EUROPEAN DATA PROTECTION SUPERVISOR

Avis nº 8/2015

Diffusion et utilisation de technologies de surveillance intrusive

15 décembre 2015

Le contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'UE chargée en vertu de l'article 41, paragraphe 2, du règlement nº 45/2001 «[e]n ce qui concerne le traitement de données à caractère personnel, [...] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, soient respectés par les institutions et organes communautaires», et «[...] de conseiller les institutions et organes communautaires et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel». Le contrôleur européen et le contrôleur adjoint ont été nommés en décembre 2014 avec comme mission spécifique d'être plus constructifs et proactifs. Le CEPD a publié en mars 2015 une stratégie quinquennale exposant la manière dont il entend mettre en œuvre ce mandat et en rendre compte.

Le présent avis fait suite au précédent avis du CEPD sur le règlement général sur la protection des données qui visait à aider les principales institutions de l'UE à trouver un consensus sur un ensemble de règles réalisables et orientées vers l'avenir qui renforce les droits et les libertés des personnes physiques. Dans le présent avis, comme il l'avait fait dans l'avis sur la santé mobile publié début 2015, le CEPD aborde le défi du passage en «mode numérique» de la protection des données – le troisième objectif de la stratégie du CEPD – en «visant à adapter les principes de protection des données au monde numérique», compte tenu également des projets de l'UE concernant le marché unique numérique. L'avis est conforme à l'approche du groupe de travail «Article 29» sur les aspects de l'utilisation des nouvelles technologies liés à la protection des données, comme l'«internet des objets», à laquelle le CEPD a contribué en tant que membre à part entière du groupe.

Dans le présent avis, le CEPD aborde les questions que la diffusion et l'utilisation de technologies de surveillance intrusive soulèvent en matière de protection des données et de respect de la vie privée.

Résumé

Dans le présent avis, le CEPD aborde les questions que la diffusion et l'utilisation de technologies de surveillance intrusive soulèvent en matière de protection des données et de respect de la vie privée. L'utilisation de ces outils suppose, par défaut, le traitement de données à caractère personnel et une possible intrusion dans la vie privée de personnes: les outils de surveillance intrusive visent principalement à infiltrer des systèmes informatiques à distance (généralement via l'internet) en vue d'opérer un contrôle clandestin des activités de ces systèmes informatiques et, au fil du temps, de retourner des données à l'utilisateur des outils de surveillance.

Si ces outils peuvent être utiles dans le cadre d'un usage légitime (et réglementé) par les organes chargés de l'application de la loi ou les services de renseignement, ils peuvent également être utilisés comme des «chevaux de Troie» à des fins de contournement des mesures de sécurité entourant les communications électroniques et le traitement des données.

Il est nécessaire que les politiques de l'UE, les politiques nationales et tous les acteurs intervenant dans le secteur des technologies de l'information et des communications («TIC») (développeurs, prestataires de services, vendeurs, intermédiaires, distributeurs et utilisateurs) abordent la question de la tension existant entre, d'une part, l'utilisation positive d'outils informatiques, et d'autre part, l'incidence négative que l'utilisation abusive de la technologie peut avoir sur les droits de l'homme, et en particulier sur la protection des données à caractère personnel et le respect de la vie privée.

Dans le présent avis, le CEPD propose d'aborder la menace que constitue l'utilisation de technologies de surveillance intrusive par la mise en œuvre des actions suivantes:

- il conviendrait d'examiner les normes européennes existantes en matière de TIC, en vue de renforcer la protection des droits de l'homme, particulièrement dans le cas de l'exportation de technologies d'interception ou de surveillance et de services dans ce domaine;
- l'utilisation et la diffusion (y compris au sein de l'UE) d'outils de surveillance et d'interception, et de services dans ces domaines, devraient faire l'objet d'une réglementation adaptée tenant compte du risque de violation de droits fondamentaux, et en particulier des droits au respect de la vie privée et à la protection des données;
- le Conseil de l'UE, le Parlement européen, la Commission européenne et le Service européen pour l'action extérieure devraient concevoir des politiques cohérentes et plus efficaces concernant l'exportation d'outils de surveillance intrusive dans le cadre des technologies à double usage, à l'échelle de l'UE et à l'échelle internationale;
- les politiques mises à jour devraient réglementer les vulnérabilités et les exploits «jour zéro» afin d'éviter que ceux-ci ne soient utilisés à des fins de violation des droits fondamentaux;
- les politiques sur la cybersécurité de l'UE devraient tenir compte de la diffusion des technologies d'interception et de surveillance et aborder cette question de manière spécifique dans le cadre de la législation adaptée;
- les investissements dans le domaine de la sécurité sur l'internet et les initiatives de prise en compte du respect de la vie privée dès la conception de nouvelles solutions technologiques devraient être encouragés;

- il conviendrait d'établir une approche cohérente pour accorder une protection internationale aux dénonciateurs qui contribuent à révéler l'existence de violations des droits de l'homme commises en utilisant des technologies d'interception et de surveillance.

TABLE DES MATIÈRES

1 Le contexte

Au début du mois de juillet 2015[1], une entreprise italienne a été victime d'une violation de données de grande ampleur. Les auteurs de l'attaque ont volé un volume important de données (plus de 400 gigaoctets, d'après les indications communiquées) qu'ils ont publiées sur l'internet. Les données publiées comportaient des documents internes, des enregistrements audio, des correspondances électroniques, des mots de passe d'employés, des listes de clients et, plus important dans le cadre du présent avis, des informations techniques et le code source d'un logiciel de surveillance intrusive perfectionné.

Selon les médias[2], ce logiciel de surveillance intrusive permettrait à son utilisateur de contourner les cryptages, de recueillir des données à partir de quelque dispositif que ce soit et de contrôler une cible clandestinement et à distance[3]. En outre, les clients potentiels seraient les organes chargés de l'application de la loi et les services de renseignement, l'offre étant limitée, dans le même temps, aux gouvernements ou pays ne figurant pas sur les listes noires des États-Unis, de l'UE, de l'ONU, de l'OTAN ou de l'ASEAN[4]. Cependant, les médias[5] ont indiqué que le logiciel aurait pu être vendu aux «gouvernements et aux services de renseignement de l'Azerbaïdjan, du Kazakhstan, de l'Ouzbékistan, de la Russie, du Bahreïn, de l'Arabie saoudite et des Émirats arabes unis qui, pour nombre d'entre eux, ont été critiqués par des organisations internationales de défense des droits de l'homme en raison de la surveillance agressive qu'ils exercent à l'égard de citoyens, de militants et de journalistes sur leur territoire national et à l'étranger».

Plusieurs entreprises sont des acteurs de ce segment du domaine de la cybersécurité et fournissent des services dans ce domaine[6]. D'autres entreprises[7], qui évoluent dans la même sphère d'activités, opèrent dans le secteur de la cybersécurité en commercialisant des éléments désignés par le nom d'«exploits» (chapitre **Error! Reference source not found.**) qui permettent d'utiliser les outils de surveillance intrusive au mieux de leur capacité. Le modèle d'affaire de ces entreprises consiste à fournir aux clients les capacités techniques nécessaires pour réaliser des attaques de systèmes informatiques.

Dans le présent avis, le CEPD se concentre sur le cas spécifique des outils de surveillance intrusive qui sont conçus, commercialisés et vendus à des fins de surveillance (de masse), d'intrusion et d'exfiltration. Ces outils sont utilisés pour attaquer les systèmes de cibles définies. Le CEPD n'aborde pas le débat politique plus large concernant une éventuelle réglementation des technologies en matière de sécurité des réseaux et de l'information, comme la limitation du cryptage[8] et l'obligation d'affaiblissement des systèmes de sécurité par l'utilisation de portes dérobées[9].

2 Concepts et implications techniques

Les outils de surveillance intrusive visent principalement à infiltrer des systèmes informatiques à distance (à savoir, via l'internet) en vue d'opérer un contrôle clandestin des activités de ces systèmes informatiques et, au fil du temps, de retourner des données à l'utilisateur des outils de surveillance. Pour comprendre la manière dont cet objectif est réalisé, il est possible de diviser les explications relatives aux outils de surveillance intrusive en deux parties: la partie concernant la gestion (chapitre 2.1) et les exploits (chapitre 2.2). Nous examinerons ensuite plusieurs conséquences techniques clés liées à l'utilisation de ce type de logiciel (chapitre 2.3).

2.1 Partie concernant la gestion des outils d'intrusion et de surveillance

En substance, la partie concernant la gestion des outils de surveillance intrusive peut être définie comme un logiciel perfectionné destiné à gérer l'infiltration de cibles et à fournir des exploits aux utilisateurs (voir également chapitre 2.2) concernant les cibles qui les intéressent dans un langage clair.

Généralement, l'utilisateur dispose d'une interface graphique qui lui permet d'accomplir les actions suivantes:

- saisir l'adresse IP (protocole internet) d'un système informatique connecté à l'internet (la cible) afin de recueillir des données de base sur cette cible, comme le type de système d'exploitation [en anglais, «Operating System» (OS)] en cours d'utilisation, les services en cours d'utilisation (à titre d'exemples, serveur internet, serveur de messagerie), des informations de géolocalisation, etc. Cette première étape est utile afin de définir la meilleure façon d'attaquer cette cible;

- gérer et lancer des attaques de cibles en vue d'infiltrer ces cibles et d'y recueillir des données. Les attaques peuvent prendre de nombreuses formes, mais elles sont généralement effectuées en utilisant des exploits (examinés au chapitre 2.2);

- une fois que la cible est infiltrée, en poursuivre la compromission (à savoir, tenter de contourner les mesures de sécurité locales mises en place pour protéger la cible, en utilisant d'autres exploits, en vue de pouvoir effectuer davantage d'opérations, obtenir des droits d'accès ou accéder à un plus grand nombre de données gérées par la cible) et installer un petit logiciel (comparable à un cheval de Troie[10]) qui recueillera des données et les enverra à l'utilisateur des outils de surveillance;

- utiliser une cible compromise pour lancer une attaque contre une autre cible qui lui est connectée;

- procéder au suivi des cibles qui ont déjà été infiltrées et des données reçues/exfiltrées de ces cibles. L'obtention de ces données est la motivation principale de l'utilisation d'outils de surveillance intrusive et ces données peuvent inclure toutes les données traitées par la cible, comme les données de navigation sur l'internet provenant de tout navigateur utilisé sur cette cible, les courriers électroniques envoyés et reçus, les fichiers enregistrés sur les disques durs auxquels la cible a accès (que ces fichiers soient situés sur la cible elle-même ou dans d'autres systèmes informatiques auxquelles la cible a accès), tous les journaux de connexion enregistrés, toutes les pressions exercées sur des touches du clavier (ces données permettent de recueillir des mots de passe), des captures d'écran de ce que l'utilisateur de la cible voit sur son propre écran, des captures des flux vidéo et audio des webcams et des microphones connectés à la cible, etc.

Cette liste de fonctionnalités n'est naturellement pas exhaustive. Cependant, elle devrait être suffisante pour analyser les conséquences de l'utilisation de ces outils dans le cadre du présent avis.

2.2 Exploits

Les exploits sont de petits éléments logiciels, des suites de commandes ou des données destinés à tirer profit d'une faille/vulnérabilité du logiciel du système informatique ciblé pour

provoquer une réaction involontaire et imprévue de ce logiciel. Souvent, l'objectif est de concevoir l'exploit d'une manière telle que la réaction automatique du logiciel attaqué permette à l'auteur de l'attaque d'accéder à la cible ou d'en acquérir un certain contrôle.

Un exploit ne peut exister que si le logiciel concerné présente une faille/vulnérabilité. Les failles/vulnérabilités sont identifiées au fil du temps par les chercheurs, les éditeurs de logiciels et le public et elles peuvent se produire dans tout logiciel comme MS Windows, Linux, Mac OS X, Android, Apple iOS, Blackberry OS ou tout autre système d'exploitation, ainsi que dans tout logiciel utilisé en combinaison avec l'internet et via l'internet, comme Adobe Flash (utilisé par un grand nombre de sites web comme YouTube, Google, etc.), Firefox, Safari, Internet Explorer, etc.

En règle générale, lorsqu'un éditeur de logiciels apprend que son produit présente une faille/vulnérabilité, il est en mesure de corriger cette dernière et de fournir au public une nouvelle version du logiciel. Une fois que le logiciel mis à jour est installé sur un système informatique, l'exploit correspondant ne peut plus nuire au système informatique.

L'expression «exploits "jour zéro"» est utilisée pour désigner les exploits qui utilisent une faille/vulnérabilité dont l'éditeur du logiciel n'a pas connaissance et pour laquelle il n'existe pas de correctif. Ces types d'exploits sont précieux étant donné qu'ils pourront très probablement être utilisés pour attaquer avec succès un système utilisant le logiciel défaillant correspondant. Les prix des exploits peuvent aller au-delà de 100 000 euros et dépendent de nombreux facteurs techniques[11].

Dans le cas de Hacking Team, l'un des exploits dont les médias se sont largement fait l'écho se rapportait au logiciel Adobe Flash[12]. Cet exploit nuisait à la version qui était alors la plus récente du logiciel Adobe Flash et qui était utilisée par toute une gamme de plateformes et de navigateurs. Il permettait à l'auteur de l'attaque d'exécuter le programme qu'il voulait sur la cible. Le scénario d'attaque ci-après aurait été un scénario crédible:

- un utilisateur navigue sur le web en utilisant une version vulnérable d'Adobe Flash installée sur son ordinateur. L'utilisateur accède à un site web contenant le contenu Adobe Flash (comme une vidéo) qui, lui-même, contient l'exploit;

- l'ordinateur de l'utilisateur lit le contenu Adobe Flash et, dans le même temps, exécute l'exploit, sans aucun signe visible pour l'utilisateur;

- l'auteur de l'attaque (la personne qui a conçu le contenu Adobe Flash contenant l'exploit) a désormais accès à l'ordinateur de l'utilisateur, avec les mêmes droits que l'utilisateur;

- l'auteur de l'attaque peut désormais exécuter d'autres exploits, pour obtenir un accès plus large à l'ordinateur de l'utilisateur, et/ou installer un logiciel qui lui renverra des données.

Il existe un vaste marché[13] pour les exploits du type de celui susvisé, car ces exploits sont extrêmement utiles dans le cadre d'outils de surveillance. En outre, sans ces exploits, l'infiltration d'un système informatique serait beaucoup plus difficile à mettre en œuvre et nécessiterait une participation plus active d'un utilisateur disposant déjà d'un accès à la cible. Les sociétés concernées ont grand intérêt à veiller à limiter étroitement les cercles ayant connaissance des informations concernant ces failles/vulnérabilités.

2.3 Implications techniques

En conséquence des violations de données qui ont fait l'objet d'une large médiatisation sur l'internet[14], des logiciels de surveillance intrusive sont désormais mis à la disposition du grand public. Selon des indications publiées dans la presse, «le volume de code publié est suffisant pour permettre à quiconque d'utiliser le logiciel pour attaquer la cible de son choix», «il n'est plus possible de contrôler l'identité des utilisateurs de la technologie», «la situation nous semble extrêmement dangereuse»[15].

Il convient de relever qu'une fois que l'existence d'un exploit (et des failles/vulnérabilités correspondantes) a été divulguée, les fournisseurs de logiciels publient des logiciels correctifs ou de nouvelles versions de leurs logiciels qui ne sont pas vulnérables aux mêmes attaques. Pour autant qu'il ait installé ces nouvelles versions ou ces logiciels correctifs, l'utilisateur sera protégé contre ces problèmes spécifiques. Ce qui précède démontre l'importance, pour toute entité (entreprise privée, organisme public ou personne physique), de veiller au suivi des logiciels qu'elle utilise et de mettre à jour rapidement ses systèmes informatiques.

Néanmoins, généralement, dans leur propre intérêt, les fournisseurs et les utilisateurs de ces outils de surveillance ne divulguent pas d'informations concernant des failles/vulnérabilités existantes: les fournisseurs s'en abstiennent pour que leur logiciel d'intrusion reste efficace le plus longtemps possible (et, par extension, pour assurer leur succès commercial) et les utilisateurs de ces outils de surveillance veulent conserver toutes les capacités informatiques dont ils disposent, au détriment de la sécurité et du respect de la vie privée de centaines de milliers, voire de millions, d'utilisateurs. Des groupes moins recommandables (groupes criminels organisés, pirates informatiques, etc.) peuvent parfaitement connaître et exploiter ces mêmes failles/vulnérabilités pour leur propre bénéfice.

En outre, les outils de surveillance intrusive ne permettent pas d'opérer une distinction entre les divers utilisateurs d'une cible spécifique donnée: une fois que la cible est compromise, toutes les données demandées par les outils de surveillance seront recueillies, quelle que soit la personne physique qui utilise la cible.

En outre, en fonction des modalités selon lesquelles elles sont réalisées, les attaques des cibles peuvent nuire, au cours de leur exécution, à des personnes qui n'étaient pas visées et qui utilisent des systèmes informatiques complètement différents:

- si l'on reprend l'exemple présenté dans la partie 2.2, un utilisateur peut naviguer sur l'internet, tomber sans le savoir sur le contenu Adobe Flash intégrant les exploits et faire l'objet d'une attaque injustifiée qui compromet sa sécurité et le respect de sa vie privée;

- pour compromettre avec succès une cible spécifique, l'utilisateur des outils de surveillance intrusive peut devoir compromettre un autre système informatique auquel il sait que la cible a accès (à titre d'exemple, pour obtenir l'accès au compte bancaire en ligne d'un utilisateur, il est possible que l'auteur de l'attaque commence par cibler le site de vidéo à la demande que cet utilisateur consulte ou le compte Facebook de l'un de ses amis). Ceci supposerait, une fois encore, de compromettre la sécurité et le respect de la vie privée de personnes physiques qui n'ont aucun lien avec la recherche, hormis leur qualité d'utilisateurs malheureux d'un système informatique connecté à la cible.

En fonction des spécifications techniques et du contexte spécifique, les outils de surveillance intrusive peuvent, dans certaines circonstances, être utiles dans le cadre d'un usage légitime (et réglementé) par les organes chargés de l'application de la loi ou les services de renseignement. Ils peuvent également être utilisés comme des «chevaux de Troie» à des fins de contournement des mesures de sécurité entourant les communications électroniques (à titre d'exemple, le cryptage du réseau): une fois l'attaque de la cible réalisée avec succès, les outils de surveillance accéderont aux données de la cible avant même que ces données ne soient transmises sur l'internet, et donc avant qu'elles aient fait l'objet des mesures de cryptage du réseau. Dans ces circonstances, l'éventuel cryptage mis en œuvre par la cible perdrait naturellement toute utilité.

3 Le rôle du CEPD et des autres autorités chargées de la protection des données

Conformément au règlement nº 45/2001, le CEPD, dans le cadre de ses fonctions, conseille l'ensemble des institutions et organes de l'UE pour toutes les questions concernant le traitement de données à caractère personnel[16]. En application du même règlement, le CEPD peut également adopter des avis, de sa propre initiative, en vue de signaler l'existence de risques d'atteinte aux droits au respect de la vie privée et à la protection des données des citoyens. Dans le présent avis, le CEPD aborde les questions que soulève la diffusion de dispositifs et de logiciels de surveillance en matière de protection des données et de respect de la vie privée. En effet, l'utilisation de ces outils suppose, par défaut, le traitement de données à caractère personnel et une possible interférence avec le droit au respect de la vie privée.

En parallèle, la directive 95/46 s'applique également «*au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier*»[17].

Il ne fait aucun doute que l'utilisation d'outils de surveillance intrusive suppose le traitement de données à caractère personnel. En effet, la notion de données à caractère personnel recouvre, notamment, l'ensemble des informations, communications, métadonnées, activités et mouvements concernant une personne physique identifiée ou identifiable. Il s'agit là à l'évidence du type d'informations traitées par les systèmes de surveillance. En outre, la collecte, la conservation ou l'interception de ces données est considéré comme un traitement de ces données. En conséquence, dès lors que le traitement de ces données est effectué de manière automatisée par des outils de surveillance et qu'il demeure dans le champ d'application de la directive 95/46/CE, les règles et les principes posés par cette dernière (tels que transposés dans les droits nationaux et mis en œuvre par le règlement nº 45/2001) sont applicables.

Ce qui précède signifie, en particulier, que quand bien même il serait satisfait à d'autres dispositions de nature réglementaire ou administrative (portant, à titre d'exemple, sur la diffusion, l'exportation et l'utilisation de la technologie), il demeure nécessaire de respecter les principes du régime de la protection des données. En d'autres termes, si la vente au public et l'utilisation par le public d'une technologie ou d'un dispositif sont autorisés, cette autorisation ne saurait en aucun cas avoir d'effet sur l'incidence que cette technologie

pourrait avoir sur la sphère privée des personnes physiques et sur le fait que toute utilisation doit être conforme aux règles du respect de la vie privée et de la protection des données.

En conséquence, le CEPD et les autres autorités chargées de la protection des données à l'échelle de l'UE, outre leur rôle consultatif concernant toutes les mesures administratives ou réglementaires relatives à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel, peuvent intervenir pour signaler des risques spécifiques d'atteinte au droit des citoyens qui pourraient survenir en lien avec l'utilisation de la technologie de surveillance intrusive.

À cet égard, il convient de souligner que l'interception de communications, le stockage de données à caractère personnel et l'analyse d'ensembles de données ont, à l'évidence, une incidence sérieuse sur le respect de la vie privée et la protection des données à caractère personnel de chacun.

4 Évaluation des politiques concernées

Dans le présent chapitre, le CEPD présentera brièvement:

1. *les défis découlant de l'utilisation de technologies de surveillance et d'interception qui devront être relevés;*
2. *les politiques existantes concernant les technologies de surveillance intrusive;*
3. *les résultats possibles et une approche prospective de nouvelle réglementation.*

4.1 Les défis

Certains systèmes technologiques peuvent être utilisés pour commettre des actes de violation des droits de l'homme, comme la censure, la surveillance, l'accès non autorisé à des dispositifs, le brouillage, l'interception ou le contrôle de personnes physiques. Ces violations peuvent être le fait d'organisations privées ou d'organes publics (y compris d'entités chargées de l'application de la loi et de gouvernements). Les cyberattaques, l'interception illégale, la surveillance de masse par des organes gouvernementaux et les attaques de systèmes informatiques sont autant d'exemples d'activités qui peuvent être perpétrées en utilisant des dispositifs ou des outils informatiques spécifiques, voire des informations spécifiques se rapportant aux TIC (à titre d'exemple, la connaissance des points de vulnérabilité d'un logiciel).

Par ailleurs, les instruments informatiques peuvent également faciliter la diffusion d'idées et d'informations et l'organisation de mouvements sociaux, en particulier dans les régions contrôlées par des régimes autoritaires. L'internet est également un lieu qui offre aux personnes physiques une multitude de possibilités pour échanger des données, des informations et des connaissances. En conséquence, les TIC peuvent avoir une incidence extrêmement positive sur le renforcement des droits de l'homme. À titre d'exemple, le cryptage peut être utilisé par les défenseurs des droits de l'homme pour éviter toute intrusion, interception ou surveillance de la part de leurs organes gouvernementaux. En outre, certaines technologies peuvent être utilisées par les journalistes pour contourner la censure dans les régimes dictatoriaux. En conséquence, il convient de reconnaître que l'utilisation des TIC peut contribuer à la protection des droits de l'homme et faciliter la mise en œuvre des droits

et libertés numériques, y compris des droits à la protection de la confidentialité, au respect de la vie privée et à la protection des données à caractère personnel.

Il est nécessaire que les politiques nationales et de l'UE et tous les acteurs intervenant dans le secteur des technologies de l'information et des communications («TIC») (développeurs, prestataires de services, vendeurs, intermédiaires, distributeurs et utilisateurs) abordent la question de la tension existant entre, d'une part, l'utilisation positive d'outils informatiques, et d'autre part, l'incidence négative que l'utilisation abusive de la technologie peut avoir sur les droits fondamentaux, et en particulier sur la protection des données à caractère personnel et le respect de la vie privée.

Dans une situation d'aggravation des préoccupations en matière de sécurité, les services de renseignement et la police peuvent choisir d'utiliser des moyens technologiques (y compris la technologie de surveillance intrusive) pour mieux cibler leurs enquêtes et renforcer leur efficacité. Dans ce contexte, on ne saurait exclure l'utilisation des données massives en tant qu'outil d'enquête, compte tenu de son efficacité pour relier des informations et des preuves provenant de sources différentes. À cet égard, nous relevons que la législation sur la protection des données en vigueur, même dans une nouvelle version modifiée, pourrait ne pas être suffisamment précise pour couvrir toutes les questions que soulève l'utilisation de technologies attentatoires à la vie privée dans le cadre d'enquêtes et de mesures d'application de la loi.

Compte tenu de l'interconnexion mondiale que nous connaissons aujourd'hui, la cybersécurité revêt une dimension internationale qui va au-delà des frontières de l'UE. En raison de cette dimension internationale, l'atteinte d'une cybersécurité effective constitue un défi de taille, mais que nous nous devons de relever car la cybersécurité est un élément fondamental de la protection des données. Les droits au respect de la vie privée et à la protection des données et la cybersécurité poursuivent le même objectif: en effet, l'assurance d'un niveau élevé de cybersécurité contribuera à renforcer la sécurité de tous les informations traitées, y compris des données à caractère personnel.

Cependant, la cybersécurité ne doit pas devenir un prétexte pour procéder à des traitements de données à caractère personnel disproportionnés, comme dans le cas des outils de surveillance intrusive. Les principes de protection des données tels que les principes de nécessité et de proportionnalité aident à donner des orientations concernant l'utilisation licite des technologies d'intrusion et de surveillance. En outre, le principe de respect de la vie privée dès la conception encourage l'intégration dans la technologie, au cours de la phase de conception, d'éléments permettant de garantir la protection des données. De manière similaire, le principe de respect de la vie privée par défaut permet de s'assurer que les paramètres par défaut de la technologie sont conformes aux principes de protection des données, en l'absence de choix spécifiques des utilisateurs.

La sécurité des données, des systèmes et des réseaux est également fondamentale pour la confiance, l'intégrité des transactions et le développement du marché unique numérique, des réseaux intelligents et de l'internet des objets. L'affaiblissement du niveau de sécurité des données en vue de permettre la mise en place d'une surveillance plus généralisée aboutirait à une perte de confiance et viendrait saper le marché unique de l'UE et la stratégie numérique de l'UE. On peut comprendre que les organes chargés de la surveillance et de l'application de la loi aient besoin de moyens adaptés pour lutter contre la criminalité, y compris sur l'internet. Cependant, pour toute mesure nouvelle, il est nécessaire de procéder à

l'appréciation préalable de la nécessité et de la proportionnalité de la mesure envisagée et de fournir à l'avance des preuves étayées de la nécessité de ces mesures.

Le respect de la vie privée et la protection des données ne constituent pas l'antithèse de la croissance économique et du commerce international, ni de la cybersécurité ou de l'amélioration des services et des produits. Au contraire, ils comptent parmi les éléments constitutifs d'une solution de haute qualité.

4.2 L'appréciation des politiques concernées par les technologies de surveillance et d'interception

Les traitements de données à caractère personnel relevant du champ d'application du droit de l'UE qui sont mis en œuvre par les autorités compétentes à des fins d'application de la loi devraient également respecter les normes et les garanties prévues par la Charte des droits fondamentaux de l'UE. L'article 7 de la Charte consacre le **droit au respect de la vie privée**, aux fins duquel la protection des données à caractère personnel peut présenter une importance fondamentale. Ainsi, l'intrusion dans le domicile virtuel au moyen de logiciels espions, d'exploits ou de dispositifs similaires, devrait être considérée comme une violation de la vie privée d'une personne. Dans ce contexte, le «domicile virtuel» devrait bénéficier du même niveau de protection et de respect que le domicile physique[18]. Le **droit à la protection des données à caractère personnel** est consacré par l'article 8 de la Charte, en application duquel les personnes ont droit à la protection de certaines garanties dans tous les cas où leurs données à caractère personnel font l'objet d'un traitement. Partant, l'utilisation d'outils de surveillance devrait être couverte par une législation spécifique qui encadrerait les limites acceptables en matière de diffusion et d'utilisation de ces technologies et qui prévoirait les garanties nécessaires concernant cette utilisation.

En conséquence, les outils et les logiciels de surveillance utilisés au sein de l'UE auront une incidence sur ces deux droits fondamentaux des personnes. Par ailleurs, l'UE devrait mesurer l'incidence de ses politiques sur les droits fondamentaux des personnes dans les pays tiers. Il y aurait lieu d'encourager clairement une approche cohérente, en vue d'éviter l'existence de normes différentes pour apprécier les conséquences des politiques de l'UE au sein et à l'extérieur de l'UE.

La législation des États membres prévoit l'illicéité de l'utilisation d'outils informatiques dans certaines circonstances. L'article 6 de la **Convention de Budapest sur la cybercriminalité**, à titre d'exemple, couvre déjà la question de la production, de la vente, de l'obtention pour utilisation, de l'importation, de la diffusion ou d'autres formes de mise à disposition d'un dispositif, d'un programme informatique, d'un mot de passe, d'un code d'accès ou de données informatiques similaires dans l'intention, principalement, qu'ils soient utilisés afin de commettre une infraction. Cependant, la portée de cette disposition pourrait ne pas être adaptée pour couvrir l'ensemble des technologies de surveillance et d'interception. En outre, cette disposition ne prohibe pas les actes de surveillance ou d'interception légitimes (par exemple, les actes de ce type accomplis par des organes chargés de l'application de la loi qui y sont autorisés par la loi). Dès lors, des incertitudes subsistent, à certains égards, concernant le point de savoir si l'application effective de cette disposition permet de couvrir de manière exhaustive et appropriée la question des outils de surveillance et d'interception susceptibles d'entraîner la violation de droits de l'homme d'une manière qui pourrait également nuire aux personnes physiques établies dans l'UE.

L'**exportation de technologies de surveillance et d'interception** peut également être soumise au règlement nº 428/2009[19], connu sous le nom de règlement sur le «double usage». Conformément à ce règlement, l'exportation de technologies préjudiciables vers des pays tiers peut faire l'objet d'un contrôle. Le CEPD se félicite du fait qu'en décembre 2013, les États parties à l'Arrangement de Wassenaar sont convenus de mettre en œuvre des contrôles des exportations concernant les «logiciels d'intrusion» et les «systèmes de surveillance sur réseau IP».

Cependant, le régime du double usage de l'UE ne couvre pas de manière exhaustive la question de l'exportation de toutes les TIC[20] vers un pays qui n'offre pas toutes les garanties appropriées concernant l'utilisation de ces technologies. En conséquence, la révision en cours du règlement sur le «double usage» devrait être considérée comme une occasion de limiter l'exportation de dispositifs, de services et d'informations potentiellement préjudiciables vers des pays tiers présentant un risque pour les droits de l'homme.

Dans le cadre du double usage, il conviendrait d'établir des normes permettant d'apprécier l'utilisation qui pourrait être faite des TIC ou des informations en cause et l'incidence que cette utilisation pourrait avoir sur les droits fondamentaux au sein de l'UE[21]. Il conviendrait de réaliser une analyse de la situation dans le pays tiers en matière de protection effective des droits de l'homme ou de respect des libertés individuelles, afin d'évaluer l'opportunité d'accorder une autorisation d'exportation et les conditions de cet octroi. En outre, il est fondamental d'apprécier le cadre dans lequel les technologies sont utilisées, en vue d'évaluer leur incidence sur les droits de l'homme.

Cependant, le règlement sur le double usage de l'UE ne peut pas couvrir toutes les questions relatives à la diffusion et à l'utilisation des technologies de surveillance. Un autre instrument devrait établir un cadre pour les actions des intervenants du secteur de l'application de la loi, à savoir la **future directive sur la protection des données**, qui s'appliquera au secteur de l'application de la loi[22]. L'utilisation de TIC par les organes chargés de l'application de la loi devra intervenir dans le respect des limites posées par les dispositions de cette directive et des législations nationales de transposition correspondantes.

En conséquence, la protection efficace des systèmes informatiques contre toute attaque ou toute interception illicite est essentielle pour protéger les droits fondamentaux au respect de la vie privée et à la protection des données des personnes physiques au sein de l'UE. La **stratégie numérique de l'UE** comprend déjà un ensemble de mesures destinées à renforcer la cybersécurité et elle devrait permettre une meilleure résilience des systèmes informatiques en cas de survenance d'incidents susceptibles de porter atteinte à leur sécurité.

Dans ce contexte, l'UE a proposé une **stratégie de cybersécurité**[23], qui devrait renforcer la participation de l'ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information), mis en place des équipes d'intervention en cas d'urgence informatique (CERT) et proposé une nouvelle législation[24] et des actions[25] visant à contrer les menaces pour la sécurité et les incidents dans ce domaine. La stratégie de cybersécurité de l'EU devrait tenir compte de la possibilité que des TIC soient utilisées pour porter atteinte à des droits fondamentaux, tant au sein de l'UE que dans des pays tiers. Dès lors, il conviendrait d'adopter une approche cohérente de la diffusion des technologies informatiques de surveillance et d'interception dans le cadre de la stratégie de cybersécurité.

Enfin, le **cadre de la protection des données** est également un instrument utile dont il pourrait être fait usage pour aborder les questions de la sécurité et de la violation des droits fondamentaux. Étant donné que l'interception et la surveillance des données à caractère personnel déclencheront, en retour, l'application du cadre juridique de la protection des données, la simple conformité d'une TIC à la législation en matière commerciale, d'exportation, de sûreté ou de sécurité n'exonérera pas l'utilisateur de l'obligation de se conformer aux principes de protection des données énoncés dans la législation nationale sur la protection des données ou dans le règlement nº 45/2001.

L'**obligation d'assurer la sécurité du traitement des données à caractère personnel** est déjà inscrite dans la directive 95/46/CE[26]. Le futur cadre juridique établi par le règlement général sur la protection des données prévoit également de nouveaux principes qui pourront être utiles pour aborder les questions de la sécurité et de la protection des données à caractère personnel. À titre d'exemple, les principes de *respect de la vie privée dès la conception* et de *respect de la vie privée par défaut* devraient encourager les entreprises à concevoir l'utilisation de leurs TIC selon des modalités permettant à ces technologies de mieux servir les finalités légitimes d'une organisation, en limitant la collecte de données à ce qui est nécessaire, ou en ciblant de manière adaptée les personnes et les communications devant faire l'objet d'interceptions. L'obligation de signalement des violations de données est un autre outil qui pourrait aider à identifier les faiblesses d'un système informatique ou le niveau de sécurité insuffisant d'un traitement de données à caractère personnel déterminé.

4.3 La voie à suivre

En ce qui concerne les objectifs énoncés ci-dessus, une législation spécifique devrait réglementer, le cas échéant, l'application des garanties appropriées en matière de protection des données aux activités d'enquête et d'application de la loi qui reposent sur la technologie. Bien que l'élaboration des lois et le développement de la technologie suivent des rythmes différents, cette législation devrait avoir un caractère aussi prospectif que possible. En particulier, elle devrait être fondée sur une appréciation, et sur la prise en compte, des technologies qui, même si elles ne sont pas encore utilisées par les autorités de police et de renseignement dans le cadre de leurs enquêtes, ont déjà été testées et mises à disposition sur le marché. Dans le même temps, la législation devrait rester neutre en ce qui concerne la technologie et se concentrer sur l'effet que celle-ci peut avoir en matière de protection des données, afin d'imposer l'application de certaines garanties. Ces politiques ne devraient ni entraver la recherche légitime[27], ni limiter indûment l'accès aux informations et la communication des informations.

Le recours à des outils de surveillance aura une incidence sur les intérêts de multiples parties prenantes: les concepteurs et les éditeurs de logiciels, les organes chargés de l'application de la loi et la communauté de l'internet dans son ensemble. En conséquence, il est crucial que le débat sur les mesures législatives à adopter prévoit une large consultation de ces parties prenantes. La discussion devrait notamment porter sur les principes comme le *respect de la vie privée dès la conception* et le *respect de la vie privée par défaut*. En effet, le premier permet d'incorporer à la technologie des éléments garantissant la protection des données (et donc d'atténuer l'incidence de la technologie sur la vie des citoyens) et le second permet de veiller à ce que même les personnes physiques qui sont moins préoccupées par le respect de leur vie privée bénéficient d'un niveau de protection adéquat. Si nous comprenons que les entreprises aient besoin d'une plus grande sécurité juridique, celles-ci assument également une responsabilité morale lorsqu'elles exercent ce type d'activités.

Eu égard à ce qui précède, la nécessité d'assurer l'efficacité des outils d'enquête fondés sur la technologie tout en préservant, dans le même temps, le rôle de l'internet en tant que lieu de libre expression et d'interaction démocratique entre les citoyens constitue un défi crucial. Les citoyens exigeront de manière croissante d'être protégés contre des menaces extérieures (à titre d'exemple, les activités criminelles et le terrorisme). Dans le même temps, cependant, ils s'attendront légitimement à ce que le renforcement de la sécurité ne se fasse pas au détriment de leurs libertés fondamentales. L'application des principes comme la nécessité et la proportionnalité devrait garantir que les enquêtes et les activités policières seront ciblées et auront une incidence limitée sur la sphère privée des citoyens.

Il est nécessaire que tous les acteurs du domaine de la cybersécurité [chercheurs, organes chargés de l'application de la loi, CERT (équipes d'intervention en cas d'urgence informatique), organisations privées et publiques, etc.] partagent les informations relatives aux failles/vulnérabilités de logiciels ainsi que les informations concernant les violations de la sécurité et les incidents dans ce domaine, en vue de garantir l'adoption la plus efficace, la plus effective et la plus large des logiciels et des mesures de sécurité appropriés. Dans notre monde interconnecté, la sécurité de chaque entité est dépendante de la sécurité de l'ensemble. C'est en agissant ensemble et de manière coordonnée que nous sommes les plus efficaces pour garantir la cybersécurité de toute la population.

En outre, les révélations concernant la surveillance de masse ont fait naître des préoccupations importantes concernant le respect de la protection des personnes concernées de l'UE. La sécurité nationale ne saurait justifier une surveillance secrète, non ciblée et exercée sans discernement. En conséquence, l'UE devrait adopter une approche cohérente à l'échelle mondiale: les pratiques de surveillance révélées par Edward Snowden aux États-Unis soulèvent des préoccupations quant à la compatibilité de ces pratiques avec les droits fondamentaux des personnes concernées en Europe et dès lors, les États membres devraient prévoir la possibilité d'accorder aux dénonciateurs une protection internationale, y compris le droit de demander l'asile.

5 Conclusions

Compte tenu de ce qui précède, le CEPD considère qu'il serait possible d'aborder la menace que fait naître l'utilisation de technologies de surveillance intrusive par la voie des actions suivantes:

- il conviendrait d'examiner les normes européennes existantes en matière de TIC, en vue de renforcer la protection des droits de l'homme, particulièrement dans le cas de l'exportation de technologies d'interception ou de surveillance et de services dans ce domaine;
- l'utilisation et la diffusion (y compris au sein de l'UE) d'outils de surveillance et d'interception, et de services dans ces domaines, devraient faire l'objet d'une réglementation adaptée tenant compte du risque de violation de droits fondamentaux, et en particulier des droits au respect de la vie privée et à la protection des données;
- le Conseil de l'UE, le Parlement européen, la Commission européenne et le Service européen pour l'action extérieure devraient concevoir des politiques cohérentes et plus efficaces concernant l'exportation d'outils de surveillance intrusive dans le cadre des technologies à double usage, à l'échelle de l'UE et à l'échelle internationale;
- les politiques mises à jour devraient réglementer les vulnérabilités et les exploits «jour zéro» afin d'éviter que ceux-ci ne soient utilisés à des fins de violation des droits fondamentaux;
- les politiques sur la cybersécurité de l'UE devraient tenir compte de la diffusion des technologies d'interception et de surveillance et aborder cette question de manière spécifique dans le cadre de la législation adaptée;
- les investissements dans le domaine de la sécurité sur l'internet et les initiatives de prise en compte du respect de la vie privée dès la conception de nouvelles solutions technologiques devraient être encouragés;
- il conviendrait d'établir une approche cohérente pour accorder une protection internationale aux dénonciateurs qui contribuent à révéler l'existence de violations des droits de l'homme commises en utilisant des technologies d'interception et de surveillance.

Fait à Bruxelles, le 15 décembre 2015.

(**signé**)

Giovanni BUTTARELLI

Contrôleur européen de la protection des données

Notes

[1] http://www.engadget.com/2015/07/09/how-spyware-peddler-hacking-team-was-publicly-dismantled/.

[2] http://www.engadget.com/2015/07/09/how-spyware-peddler-hacking-team-was-publicly-dismantled/.

[3] https://www.hackingteam.com/images/stories/galileo.pdf.

[4] https://www.hackingteam.com/index.php/customer-policy.

[5] http://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim.

[6] https://www.finfisher.com/FinFisher/company.html.
https://www.finfisher.com/FinFisher/products_and_services.html.
http://www.zdnet.com/article/top-govt-spyware-company-hacked-gammas-finfisher-leaked.

[7] https://www.zerodium.com/about.html.

[8] http://www.theverge.com/2015/11/10/9703526/tim-cook-encryption-uk-investigatory-powers-bill.

[9] https://fr.wikipedia.org/wiki/Porte_dérobée.

[10] http://malware.wikia.com/wiki/Trojan.

[11] http://www.wired.com/2015/11/heres-a-spy-firms-price-list-for-secret-hacker-techniques/.

[12] http://arstechnica.com/security/2015/07/hacking-team-leak-releases-potent-flash-0day-into-the-wild/.

[13] http://arstechnica.com/security/2015/07/hacking-team-leak-releases-potent-flash-0day-into-the-wild/.

[14] http://www.engadget.com/2015/07/09/how-spyware-peddler-hacking-team-was-publicly-dismantled/,
http://www.zdnet.com/article/top-govt-spyware-company-hacked-gammas-finfisher-leaked

[15] Communiqués de presse de Hacking Team des 8 juin 2015, 14 juin 2015 et 22 juin 2015 (http://www.hackingteam.it/index.php/about-us).

[16] Article 43 du règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

[17] Article 3, paragraphe 1, de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[18] Voir, à titre d'exemple, décision de la Cour constitutionnelle allemande du 27 février 2008, BVerfG, 1 BvR 370/07, Absatz-Nr. (1 - 267), http://www.bverfg.de/e/rs20080227_1bvr037007en.html.

[19] Règlement nº 428/2009 du Conseil du 5 mai 2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage.

[20] Pour que le régime du double usage soit exempt de toute faille ou lacune, il faudrait qu'il s'applique à l'ensemble des technologies, des informations, des exploits, des logiciels et des dispositifs susceptibles d'avoir une incidence sur les droits de l'homme.

[21] À titre d'exemple, voir l'action 6 proposée par M. SCHAAKE, membre du Parlement européen, qui suggère d'appliquer des lignes directrices de l'UE relatives aux exportations prévoyant l'«obligation de connaître son client»: http://www.marietjeschaake.eu/2015/10/marietje-schaake-proposes-12-actions-to-remedy-human-rights-shortcomings-in-the-eus-dual-use-regulation/.

[22] 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.

[23] Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé, http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52013JC0001.

[24] Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union - COM(2013) 48 final - 07.02.2013 - FR. La Commission, le Conseil et le Parlement sont parvenus à un accord sur ce texte le 8 décembre: voir http://europa.eu/rapid/press-release_IP-15-6270_fr.htm.

[25] http://ec.europa.eu/digital-agenda/en/our-goals/pillar-iii-trust-security%23Our%20Actions.

[26] Article 17.

[27] Y compris les programmes de versement d'une récompense aux personnes physiques découvrant un bogue, destinés à inciter ces personnes à fournir des informations concernant des vulnérabilités aux entreprises de logiciels.