ligne de défense face aux violations portant sur la protection des données.

La Commission LIBE a ainsi obtenu, par exemple, une indépendance accrue des APD. Leur manque d'indépendance avait polarisé les critiques ces dernières années. Les amendements de la Commission LIBE assureront que des ressources financières adéquates ainsi que le personnel nécessaire à l'exécution de leurs obligations soient attribuées aux APD. Ces avancées encourageantes suivent certains des avis de la FRA[49] qui exprimaient sa préoccupation devant le manque d'indépendance des APD. La Commission LIBE a aussi amélioré l'accès aux voies de recours en renforçant le pouvoir de sanction des APD : l'arsenal des sanctions comprend maintenant l'obligation d'effectuer des audits périodiques et les sanctions peuvent atteindre 100 millions EUR ou 5 % du chiffre d'affaires annuel global. Ces pouvoirs doivent être exercés « de manière effective, proportionnée et dissuasive ». Ces amendements ont été soutenus par les conclusions de la FRA publiées dans le rapport portant sur l'Accès aux voies de recours en matière de protection des données à caractère personnel dans les États membres de l'UE (*Access to data protection remedies in EU Member States*).

Les révélations d'Edward Snowden n'ont pas conduit le Conseil à finaliser la réforme sur la protection des données avant la fin de 2013. Les ministres de la

justice de l'Union, qui se sont rencontrés informellement en janvier et juillet 2013 (à Dublin et Vilnius, respectivement), et formellement lors des réunions des affaires intérieures et de la justice du Conseil de l'UE, ont discuté intensivement de la réforme portant sur les données. Les principaux sujets de discussion se concentrèrent sur les obligations des contrôleurs, les approches basées sur le risque, les règles spécifiques aux entreprises de petite et moyenne taille, les mécanismes de guichet unique permettant aux plaignants d'avoir accès à des voies de recours devant une seule APD, le mécanisme de cohérence et les questions concernant l'examen judiciaire et la réparation judiciaire.

ACTIVITÉ DE LA FRA

Étude de l'accès aux voies de recours en matière de protection des données dans les États membres de l'UE

La FRA a mené une recherche sur la manière dont les violations en matière de protection des données font l'objet de recours en pratique afin d'établir les principaux défis auxquels les différents acteurs font face et la manière d'améliorer l'accès à ces voies de recours. Cette recherche montre que les voies de recours les plus couramment utilisées sont les autorités chargées de la protection des données (APD) alors que les procédures judiciaires sont rarement utilisées. Mais cette étude, basée sur une analyse de cadres juridiques dans les 28 États membres de l'UE et complétée par une étude sur le terrain auprès de plus de 700 personnes dans 16 États membres de l'UE, a mis en évidence les grandes variations quant au pouvoir qu'on les APD nationales de remédier aux violations du droit à la protection des données. Alors que certaines institutions non judiciaires ont des pouvoirs suffisants pour offrir des recours effectifs, il existe une coordination minimale entre les APD et les autres institutions non judiciaires. Le projet définit d'autres domaines dans lesquels il reste du travail à faire, suggérant, par exemple, la nécessité de mesures de sensibilisation à la législation de l'UE. Les conclusions de la FRA dans son rapport sur l'*Accès aux voies de recours en matière de protection des données à caractère personnel dans les États membres de l'UE* ont nourris le travail effectuée par la Commission européenne sur les réformes proposées au droit européen de la protection des données.

Pour plus d'informations, voir : Access to data protection remedies in EU Member States, *et* Accès aux voies de recours en matière de protection des données à caractère personnel dans les États membres de l'UE - Résumé, *http://fra.europa.eu/fr/publication/2014/acces-aux-voies-de-recours-en-matiere-de-protection-des-donnees-caractere-personnel*

3.2.2. Les réformes clés affectent les autorités chargées de la protection des données

Le rôle joué par les autorités chargées de la protection des données dans l'application des garanties est essentiel. Comme d'autres institutions non judiciaires qui protègent les droits fondamentaux, leur indépendance est cruciale (voir Chapitre 8 sur l'accès à la justice et la coopération judiciaire et Chapitre 10 sur les obligations internationales des États membres de l'UE).

Comme la FRA l'a signalé dans ses rapports annuels précédents et l'a analysé dans le *Manuel de droit européen en matière de protection des données,* publié conjointement avec le Conseil de l'Europe[50], la CJUE a fait part de ses préoccupations concernant l'indépendance des APD. La CJUE a interprété la directive 95/46/CE en termes d'indépendance dans deux décisions historiques concernant l'Autriche et la Hongrie[51]. En réponse à l'arrêt de la CJUE du 16 octobre 2012, qui considérait que l'APD autrichienne manquait d'indépendance, l'**Autriche** a introduit en 2013 une législation modifiant son cadre juridique. À compter du 1er janvier 2014, une nouvelle autorité chargée de la protection des données remplace la précédente commission de protection des données[52]. Dans l'affaire *Commission c. Hongrie*, qui a aussi trait aux impératifs d'indépendance des APD, la CJUE doit formuler son jugement en 2014. L'avocat général de la CJUE a conclu le 10 décembre 2013 que la **Hongrie** avait violé le droit de l'UE en mettant fin de manière anticipée au mandat du commissaire chargé de la protection des données et a recommandé à la CJUE de déclarer que la Hongrie n'avait pas respecté les exigences d'indépendance des APD[53].

Les conséquences de la jurisprudence de la CJUE sur l'indépendance des APD ont suscité une réforme de la législation nationale dans d'autres États membres également. Le Parlement **letton** a travaillé à des amendements à la loi sur la protection des données à caractère personnel[54] à la fin de 2013. Ces amendements précisent les tâches et la compétence de l'Inspection nationale des données, en particulier dans le domaine des plaintes liées à la violation des droits en matière de protection des données. En **Lituanie** a été approuvé, le 27 novembre 2013, le nouveau règlement renforçant l'indépendance de l'Inspection nationale des données[55]. Aux termes de ce règlement, c'est maintenant l'administrateur qui est chargé de la structure administrative des APD, qui relevait précédemment du gouvernement. Celui-ci agit désormais en totale indépendance. Le Parlement **slovaque** a voté le 30 avril 2013 une loi sur la protection des données qui améliore la transposition de la directive sur la protection des données[56]. En **Pologne**, l'établissement de succursales locales de l'autorité chargée

de la protection des données, afin de décentraliser l'institution et de la rendre plus accessible aux personnes concernées et vivant en dehors de Varsovie (seul siège actuel) fut le changement clé discuté au niveau national. Cependant un manque de fonds a, jusqu'à ce jour, empêché cette réalisation.

Le rapport de la FRA de 2010 sur *La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données* considérait que la procédure de nomination des APD grecques consistait une pratique encourageante[57]. La constitution grecque exige une majorité des quatre-cinquièmes de la Conférence des présidents, instrument parlementaire, pour que soit approuvée la nomination des membres de toutes les autorités indépendantes, y compris de l'APD grecque. Cette pratique existe toujours. Du fait de l'absence d'un large consensus parmi les forces politiques du Parlement actuel, cependant, il n'est pas toujours possible d'atteindre le consensus nécessaires à ces nominations. Cette question a affecté d'autres autorités indépendantes mais pas l'APD grecque.

3.2.3. Sensibiliser le public à la protection des données

Le méconnaissance des garanties existantes concernant la protection des données est la conclusion essentielle du rapport de la FRA sur l'*Accès aux voies de recours en matière de protection des données dans les États membres de l'UE*. Pour pallier ce manque, la FRA et le Conseil de l'Europe ont finalisé la publication d'un manuel facile à utiliser et plusieurs APD dans différents États membres de l'UE ont lancé des projets, parmi lesquels la publication de fascicules visant à sensibiliser les jeunes sur la question de la protection des données pour qu'ils soient mieux informés de leurs droits.

ACTIVITÉ DE LA FRA

Une présentation simplifiée du droit sur la protection des données de l'UE et du Conseil de l'Europe

La FRA, le Conseil de l'Europe et la CouEDH ont rédigé un *Manuel de droit européen en matière de protection des données* qui détaille le droit européen de la protection des données issu de l'UE et du Conseil de l'Europe. Conçu pour des professionnels du droit non spécialisés dans ce domaine, ce manuel examine le droit de la protection des données issus des deux systèmes européens, y compris avec une sélection d'arrêts importants.

Pour plus d'informations, voir : Manuel de droit européen en matière de protection des données, http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law

Pratiques encourageantes

Sensibiliser et lutter contre l'abus de données à caractère personnel relatives à des enfants

Dans plusieurs États membres, les APD mettent en œuvre diverses activités visant spécifiquement à protéger les enfants (voir le Chapitre 4 sur les droits de l'enfant et la protection de l'enfant).

Le Commissaire fédéral allemand à la protection des données et à la liberté d'information pour la Rhénanie-Palatinat a lancé le premier site d'APD allemand ciblant explicitement les jeunes. Il sensibilise aux questions de la protection des données et dispense des connaissances sur la manière de protéger les données à caractère personnel en général et sur l'internet en particulier. Il propose des suggestions concrètes sur la manière de protéger les données personnelles lors de l'utilisation de médias sociaux ou de consoles de jeu.

Pour plus d'informations, voir : www.youngdata.de

L'Autorité nationale hongroise pour la protection des données et la liberté de l'information a publié un manuel sur la protection des données destiné aux enfants[58]. Son objectif est d'attirer l'attention sur les risques encourus par les enfants, et plus particulièrement les jeunes de 10 à 16 ans, lorsque ceux-ci utilisent internet. Ce manuel cherche à déterminer les défis futurs liés à l'utilisation du net, à promouvoir une utilisation responsable d'internet et à encourager le plein exercice du droit à la vie privée.

Pour plus d'informations, voir : Autorité nationale pour la protection des données et la liberté de l'information (2013), Clés pour le monde d'internet!, www.naih.hu/files/2013-projektfuzet-internet.pdf

3.2.4. Réforme et mise en œuvre de la directive sur la conservation des données

L'UE poursuit son travail de révision de la directive sur la conservation des données à caractère personnel[59] qui encourage la lutte contre la criminalité et le terrorisme en exigeant des fournisseurs d'accès qu'ils conservent les données de localisation et de trafic sur une durée allant de six mois à deux ans à compter de la date de la communication.

Plusieurs États membres ont amendé leur législation tandis que d'autres mettaient en doute la légalité des lois adoptées dans le cadre de la transposition dans la législation nationale de la directive sur la conservation des données. Le gouvernement **Belge**, par exemple, a adopté un arrêté royal transposant la directive sur la conservation des données dans le droit belge[60]. En **Pologne**, un amendement législatif au droit des communications

a réduit la durée de conservation des données de 24 à 12 mois et interdit la conservation des données dans les procédures civiles[61]. Le Parlement **danois** a décidé de reporter la révision des règles sur la conservation des données jusqu'à la session parlementaire 2014–2015 afin d'attendre la révision de la directive sur la conservation des données[62]. Le commissaire **slovène** à l'information a demandé une révision constitutionnelle de la nouvelle loi sur les communications électroniques régissant la conservation des données qui est entrée en vigueur en janvier 2013[63]. Selon la Cour constitutionnelle, cette tâche relève de la compétence exclusive de la CJUE, elle a donc retardé la révision jusqu'à ce que la CJUE ait statué sur les deux affaires jointes de l'Irlande et de l'Autriche, respectivement C-293/12 et C-594/12[64].

Le 12 décembre 2013, un avocat général de la CJUE a publié ses conclusions sur les affaires jointes de l'Irlande[65] et de l'Autriche[66] concernant la directive sur la conservation des données. Les décisions préliminaires concernaient la compatibilité de la directive sur la conservation des données avec les droits fondamentaux. Pour l'avocat général : «la directive sur la conservation des données est dans son ensemble incompatible avec l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne dès lors que les limitations à l'exercice des droits fondamentaux qu'elle comporte, du fait de l'obligation de conservation des données qu'elle impose, ne s'accompagnent pas des principes indispensables appelés à régir les garanties nécessaires à l'encadrement de l'accès auxdites données et de leur exploitation ».

3.2.5. Google

Politique de Google en matière de respect de la vie privée

Le 20 juin 2013, l'APD **française** a ordonné à Google de se conformer à la loi française sur la protection des données à caractère personnel dans un délai de trois mois. Google n'ayant pas obtempéré, l'APD française a entamé une procédure formelle d'application de sanctions, infligeant à Google le 3 janvier 2014 une amende de 150 000 EUR[67].

En juillet 2013, l'APD du **Royaume-Uni** a déclaré que la politique de Google en matière de respect de la vie privée soulevait des préoccupations sérieuses quant à sa conformité avec la loi sur la protection des données et que par conséquent, l'APD du Royaume-Uni avait lancé une enquête[68]. L'Office du Commissaire à l'information (ICO) a quant à lui ordonné à Google de réviser d'ici le 20 septembre sa politique en matière de respect de la vie privée pour la rendre plus accessible[69]. En l'absence de modifications, l'ICO pourrait prendre des mesures coercitives officielles mais à la fin de la période considérée, l'APD n'avait pris aucune mesure.

Le 19 décembre 2013, l'autorité **espagnole** chargée de la protection des données a infligé à Google une amende de 300 000 EUR pour avoir violé la loi espagnole sur la protection des données, déclarant que Google avait effectué des traitements d'informations illégaux grâce à sa nouvelle politique en matière de respect de la vie privée[70].

Moteurs de recherche de Google

En **Allemagne**, la Cour de justice fédérale a statué en faveur de plaignants qui demandaient que Google désactive une fonction de son moteur de recherche qui aboutissait à l'affichage automatique de termes compromettants lorsque les noms des plaignants étaient tapés dans le champ de recherche de Google. Le Tribunal ne s'attendait pas à ce que Google prenne des mesures de précaution pour empêcher que les effets indésirables de cette fonction se produisent encore. Les juges ont décidé, cependant, que l'entreprise doit examiner les plaintes des personnes concernées et faire cesser l'affichage de termes, appelés « prédictions », apparaissant dans la recherche avec le nom d'une personne, si cela est nécessaire afin de protéger la vie privée des plaignants[71].

Dans une autre affaire, une personne qui souhaitait que certaines données soient effacées de la page d'un journal publié en ligne a déposé une réclamation auprès de l'Autorité espagnole chargée de la protection des données (AEPD). Dans cette affaire, l'APD espagnole a considéré que les données étaient publiées de manière licite et a refusé d'ordonner leur retrait. L'affaire a été portée devant la Haute Cour nationale espagnole (*Audiencia Nacional*), qui a présenté une série de questions préliminaires à la CJUE. Le 25 juin 2013, l'avocat général de la CJUE a communiqué son avis dans l'affaire *Google c. AEPD*.[72] Celui-ci a conclu que Google n'était pas responsable des informations ou de la diffusion des données composant les résultats d'une recherche. Il a refusé de qualifier Google de « contrôleur » des données à caractère personnel selon la signification donnée par la directive sur la protection des données et a, enfin, considéré que la directive n'assure pas de droit général à l'oubli. La CJUE rendra son arrêt en 2014.

Google Street View

En juillet 2013, Google a commencé à photographier les rues de **Slovénie** pour son application Google Street View. Le Commissaire à l'information a signalé que Google s'était engagé à adopter des mesures visant à réduire l'interférence avec la vie privée qui se produit inévitablement dans de telles occasions. Ces mesures comprennent, entre autres : informer le public régulièrement sur la localisation des voitures de Google ; fournir plus d'informations sur cette application ; flouter les visages et les plaques d'immatriculation sur les photographies avant leur publication ; installer des boutons « signaler une erreur » dans chaque image ; introduire des procédures de sécurité et des mesures visant à la protection des données collectées ; former les chauffeurs et adapter les calendriers de tournage et les lieux[73].

3.3. Société de l'information : l'UE propose de protéger et de codifier les droits fondamentaux en ligne

Les technologies modernes ont un impact considérable sur la protection des droits fondamentaux en ce qu'elles présentent de nouvelles voies pour réaliser pleinement ces droits tout en posant aussi de nouveaux défis pour leur protection. Les révélations d'Edward Snowden sur la surveillance de masse ont fourni un exemple marquant en 2013. Pour la première fois en 2013, le Forum sur la gouvernance d'internet[74] a organisé une séance plénière sur les droits de l'homme sur internet. L'accès à internet et son utilisation du point de vue des droits de l'homme ont été au centre des discussions. Il a été unanimement admis que les droits de l'homme et la liberté d'expression en ligne devaient rester une priorité de l'ordre du jour du Forum sur la gouvernance[75].

3.3.1. La protection des droits fondamentaux en ligne

La protection des droits fondamentaux dans l'environnement numérique est une question très controversée. Au niveau universel, il est maintenant admis que les droits de l'homme sont protégés de la même manière en ligne et dans le monde physique[76]. Au niveau régional, le Conseil de l'Europe a adopté cette approche, affirmant dans sa Stratégie sur la gouvernance d'internet que la législation en matière de droits de l'homme est autant applicable en ligne qu'hors ligne[77]. L'UE a aussi accepté dans sa Stratégie de cybersécurité que les valeurs fondamentales de l'UE s'appliquent tant dans le cyberespace que dans le monde réel et que les droits fondamentaux inscrits dans la Charte des droits fondamentaux de l'UE doivent être promus au sein du cyberespace[78].

« Pour que le cyberespace reste libre et ouvert, les normes, principes et valeurs que l'UE défend hors ligne doivent aussi s'appliquer en ligne. »

Cecilia Malmström, Commissaire européenne chargée des Affaires intérieures, « Présentation de la stratégie de cybersécurité visant à protéger une Europe interconnectée », 16 mai 2013, Discours/13/423, http://europa.eu/rapid/press-release_SPEECH-13-423_en.htm?locale=en

La Stratégie de cybersécurité de la Commission européenne met en évidence les tâches respectives des acteurs clés tant au sein du secteur public que du secteur privé : les gouvernements ont besoin de sécuriser l'accès et l'ouverture d'internet, de respecter et de protéger les droits fondamentaux en ligne et de maintenir la fiabilité et l'interopérabilité d'internet. En parallèle, le rôle prépondérant du secteur privé, qui détient et exploite des parties importantes du cyberespace, devra être reconnu si l'on veut de garantir la réussite de toute initiative dans ce domaine[79].

3.3.2. Codifier les droits fondamentaux en ligne

La contribution du secteur privé est essentielle quand il s'agit de la mise en œuvre des droits fondamentaux en ligne. En effet, les représentants du secteur privé, conjointement avec les personnes concernées, les ONG et les acteurs gouvernementaux, travaillent ensemble sur tous les sujets liés au développement d'internet. En 2013, le suivi d'une approche multi-parties prenantes a permis d'obtenir des résultats concrets dans la codification des droits fondamentaux en ligne. Le projet de guide des droits de l'homme pour les utilisateurs d'internet par le Conseil de l'Europe et la Charte des droits de l'homme et principes pour internet ont été publiés. En outre, l'UE a publié le Code des droits en ligne dans l'UE. Le Tableau 3.4 présente les similitudes et différences existant entre ces deux textes.

La proposition de la Commission européenne d'un règlement fixant des mesures concernant le marché unique européen des communications électroniques et visant à faire de l'Europe un continent connecté[80] établit la liberté des utilisateurs finaux d'accéder à des informations et à des contenus et de les distribuer, d'exploiter des applications et d'utiliser les services de leur choix par l'intermédiaire de leur fournisseur d'accès à internet. Elle vise à garantir un internet véritablement libre et ouvert en interdisant aux opérateurs de bloquer, ralentir, dégrader ou exercer une discrimination à l'encontre de contenus, applications et services ou catégories particuliers , à l'exception d'un nombre très limité de cas où une opération raisonnable de gestion du trafic peut être appliquée. Ces mesures doivent être transparentes, non-discriminatoires et proportionnées.

Le Code des droits en ligne dans l'UE[81], publié le 21 décembre 2012, n'établit pas de droits nouveaux et n'est pas non plus directement exécutoire. Il résume et consolide les droits existants dérivant de la législation de l'Union sur les communications électroniques, le commerce électronique, la protection des données et la protection des consommateurs. Conformément à ce code, les droits fondamentaux inscrits dans la Charte des droits fondamentaux de l'UE doivent être respectés et le caractère ouvert et neutre d'internet doit être préservé.

La Charte des droits de l'homme et principes pour l'internet est le document phare de la Coalition dynamique droits et principes d'internet[82]. Cette coalition fait partie du Forum sur la gouvernance d'internet qui fournit à toutes les parties prenantes un espace neutre permettant de discuter des questions liées à la gouvernance d'internet[83]. La coalition est composée de chercheurs, de juristes, de militants, d'ONG, d'organisations intergouvernementales et de fournisseurs d'accès à internet. La Charte s'appuie sur les normes existantes en matière de droits de l'homme, notamment la Déclaration universelle des droits de l'homme. Elle doit être un document de politique

Tableau 3.4 : Codification des droits fondamentaux en ligne

Nom	Auteur	Base juridique	Capacité juridique	Objectif	Droits concernés
Code des droits en ligne dans l'UE	Commission européenne (Ordre du jour numérique, action 16)	Législation de l'UE sur la communication électronique, le commerce électronique, la protection des données à caractère personnel et la protection des consommateurs	Il n'établit pas de droits nouveaux et n'est non plus directement exécutoire. Il consolide les droits existants minimaux.	Sensibiliser les consommateurs et accroître leur confiance, afin de promouvoir l'utilisation de services en ligne	Droits et principes applicables lors de l'accès et de l'utilisation de services en ligne Droits et principes applicables à de l'achat de biens ou de services en ligne Droits et principes protégeant les consommateurs en cas de conflit
Charte des droits de l'homme et principes pour internet	Coalition dynamique droits et principes d'internet	Déclaration universelle des droits de l'homme et autres accords qui composent la Charte internationale des droits de l'homme des Nations Unies	Non contraignant	Fournir un point de référence pour le dialogue et la coopération entre les différentes parties prenantes, document qui peut encadrer des décisions de politique pour les dimensions locales, nationales et mondiales de la gouvernance d'internet et outil de sensibilisation pour les gouvernements, les entreprises et la société civile	Droit d'accès à internet, droit à la non-discrimination dans l'accès à internet, l'utilisation et la gouvernance, la liberté et la sécurité, le développement grâce à internet, la liberté d'expression et d'information, la liberté de religion et de croyance, la liberté de réunion en ligne, le droit à la vie privée, la protection des données numériques, l'accès à la connaissance, les droits des enfants, les droits des personnes handicapées, le droit au travail, la participation aux affaires publiques, la protection des consommateurs, la santé et les services sociaux, des voies de recours juridique et un procès équitable pour des actes impliquant internet, un ordre social et international adéquat pour l'internet, devoirs et responsabilités sur 'internet, clauses générales
Guide des droits de l'homme pour les utilisateurs d'internet	Comité des Ministres du Conseil de l'Europe	Convention européenne des droits de l'homme et autres conventions et instruments du Conseil de l'Europe tels qu'interprétés par la Cour européenne des droits de l'homme	Non contraignant. Il ne crée pas de droits nouveaux. Il s'agit d'une explication ni exhaustive ni prescriptive des normes des droits de l'homme	Sensibiliser. Pouvant être utile à tout utilisateur d'internet, sans connaissances spécialisées, afin de comprendre et profiter de ses droits en ligne	Accès et non-discrimination, liberté d'expression et d'information, de réunion, d'association et de participation, respect de la vie privée et protection des données à caractère personnel, éducation et alphabétisme, enfant et jeunes, recours effectifs

Source : FRA, 2013

pour toutes les parties prenantes. Elle est sous-tendue par l'idée que chacun a le droit d'avoir accès à internet et de l'utiliser. À partir des consultations en vue de la Charte, la coalition a aussi compilé les « dix droits et principes » qui doivent constituer le socle de la gouvernance d'internet[84]. Certains de ces principes, tels que la liberté d'expression, la protection de la vie, de la liberté, de la sécurité et de la vie privée, sont enracinés dans les droits fondamentaux.

Conformément à la Stratégie du Conseil de l'Europe 2012-2015 sur la gouvernance d'internet[85], le Conseil de l'Europe a finalisé un projet de guide des droits de l'homme pour les utilisateurs d'internet[86]. Ce guide vise à informer et à aider les utilisateurs d'internet à comprendre et à exercer les droits qu'ils ont en ligne. Il ne crée pas de droits nouveaux mais il s'ajoute aux droits inscrits dans la CEDH et d'autres documents du Conseil de l'Europe, tels qu'ils sont interprétés par la CouEDH. Ce guide donne des informations sur leur application aux environnements en ligne. Il doit être adopté par le Comité des Ministres du Conseil de l'Europe en 2014.

3.3.3. Responsabilité des entreprises

Le résultat du modèle multi-parties prenantes qui sous-tend la gouvernance d'internet est que les acteurs du secteur privé jouent un rôle important dans la sauvegarde des droits fondamentaux dans l'environnement numérique. Les principes directeurs des Nations Unies sur le monde des affaires et les droits de l'homme ont été largement acceptés et sont maintenant un point de référence global pour les affaires et les droits de l'homme. Ils sont basés sur les trois piliers des Nations Unies « protéger, respecter, remédier » qui sont : le devoir de l'État de fournir une protection contre les violations des droits de l'homme par des tiers, y compris les entreprises ; la responsabilité pour les entreprises de respecter les droits de l'homme, ce qui signifie à la fois éviter les violations des droits de l'homme et traiter les conséquences négatives lorsque des entreprises sont impliquées dans ces violations ; et la nécessité d'un meilleur accès aux voies de recours effectives des victimes de violations des droits de l'homme liées aux entreprises, tant par des moyens judiciaires que non judiciaires (voir le Chapitre 10 sur les États membres et les obligations internationales)[87].

Dans le cadre de sa politique en matière de responsabilité des entreprises[88], la Commission européenne a publié trois guides en juin 2013, appliquant les principes directeurs des Nations Unies dans les secteurs suivants : agences de recrutement et pour l'emploi, technologies de l'information et des communications (TIC) et pétrole et gaz. Le guide du secteur des TIC[89] n'est pas un instrument juridiquement contraignant mais il a été conçu pour être utile à toutes les entreprises de ce secteur, en les aidant à mettre ces principes efficacement en œuvre dans leur politique. En particulier, ce guide établit les éléments clés que les entreprises pourront mettre en place afin de garantir le respect des droits de l'homme: l'élaboration de plans d'actions engagés visant à faire respecter les droits de l'homme ; une étude d'impact des droits de l'homme au sein de l'entreprise, dont les conclusions doivent ensuite être prises en compte ; la mise en place d'un suivi et d'une communication sur la manière avec laquelle ces impacts pourront être efficacement traités; et enfin des mécanismes de recours. Pour chacun de ces éléments, le guide résume ce que prévoient les principes directeurs des Nations Unies, il explique en quoi cela est important et donne ensuite des orientations en indiquant les approches possibles que l'entreprise pourrait utiliser pour s'attaquer au problème. Il propose aussi une liste de ressources visant à fournir des informations complémentaires et donne des exemples pris dans la vie quotidienne des entreprises : comment une entreprise de TIC utilise des icônes pour informer les utilisateurs sur des questions liées à la vie privée ou comment une entreprise de télécommunications a élaboré un contrat cadre mondial.

3.3.4. Responsabilité intermédiaire

Dans quelle mesure un portail web peut-il être tenu pour responsable du contenu téléchargé par les utilisateurs de blogs ou de sites d'informations ? Cela est sujet à débat et soulève la question de l'objectif de la responsabilité intermédiaire, particulièrement dans le cas de commentaires diffamatoires postés par ces lecteurs. La CouEDH a rendu un jugement dans l'affaire *Delfi AS c. Estonie*[90] qui a généré une inquiétude considérable parmi les acteurs d'internet. La Cour a soutenu que tenir un portail pour responsable des commentaires répréhensibles postés par des lecteurs au-dessous de l'un des articles mis en ligne constituait une restriction justifiée et proportionnée du droit de ce portail à la liberté d'expression.

En **Pologne**, la Cour suprême administrative[91] a considéré qu'une personne a le droit de demander à un fournisseur d'accès internet de divulguer les adresses électroniques et celles des protocoles internet associées aux communications en ligne répréhensibles parce que ces données sont nécessaires pour que les victimes d'une violation du droit à la vie privée en ligne puissent revendiquer efficacement leur droit devant le tribunal. Les fournisseurs d'accès à internet avaient pour la plupart allégué le fait que, selon le droit du commerce électronique[92], seules des autorités chargées de l'application des lois pouvaient avoir accès à ces données et que les tribunaux avaient généralement accepté cet argument. La Cour suprême administrative, cependant, a jugé que les fournisseurs d'accès internet devaient permettre aux personnes d'avoir accès à ces données si cette divulgation répond à un but légitime et est proportionnée aux circonstances d'une affaire donnée.

Au **Royaume-Uni**, la Cour d'appel a rendu sa décision dans l'affaire *Tamiz c. Google*[93] au sujet de la responsabilité de Google concernant des commentaires

diffamatoires postés sur un blog hébergé par le service de blogs de Google. La Haute Cour avait soutenu que Google ne pouvait pas être considéré comme un éditeur en raison de son rôle passif par rapport aux mentions et aux commentaires d'un blog. La Cour d'appel a soutenu la majeure partie de ces conclusions. Cependant, elle a analysé de manière différente la période suivant la notification de la plainte, concluant que Google aurait très bien pu devenir un éditeur puisqu'il permettait aux commentaires diffamatoires de rester sur le blog après la notification. L'appel a toutefois été rejeté, car le tribunal a jugé que le dommage pour la réputation du demandeur était négligeable.

Beaucoup considèrent l'affaire *Google-Vividown* comme l'affaire **italienne** la plus significative en ce qui concerne les droits sur internet. En février 2013, la Cour d'appel a renversé la décision de première instance qui avait condamné trois dirigeants de Google à six mois de prison parce que le moteur de recherche de Google avait diffusé une vidéo montrant un garçon handicapé se faire brutaliser. La Cour d'appel a considéré que le responsable était la personne qui avait mis la vidéo en ligne, et non le site hébergeur.

3.3.5. Le droit à une voie de recours efficace

ACTIVITÉ DE LA FRA

Obtenir des voies de recours en matière de violation en ligne du droit à la protection des données à caractère personnel

En 2014, la FRA a publié un rapport sur l'Accès aux voies de recours en matière de protection des données à caractère personnel dans les États membres de l'UE qui examine les mécanismes des voies de recours possibles pour traiter les violations du droit à la protection des données. Ce rapport identifie les défis auxquels sont confrontées les personnes et propose des améliorations. Les violations de la protection des données à caractère personnel les plus fréquentes mentionnées lors du travail de recherche sur le terrain dans 16 États membres de l'UE concernent des activités liées à internet. Celles-ci comprennent les médias sociaux, les achats en ligne, la fuite de données à caractère personnel depuis un site de e-commerce, le piratage d'un compte de messagerie ou d'une base de données, l'usurpation d'identité, les atteintes à la sécurité et l'utilisation abusive de données à caractère personnel par des multinationales présentes sur le net. C'est la raison pour laquelle des voies de recours efficaces sur internet doivent être mises en place (voir aussi la Section 3.2.3).

Pour de plus amples informations, voir : FRA (2014), Accès aux voies de recours en matière de protection des données à caractère personnel dans les États membres de l'UE – Résumé, *Luxembourg, Office des publications*

Le caractère unique d'internet ne modifie pas le principe selon lequel les victimes de violations des droits fondamentaux ont besoin d'avoir accès à des voies de recours. Le droit à une voie de recours effective est inscrit dans tous les documents principaux mentionnés dans le cadre des droits fondamentaux des utilisateurs d'internet. La fréquente violation de droits en ligne rend indispensable l'existence de mécanismes de recours dans le domaine de la société de l'information. En même temps, le rôle crucial que joue le secteur privé dans la gouvernance d'internet est à l'origine des défis concernant la mise en œuvre appropriée de voies de recours.

Pratique encourageante

En France, l'APD a créé un document en ligne, consultable sur son site internet et intitulé « Comment effacer des informations me concernant sur un moteur de recherche? ». Cette fiche de conseils fournit les instructions quant à la procédure à suivre, et un modèle de lettre à envoyer à l'administrateur du site, ainsi que des informations sur la procédure en vue de la désindexation volontaire du site web.

Pour de plus amples informations, voir : www.cnil.fr/documentation/fiches-pratiques/fiche/article/comment-effacer-des-informations-me-concernant-sur-un-moteur-de-recherche/

3.3.6. Lutte contre la cybercriminalité

L'UE a adopté en 2013 un certain nombre d'initiatives visant à renforcer la lutte contre la cybercriminalité. Dans la majorité des cas, les activités criminelles commises en ligne aboutissent à des violations des droits de l'homme et des libertés fondamentales. La Stratégie de l'UE en matière de cybersécurité, adoptée le 7 février 2013, établit comme l'un de ses principes les plus importants la protection des droits fondamentaux, de la liberté d'expression, des données à caractère personnel et de la vie privée et exprime l'opinion selon laquelle les droits des « personnes » ne peuvent être garantis sans des réseaux et des systèmes sécurisés. Dans le même temps, cette stratégie ne pourra être valable et efficace que si elle est basée sur les libertés et les droits fondamentaux inscrits dans la Charte des droits fondamentaux de l'Union européenne et les valeurs de l'UE.

Les principaux exemples de violation des droits de l'homme et des libertés fondamentales par des activités criminelles commises en ligne sont la production et la diffusion de contenus portant sur l'abus sexuel d'enfants, qui est une violation grave des droits des enfants, et les intrusions dans des systèmes informatiques, ce qui, dans la plupart des cas, a un impact direct sur la vie privée des utilisateurs et/ou se traduit par une atteinte à la protection des données.

Pour intensifier la lutte contre la cybercriminalité avec comme objectif une meilleure protection des droits

fondamentaux des citoyens, le législateur européen a adopté le 12 août 2013 une directive sur les attaques contre les systèmes d'information. Cette directive complète la directive 2011/93/UE déjà adoptée le 13 décembre 2011, qui introduit des mesures communes contre les abus sexuels et l'exploitation sexuelle d'enfants et la pédopornographie.

De plus, un Centre européen de lutte contre la cybercriminalité (EC3) a été créé en janvier 2013 au sein d'Europol afin de devenir le point focal en Europe de la lutte contre la cybercriminalité. Celui-ci a pour tâche principale d'aider et de coordonner les enquêtes transfrontalières en matière de cybercriminalité dans les trois domaines prioritaires suivants : les crimes de haute technologie (cyberattaques, logiciels malveillants), l'exploitation sexuelle des enfants en ligne et la fraude des moyens de paiement.

Les conclusions de trois grandes enquêtes de la FRA sur les personnes lesbiennes, gaies, bisexuelles et transgenres (LGBT), sur la violence contre les femmes et sur l'antisémitisme révèlent que les manifestations en ligne de crimes de haine sont un problème de plus en plus sérieux car internet peut servir de plateforme de diffusion de la haine et du harcèlement. L'anonymat qu'internet permet d'obtenir peut conduire certains utilisateurs à publier en ligne du contenu répréhensible.

Les conclusions de l'enquête de la FRA sur les personnes LGBT dans l'UE[94] ont montré que dans les 12 mois précédant l'enquête, une personne sur cinq (19 %) sur l'ensemble des personnes interrogées a été victime de harcèlement, qu'elle pensait lié en partie ou entièrement au fait qu'elle était perçue comme une personne LGBT[95]. Presqu'un incident sur 10 (9 %) des incidents les plus récents de harcèlement dû à la haine et 6 % des expériences les plus sérieuses de discrimination se sont produits en ligne[96].

Les données de l'enquête réalisée par la FRA sur la violence à l'égard des femmes[97] montrent qu'une femme sur 10 (11 %) dans l'UE a été victime de cyberharcèlement au moins une fois depuis l'âge de 15 ans, et 5 % au cours des 12 mois précédant l'enquête. Le risque pour des jeunes femmes âgées de 18 à 29 ans de devenir la cible d'avances menaçantes ou répréhensibles sur internet est deux fois plus élevé que pour les femmes âgées de 40 à 49 ans, et plus de trois fois plus élevé que pour les femmes âgées de 50 à 59 ans. Sur la base de l'enquête de la FRA, 5 % des femmes dans l'UE ont fait l'objet d'une ou plusieurs formes de traque furtive sur l'internet[98] depuis l'âge de 15 ans, et 2 % au cours des 12 mois précédant l'enquête. En tenant compte de l'âge de la victime, les chiffres sur 12 mois varient de 4 % pour les 18–29 ans à 0,3 % pour les femmes âgées de 60 ans et plus.

L'enquête de la FRA sur la discrimination et les crimes de haine contre les juifs[99] indique de la même manière que les victimes voient l'antisémitisme en ligne comme un problème sérieux. Les trois quarts de toutes les personnes interrogées (75 %) le voient comme un problème soit « très grand » soit « plutôt grand » et presque autant (73 %) estiment qu'il a augmenté au cours des cinq dernières années. Dans l'ensemble, 10 % des personnes interrogées ont fait l'objet de commentaires antisémites répréhensibles ou menaçants sur internet.

Au **Royaume-Uni**, deux personnes qui ont fait des commentaires abusifs et menaçants sur Twitter contre une militante féministe ont été condamnés à douze et huit semaines de prison[100]. La destinataire des tweets contenant des menaces a toutefois qualifié cette affaire de « petite goutte dans l'océan » en comparaison avec les discours de haine qu'elle et d'autres femmes avaient subis en ligne. Cette affaire est un exemple des problèmes aigus auxquels nous devons faire face et du défi qui nous attend pour trouver des solutions par des moyens juridiques traditionnels.

ACTIVITÉ DE LA FRA

S'attaquer à la cyberhaine

La FRA a organisé sa conférence annuelle 2013 sur les droits fondamentaux sur le thème du crime de haine, avec un atelier consacré à la cyberhaine. L'atelier de la conférence, qui a eu lieu à Vilnius les 12 et 13 novembre 2013, a examiné les problèmes liés à la montée de la cyberhaine, les défis pour la combattre, les bonnes pratiques et les solutions possibles. Les points clés soulevés comprennent la nécessité de renforcer l'éducation, la formation et le cyber alphabétisme pour tous les acteurs, y compris l'application du droit, les utilisateurs, les entreprises et les gouvernements, ainsi que d'augmenter la transparence et le reporting pour une plus grande sensibilisation. Ces objectifs pourraient être atteints par la réduction de l'anonymat des utilisateurs, tout en assurant la protection des données. Le discours haineux en ligne étant une préoccupation globale, une approche commune est nécessaire. Il convient d'harmoniser les différences entre les législations et les codes pénaux de sorte que les victimes soient toutes traitées selon des règles égales. Il convient aussi d'établir des normes minimales portant sur ce qui n'est absolument pas admis. D'autres propositions concernaient l'élaboration de mécanismes pour le signalement de contenu indésirable qui vont au-delà de la poursuite judiciaire du discours haineux. Pour sensibiliser les jeunes et répondre au défi que représente l'impunité, les participants ont fortement suggéré d'instituer des cyber acteurs d'application de la loi, dans des services, du contenu privés et chez des fournisseurs de plateformes, comme un médiateur pour Facebook. Parmi les bonnes pratiques signalées se trouvent les lignes secours pour les enfants au **Royaume-Uni**, des policiers affectés à la répression de la cyberhaine en **Finlande**, des campagnes de sensibilisation au **Danemark** et une unité de police fédérale en **Belgique** travaillant dans les écoles et sensibilisant les victimes potentielles.

Une action est nécessaire pour empêcher un mauvais usage d'internet pris comme une zone dans laquelle le crime de haine peut être commis en toute impunité. L'UE et ses États membres doivent identifier les moyens efficaces et les pratiques encourageantes pour répondre aux préoccupations croissantes concernant la haine en ligne. Cela est d'autant plus nécessaire que la nature du crime de haine en ligne signifie que le problème n'est pas limité par les frontières des États membres mais est au contraire un problème transfrontalier auquel il convient de s'attaquer conjointement (voir le ▶ Chapitre 6 sur le racisme et la discrimination ethnique).

Au niveau national, les États membres de l'UE se sont aussi engagés activement pour garantir le respect des droits de l'homme dans l'environnement numérique et promouvoir des campagnes de sensibilisation. En **Autriche**, le conseil consultatif sur la société de l'information sous la tutelle de la Chancellerie fédérale s'est réuni quatre fois en 2013[101] pour discuter des développements pertinents au niveau européen et au niveau mondial, tels l'agenda numérique de la Commission européenne pour l'Europe[102], le Paquet Télécom[103], le Forum sur la gouvernance de l'Internet et le Dialogue européen sur la gouvernance de l'internet (EuroDIG)[104], et au niveau national, tels le renforcement de la sécurité de l'information en Autriche et la garantie d'un internet plus sûr. Dans ce contexte, la Journée pour un internet plus sûr le 5 février 2013 était axée sur les droits et les responsabilités en ligne. Le gouvernement **français** a annoncé sa feuille de route sur le numérique à la fin de février[105]. En plus de propager l'utilisation des technologies de l'information et des communications (TIC) parmi les jeunes et d'accroître la compétitivité des entreprises grâce aux technologies numériques, la feuille de route vise à assurer la protection des libertés civiles sur internet.

Pratique encourageante

Décourager les comportements à risque des enfants en ligne

L'initiative **espagnole** « Tu choisis », qui cible les enfants âgés de 10 à 15 ans, utilise des fiches d'exercices et une bande dessinée pour faire réfléchir les élèves aux conséquences possibles des actions qu'ils effectuent en ligne. L'accent est mis sur les réseaux sociaux et les situations à risque, comme la cyberintimidation et le harcèlement sexuel en ligne.

Pour de plus amples informations, voir : www.agpd.es/portalwebAGPD/index-ides-idphp.php

ACTIVITÉ DE LA FRA

Mettre des chiffres sur la violence exercée contre les femmes

L'enquête de la FRA menée dans toute l'UE sur la violence exercée contre les femmes montre que 5 % des femmes dans l'UE ont fait l'objet d'une ou plusieurs formes de cyberharcèlement depuis l'âge de 15 ans, et pour 2 % d'entre elles dans les 12 mois précédant l'enquête. Par comparaison avec une moyenne de 2 % de cyberharcèlement pour toutes les femmes, celles qui faisaient partie du groupe d'âge le plus jeune (dans l'enquête : 18–29 ans) étaient les plus touchées. Pour ces femmes, le cyberharcèlement correspond à la majeur partie du harcèlement qu'elles ont connu au cours des 12 mois précédant l'enquête.

Trois éléments spécifiques de l'enquête ont été examinés au titre de la cyberintimidation : l'envoi de courriels, de textos (SMS) ou de messages instantanés qui étaient répréhensibles ou menaçants ; la mise en ligne de commentaires répréhensibles sur le répondant sur l'internet ; le partage de photos ou de vidéos intimes du répondant, sur l'internet ou grâce à un téléphone portable. Pour que ces incidents soient considérés comme de l'intimidation, il faut qu'ils se soient produits plusieurs fois et que la même personne les ait commis.

Perspectives

Le scandale sur la surveillance de masse qui a miné la confiance des utilisateurs d'internet et violé leur droit à la vie privée influera sur l'élaboration des politiques en 2014. La manière dont la confiance des utilisateurs dans les technologies de l'information et les communications sera restaurée dominera les débats liés à la société de l'information, au respect de la vie privée et à la protection des données à caractère personnel. Les révélations de l'affaire Snowden se traduiront nécessairement par des appels à un plus grand respect des droits fondamentaux en ligne, dans les discussions relatives à la gouvernance de l'internet. Les initiatives de suivi, lancées en 2013, nécessiteront une implication accrue des décideurs et du secteur privé, avec des acteurs du secteur privé qui doivent s'engager davantage dans l'application des droits fondamentaux.

Au niveau de l'UE, le paquet relatif à la réforme sur la protection des données restera parmi les premières préoccupations du législateur européen. Le Conseil de l'Union européenne et le Parlement européen après les élections devront entrer rapidement dans des négociations pour rendre possible l'adoption de la réforme d'ici la fin de 2014. Les arrêts de la CJUE continueront aussi à donner des lignes directrices sur la manière d'amender la législation, comme ceux prononcés sur la directive sur la conservation des données, en précisant le champ d'application des garanties liées à la protection des données et en éclairant la question de l'indépendance nécessaire des autorités chargées de la protection des données.

Index des références aux États membres

Notes

Tous les liens hypertexte ont été consultés le 30 avril 2014.

1 Bigo, D., Carrera, S., Hernanz, N. Jeandesboz, J., Parkin, J., Ragazzi, F. et Scherrer, A. (2013), *Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law*, Article CEPS dans Liberté et Sécurité en Europe n° 61, novembre 2013, p. 2.

2 Nations Unies (ONU), Conseil des droits de l'homme (2013), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, paras. 50 et 51, 17 avril 2013, www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

3 Assemblée générale de l'ONU (2013), Resolution 68/167 on the right to privacy in the digital age, 18 décembre 2013, www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167.

4 Conseil de l'Europe, Comité des Ministres (2013), *Declaration of the Committee of Ministers on risks to fundamental rights stemming from digital tracking and other surveillance technologies*, 11 juin 2013, wcd.coe.int/ViewDoc.jsp?id=2074317&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383.

5 Conseil de l'Europe, Commissaire du Conseil de l'Europe (2013), « Le développement de la surveillance secrète menace les droits de l'homme », *Le carnet des droits de l'homme du Commissaire du Conseil de l'Europe*, 24 octobre 2013, http://fr.humanrightscomment.org/2013/10/24/le-developpement-de-la-surveillance-secrete-menace-les-droits-de-lhomme/.

6 Conseil de l'Europe, Conférence des ministres responsables des medias et de la société de l'information (2013), « Liberté d'expression et démocratie à l'ère du numérique, opportunités, droits, responsabilités », déclaration, 8 novembre 2013, www.coe.int/t/dghl/standardsetting/media/belgrade2013/Belgrade%20Ministerial%20Conference%20Texts%20Adopted_en.pdf.

7 *Ibid.*, p. 1.

8 Parlement européen (2013), Résolution portant sur le programme de surveillance de l'agence nationale de sécurité américaine, les organismes de surveillance dans divers États membres et leur impact sur le droit à la vie privée des citoyens de l'UE , 4 juillet 2013, www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2013-0322&language=FR.

9 Parlement européen (2013), Projet de rapport Moraes, www.europarl.europa.eu/sides/getDoc.do?pubRef=%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-526.085%2b02%2bDOC%2bPDF%2bV0%2f%2fEN.

10 Commission européenne (2000), Décision 2000/520/EC relative à la pertinence de la protection assure par les principes de la «sphère de sécurité» et par les questions souvent posées y afférents, publiées par le ministère du commerce des États-Unis d'Amérique, 26 juillet 2000, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML.

11 Conseil de l'Union européenne (2013), Rapport sur les conclusions des co-présidents de l'UE du groupe de travail ad hoc UE-États-Unis sur la protection des données, Doc. 16987/13, Bruxelles, 27 novembre 2013.

12 Commission européenne (2013), *Communication au Parlement européen et au Conseil – Restaurer la confiance dans les flux de données UE-États-Unis*, COM(2013) 846 final, Bruxelles, 27 novembre 2013; Commission européenne (2013), *Communication 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 final, Bruxelles, 27 novembre 2013.

13 Commission européenne (2013), *Communication 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 final, Bruxelles, 27 novembre 2013.

14 Commission européenne (2013), *Communication au Parlement européen et au Conseil – Restaurer la confiance dans les flux de données UE-États-Unis*, COM(2013) 846 final, Bruxelles, 27 novembre 2013.

15 Finlande, « Kyllä me voimme - Laki sananvapauden ja yksityisyydensuojan kansainvälisestä turvaamisesta (Lex Snowden) », www.kansalaisaloite.fi/fi/aloite/442.

16 Allemagne, Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2013), « Entschließung: Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen », Résolution, 5 septembre 2013, www.datenschutz.bremen.de/sixcms/detail.php?gsid=bremen236.c.9292.de.

17 Demonstration "Freiheit statt Angst" (2013), Bündnispartner 2013, http://blog.freiheitstattangst.de/bundnispartner-2013/.

18 Spiegel Online (2013), « NSA-Protest in Berlin. Freiheit unterm Alu-Hut », 7 septembre 2013, www.spiegel.de/netzwelt/netzpolitik/freiheit-statt-angst-2013-demonstration-gegen-nsa-ueberwachung-a-920927.html.

19 Demonstration Freiheit statt Angst (2013), *Unsere Forderungen*, http://blog.freiheitstattangst.de/unsere-forderungen/.

20 Spiegel Online (2013), « Proteste am Dagger Complex. Mit Lampions gegen die NSA », 1er septembre 2013 ; Deutsche Welle (2013), « Verhaltener Protest gegen NSA-Überwachung », 30 juillet 2013, www.dw.de/verhaltener-protest-gegen-nsa-%C3%BCberwachung/a-16986575.

21 Deutsche Welle (2013), « Cryptoparties boom following NSA scandal », 20 juillet 2013, www.dw.de/cryptoparties-boom-following-nsa-scandal/a-16964049.

22 France, Loi n° 2013-1168 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, 18 décembre 2013, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&dateTexte=&categorieLien=id.

23 Hongrie, *Egyes törvényeknek a nemzetbiztonsági ellenőrzés új szabályainak megállapítása érdekében szükséges módosításáról szóló 2013. évi LXXII. törvény.*

24 Untersinger, M. (2013) « Surveillance d'Internet : inquiétudes autour de la loi de programmation militaire », *Le Monde*, 26 novembre 2013, www.lemonde.fr/technologies/article/2013/11/26/

surveillance-d-internet-inquietudes-autour-de-la-loi-de-programmation-militaire_3518974_651865.html ; voir aussi : Hongrie, *Társaság a Szabadságjogokért*, http://tasz.hu/adatvedelem/megfigyelessel-korrupcio-ellen.

25 France, Conseil National du Numérique (2013), *Avis sur les libertés numériques n° 2013-5*, 6 décembre 2013, www.cnnumerique.fr/libertes-numeriques/.

26 Hongrie, *Nemzeti Adatvédelmi és Információszabadság Hatóság, NAIH-4867-4/2012/J* ; lettre de réponse fournie pour les besoins du présent rapport par l'Autorité nationale chargée de la protection des données à caractère personnel et de la liberté de l'information à la demande datée du 24 novembre 2013.

27 Hongrie, *Alkotmánybíróság, 32/2013. (XI. 22.) AB határozat*, 22 novembre 2013.

28 Allemagne, Bundesregierung (2013), « NSA-Aufklärung. Deutschland ist ein Land der Freiheit », communiqué de presse, 19 juillet 2013, www.bundesregierung.de/ContentArchiv/DE/Archiv17/Artikel/2013/07/2013-07-19-bkin-nsa-sommerpk.html.

29 Pays-Bas, Commissie evaluatie Wiv 2002 (2013), « Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002 », www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2013/12/02/rapport-evaluatie-wiv-2002.html.

30 Slovénie, Ministrstvo za pravosodje (2013), « Sporočila za javnost po 35. redni seji Vlade RS », communiqué de presse, 28 novembre 2013, www.mp.gov.si/si/novinarsko_sredisce/novica/select/sporocilo_za_javnost/article/12447/6713/592f3cdc597266ddb17c10a531c7e0e6/?tx_ttnews%5Byear%5D=2013&tx_ttnews%5Bmonth%5D=11.

31 Finlande, Helsińska Fundacja Praw Człowieka (2013), « 100 pytań o inwigilację do polskich władz », communiqué de presse, 16 octobre 2013, www.hfhr.pl/100-pytan-o-inwigilacje-do-polskich-wladz.

32 La Fondation Helsinki pour les droits de l'homme (FHDH) s'est plainte du refus du Bureau central anti-corruption de fournir certaines des informations demandées et a demandé aux autres services de renseignement qui ont refusé de donner des informations de reconsidérer cette requête.

33 Finlande, Helsińska Fundacja Praw Człowieka (2013), « Amerykański program PRISM – odpowiedzi na wnioski o informację publiczną », 6 décembre 2013, www.hfhrpol.waw.pl/precedens/aktualnosci/amerykanski-program-prism-odpowiedzi-na-wnioski-o-informacje-publiczna.html.

34 Pologne, Rzecznik Praw Obywatelskich (2013), « Wystąpienie do Prokuratora Generalnego w sprawie zapobiegania sytuacjom nieautoryzowanego przetwarzania danych osobowych polskich internautów », RPO/738662/13/I/115.2 RZ, 23 septembre 2013.

35 Pologne, Prokurator Generalny (2013), PG K01 2353/13, 19 novembre 2011.

36 Irish Times (2013), « Facebook decision can be reviewed », 24 octobre 2013, www.irishtimes.com/business/sectors/technology/facebook-decision-can-be-reviewed-1.1571049.

37 Luxembourg, Commission nationale pour la protection des données (2013), « Pas de violation constatée en matière de protection des données de la part de Skype et Microsoft au Luxembourg », communiqué de presse, 18 novembre 2013, www.cnpd.public.lu/fr/actualites/national/2013/11/skype-microsoft/index.html.

38 CEDH, *Big Brother Watch et autres c. le Royaume-Uni*, N° 58170/13, communiqué le 9 janvier 2014; voir aussi CEDH, *Centrum för Rättvisa c. la Suède*, n° 35252/08.

39 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, JO 1995 L 281.

40 Commission européenne (2012), *Proposition de règlement du Parlement européen et du Conseil 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 (règlement sur la protection des données)*, COM(2012) 11 final, Bruxelles, 25 janvier 2012.

41 Commission européenne (2012), *Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales, et à la libre circulation de ces données*, COM(2012) 10 final, Bruxelles, 25 janvier 2012.

42 Conseil de l'Union européenne (2008), Décision-cadre 2008/977/JHA 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 (décision-cadre sur la protection des données), JO 2008 L 350.

43 Contrôleur européen de la protection de données (2013), *Commentaires supplémentaires du CEPD relatifs au paquet de réformes sur la protection des données à caractère personnel*, 20 mars 2013.

44 Groupe de travail « Article 29 » (2013), *Avis 01/2013 apportant une contribution supplémentaire aux discussions sur la proposition de directive relative à la protection des données traitées dans les domaines de la police et de la justice pénale*, WP 201, 26 février 2013.

45 Groupe de travail « Article 29 » (2013), *Document de travail 01/2013 Contribution au débat sur les propositions d'actes d'exécution*, WP 200, 22 janvier 2013.

46 Financial Times, 4 février 2013.

47 Parlement européen, Commission des libertés civiles, de la justice et des affaires intérieures (2013), *Projet de rapport sur la proposition d'un règlement du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et la libre circulation de ces données* (Règlement sur la protection des données), 16 janvier 2013.

48 Parlement européen, Commission des libertés civiles, de la justice et des affaires intérieures (2012), Projet de rapport sur la proposition d'une directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par des autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales, et à la libre circulation de ces données , 20 décembre 2012.

49 Agence des droit fondamentaux de l'Union

européenne (FRA) (2010), *La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données*, Luxembourg, Office des publications de l' Union européenne (Office des publications) ; voir aussi : FRA (2012), *Avis de l'Agence des droits fondamentaux de l'Union européenne concernant le programme de réforme des règles en matière de protection des données à caractère personnel*, Vienne, 1er octobre 2012 ; FRA (2014), *Access to data protection remedies in EU Member States*, Luxembourg, Office des publications ; FRA (2014), *Accès aux voies de recours en matière de protection des données à caractère personnel dans les États membres de l'UE – Résumé*, Luxembourg, Office des publications.

50 FRA (2014), *Manuel de droit européen en matière de protection des données,* Luxembourg, Office des publications.

51 CJUE, C-518/07, *Commission européenne c. République fédérale d'Allemagne*, 9 mars 2010, CJUE, C-614/10, *Commission européenne c. République d'Autriche*, 16 octobre 2012.

52 Autriche , *83. Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2014),* 23 mai 2013, www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2013_I_83/BGBLA_2013_I_83.html.

53 CJUE, C-288/12, *Commission européenne c. Hongrie,* Avis de l'avocat général, 10 décembre 2013.

54 Lettonie, *Likumprojekts 'Grozījumi Fizisko personu datu aizsardzības likumā'*, http://titania.saeima.lv/LIVS11/saeimalivs11.nsf/0/B0CA8FC1A876870BC2257C310050C997?OpenDocument.

55 Lithuanie, LR Vyriausybė (2013) *Nutarimas dėl Valstybinės duomenų apsaugos inspekcijos administracijos struktūros tvirtinimo*, n. 1082, 27 novembre 2013.

56 Slovaquie, *Zákon č. 122/2013 Z.z. o ochrane osobných údajov*, 30 avril 2013.

57 FRA (2010), *La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données*, Luxembourg, Office des publications.

58 Hongrie, Autorité nationale chargée de la protection des données et de la liberté de l'information (2013), *Key to the World of the Internet!*, www.naih.hu/files/2013-projektfuzet-internet.pdf.

59 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/EC, JO 2006 L 105, Bruxelles.

60 Belgique, *Koninklijk besluit tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie/Arrêté royal portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques*, 19 septembre 2013, www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2013091920&table_name=loi.

61 Pologne, *Ustawa o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw*, 16 novembre 2012.

62 Danemark, Politi og Strafferetsafdelingen, *Report on various questions regarding the Danish data retention regulations*, affaire n° 2012-187-0020, document n° 549331, www.ft.dk/samling/20121/almdel/reu/bilag/125/1200765.pdf.

63 Slovénie, *Zakon o elektronskih komunikacijah*, ZEKom-1, 20 décembre 2012.

64 Slovénie, *Ustavno sodišča Republike Slovenije*, U-I-65/13-16, 26 septembre 2013, .

65 CJUE, C-293/12, Demande de décision préjudicielle présentée par la High Court of Ireland, le 11 juin 2012 – *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General*, 25 août 2012.

66 CJUE, C-594/12, Demande de décision préjudicielle présentée par la Cour constitutionnelle d'Autriche, 19 décembre 2012.

67 France, Commission nationale de l'informatique et des libertés (CNIL) (2014), Délibération n° 2013-420, 3 janvier 2014: www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000028450267&fastReqId=2000051504&fastPos=1.

68 Royaume-Uni, Information Commissioner's Office (ICO) (2013), *ICO statement regarding investigation into Google privacy policy,* déclaration, 2 avril 2013, www.ico.org.uk/news/latest_news/2013/ico-statement-investigation-google-privacy-policy-02042013.

69 Royaume-Uni, ICO (2013), *ICO update on Google privacy policy,* déclaration, 4 juillet 2013, www.ico.org.uk/news/latest_news/2013/ico-update-on-google-privacy-policy-04072013.

70 Espagne, Agencia Española de Protección de Datos (AEPD) (2013), « The AEPD sanctions Google for serious violation of the rights of the citizens », communiqué de presse, 19 décembre 2013.

71 Allemagne, Bundesgerichtshof (2013), « Bundesgerichtshof entscheidet über die Zulässigkeit persönlichkeitsrechtsverletzender Suchergänzungsvorschläge bei «Google» », communiqué de presse n° 87/2013, 14 mai 2013, http://juris.bundesgerichtshof.de/cgibin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&nr=64071&linked=pm.

72 CJUE, C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González,* 25 juin 2013, http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1090622.

73 Slovénie, Informacijski pooblaščenec (2013), « Snemanje ulic za storitev Google Street View », communiqué de presse, 2 juillet 2013, www.ip-rs.si/novice/detajl/snemanje-ulic-za-storitev-google-street-view/?cHash=2113761ece703e0badf20352fa2faa35.

74 Voir : Internet Governance Forum, www.intgovforum.org/cms/.

75 8ème réunion du Forum sur la gouvernance d'internet, résumé du président, p. 16.

76 Nations Unies, Conseil des droits de l'homme (2012), *Resolution 20/8 on the promotion, protection and enjoyment of human rights on the Internet*, http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/G12/153/25/PDF/G1215325.pdf?OpenElement ; UNESCO (2013), *First WSIS+10 Review Event, Final Recommendations*, 27 février 2013, p. 3, www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/wsis/

WSIS_10_Event/wsis10_recommendations_en.pdf. In November 2013 ; 195 pays de l'UNESCO ont approuvé les recommandations finales; voir aussi : Assemblée générale des Nations Unies (2013), Resolution 68/167 on the right to privacy in the digital age, 18 décembre 2013, www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167.

77 Conseil de l'Europe, Comité des Ministres (2011), *Internet Governance Strategy 2012-2015*, CM(2011)175 final, 15 mars 2012.

78 Commission européenne (2013), *Stratégie de cybersécurité de l'Union européenne : un cyberspace ouvert, sûr et sécurisé*, Joint COM(2013) 1 final, Bruxelles, 7 février 2013, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:EN:PDF.

79 Commission européenne (2013), *Stratégie de cybersécurité de l'Union européenne : un cyberspace ouvert, sûr et sécurisé*, Joint COM(2013) 1 final, Bruxelles, 7 février 2013.

80 Proposition d'un règlement établissant des mesures relatives à un marché unique européen des communications électroniques et visant à faire de l'Europe un continent connecté, et modifiant les directives 2002/20/CE, 2002/21/CE et 2002/22/CE et les règlements (CE) n° 1211/2009 et (UE) n° 531/2012; COM(2013) 0627 final, https://ec.europa.eu/digital-agenda/en/news/regulation-european-parliament-and-council-laying-down-measures-concerning-european-single.

81 Commission européenne (2012), *Code des droits en ligne dans l'UE*, https://ec.europa.eu/digitalagenda/sites/digitalagenda/files/Code%20EU%20online%20rights%20EN%20final%202.pdf.

82 Internet Rights and Principles Coalition (2013), *Charter for Human Rights and Principles for the internet, (version 2.0)*, http://internetrightsandprinciples.org/site/wpcontent/uploads/2013/10/IRP_booklet_final1.pdf.

83 Voir : Internet Governance Forum, www.intgovforum.org/cms/.

84 Internet Rights and Principles Coalition (2011), *10 internet rights and principles*, http://internetrightsandprinciples.org/images/IRPflyer.pdf.

85 Conseil de l'Europe, Comité des Ministres (2011), *Internet Governance Strategy 2012-2015*, CM(2011)175 final, 15 mars 2012.

86 Conseil de l'Europe, Committee of Experts on Rights of Internet Users (2013), *Draft recommendation of the Committee of Ministers to member states on a guide on human rights for Internet users*, MSI DUI (2013)07Rev7, 6 décembre 2013.

87 Nations Unies, Bureau du Haut commissariat aux droits de l'homme (2011), *Guiding Principles on Business and Human Rights – Implementing the United Nations "Protect, Respect and Remedy" Framework*, New York et Genève, .

88 Commission européenne (2011), *Communication au Parlement européen, au Conseil, au Comité européen économique et social et au Comité des régions – Une nouvelle stratégie de l'UE pour la période 2011–14 : responsabilité sociale des entreprises*, COM(2011) 681 final, Bruxelles, 25 octobre 2011.

89 Commission européenne (2013), *Guide du secteur des TIC concernant la mise en oeuvre des principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme*, juin 2013, www.ihrb.org/pdf/eu-sector-guidance/EC-Guides/ICT/EC-Guide_ICT.pdf.

90 Cour européenne des droits de l'homme (CouEDH), *Delfi AS c. Estonie*, n° 64569/09, 10 octobre 2013, affaire pendant devant la Grande Chambre de la CouEDH.

91 Pologne, *Naczelny Sąd Administracyjny*, I OSK 1666/12, 21 août 2013.

92 Pologne, *Ustawa o świadczeniu usług drogą elektroniczną,* 18 juillet 2012.

93 Royaume-Uni, Court of Appeal (2013), *Tamiz c. Google*, EWCA Civ 68, www.bailii.org/ew/cases/EWCA/Civ/2013/68.html.

94 L'enquête de la FRA sur les personnes LGBT dans l'UE a été réalisée en ligne dans les 27 États membres de l'UE et en Croatie entre avril et juillet 2012. Cette enquête a collecté des informations auprès de 93 079 personnes âgées de 18 ans et plus qui se considèraient comme lesbiennes, gays, bisexuelles ou transgenre, et qui vivaient dans l'UE ou en Croatie.

95 FRA (2013), *Enquête sur les personnes LGBT dans l'UE – Enquête sur les personnes lesbiennes, gays, bisexuelles et transgenres dans l'Union européenne – Les résultats en bref,* Luxembourg, Office des publications, p. 23, http://fra.europa.eu/en/publication/2013/eu-lgbt-survey-european-union-lesbian-gay-bisexual-and-transgender-survey-results.

96 FRA (2014), *EU LGBT survey: Main results,* Luxembourg, Office des publications.

97 L'enquête de la FRA sur la violence exercée contre les femmes a interrogé (entretiens face-à-face) 42 000 femmes, qui avaient entre 18 et 74 ans et habitaient dans l'un des 28 États mebres (environ 1 500 par pays). Les répondants étaient sélectionnés à partir d'un échantillonnage aléatoire. Les données ont été collectées entre avril et juillet 2012. Voir : FRA (2014), *Violence against women – an EU-wide survey. Main results,* Luxembourg, Office des publications et FRA (2014), *La violence à l'égard des femmes : une enquête à l'échelle de l'UE – Les résultats en bref*, Luxembourg, Office des publications, http://fra.europa.eu/fr/publication/2014/violence-femmes-enquete-ue-resultats-en-bref.

98 Trois éléments spécifiques de l'enquête ont été examinés au titre de la cyberintimidation : l'envoi de courriels, de textos (SMS) ou de messages instantanés qui étaient répréhensibles ou menaçants ; la mise en ligne de commentaires répréhensibles sur le répondant sur l'internet ; le partage de photos ou de vidéos intimes du répondant, sur l'internet ou grâce à un téléphone portable. Pour que ces incidents soient considérés comme de l'intimidation, il faut qu'ils se soient produits plusieurs fois et que la même personne les ait commis.

99 L'enquête de la FRA sur la discrimination et les crimes de haine contre les personnes juives a été menée en ligne dans huit États membres : la Belgique, la France, l'Allemagne, la Hongrie, l'Italie, la Lettonie, la Suède et le Royaume-Uni en septembre et octobre 2012. L'enquête s'est appuyée sur 5 847 personnes juives s'étant identifiés comme telles âgées de 16 ans et plus. FRA (2013), *Discrimination and hate crime against Jews in EU Member States: experience and perceptions of antisemitism,* Luxembourg, Office des publications, http://fra.europa.eu/sites/default/files/fra-2013-discrimination-hate-crime-against-jews-eu-member-states_en.pdf.

100 Royaume-Uni, BBC News (2014), « Two guilty over abusive tweets to Caroline Criado-Perez », 7 janvier 2014, www.bbc.com/news/uk-25641941.

101 Autriche, Beirat für Informationsgesellschaft (2013), www.bka.gv.at/site/4293/default.aspx.

102 Commission européenne (2010), *Un agenda numérique pour l'Europe*, COM(2010) 245 final, Bruxelles, 26 août 2010, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245:EN:NOT.

103 Commission européenne (2013), *Communication de la Commission au Parlement européen, au Conseil, au Comité européen économique et social et au Comité des régions relative au marché unique des télécommunications*, COM(2013) 634, Bruxelles, 11 septembre 2013, https://ec.europa.eu/digital-agenda/en/news/communication-commission-european-parliament-council-european-economic-and-social-committee-a-0.

104 Voir : European Dialogue on Internet Governance, www.eurodig.org/.

105 France, portail Web du gouvernement, www.gouvernement.fr/premier-ministre/le-gouvernement-presente-la-feuille-de-route-pour-le-numerique.