Etat du droit concernant les mesures de sécurité au regard de la loi vie privée et du projet de règlement européen de protection des données à caractère personnel dans le contexte Post-Snowden

Par : Liu Po-Yung Qi Hao

Professeur : Mme Cécile DE TERWANGNE

I. Introduction

Ce travail se donne pour but d'exposer dans un premier temps l'état du droit actuel concernant l'obligation de sécurité prévue par la loi vie privée belge. Ainsi, nous tenterons de mesurer la portée de cette obligation qui repose sur le responsable de traitement. Dans un second temps, nous contextualiserons aussi la question face aux défis contemporains permis par l'informatisation croissante de la société. Ainsi dans une perspective chronologique, nous examinerons la situation actuelle concernant cette obligation à la lumière notamment de la résolution du Parlement européen du 12 mars 2014 sur le programme de surveillance de la NSA et ses incidences sur les droits fondamentaux des citoyens européens. Cela nous permettra de saisir notamment les défis inédits auxquels tente de répondre le projet de règlement général européen sur la protection des données[1] qui a été adopté le même jour. À cet égard nous examinerons les recommandations de la résolution du Parlement européen aussi à la lumière de la pratique de renforcement des mesures de sécurité mises en place par les acteurs de systèmes ouverts (open source). Ces pratiques seront articulées par rapport notamment à la notion de « Privacy by design » introduite tant par la résolution que par le règlement européen. Finalement nous exposerons les autres mécanismes prévus par ce projet de règlement européen permettant un renforcement des mesures de sécurité en vue d'une protection effective des données à caractère personnel. Nous terminerons par une conclusion résumant le panorama et la tendance dans ce domaine.

II. L'obligation de sécurité dans la loi belge vie privée

En Belgique, l'obligation de sécurité se retrouve à l'article 16 §4 de la loi vie privée[2] qui dispose que « *Afin de garantir la sécurité des données à caractère personnel, le responsable du traitement et, le cas échéant, son représentant en Belgique, ainsi que le sous-traitant doivent prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non*

1 Résolution législative du Parlement européen du 12 mars 2014 sur la 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.

2 8 décembre 1992. Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. M.B.

autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel.

Ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels. »

Cette obligation impose de prendre des mesures techniques et organisationnelles pour protéger les données à caractère personnel contre tout traitement non autorisé. Pour ce faire un niveau adéquat de sécurité est exigé par la loi en fonction des critères suivant : état de la technique, frais entraînés par les mesures, natures des données et risques potentiels.

Une obligation de moyens d'un niveau de protection adéquat

Les travaux préparatoires considèrent que cette obligation est une obligation de moyens à l'égard du responsable de traitement. Il a l'obligation de mettre en œuvre tous les moyens raisonnables pour garantir ce niveau adéquat. Néanmoins la loi ne prévoit pas en tant que telle une hiérarchisation des critères. Dès lors, il n'y a pas à priori de primauté d'un critère sur un autre. Plusieurs situations pourraient se présenter : le responsable de traitement pourrait faire primer un critère sur d'autres ou bien pourrait mettre en balance différents critères. Nous pensons néanmoins qu'un seul critère ne pourrait pas primer sur tous les autres au point de les éclipser totalement, cela viderait la substance de l'obligation de la loi vie privée qui a pour but la protection des données à caractère personnel. Ainsi un responsable de traitement qui ne mettrait pas en place des mesures de sécurité (du fait qu'il justifierait que les frais engendrés seraient trop importants) ou y mettrait un niveau de sécurité trop faible (du fait du faible investissement consenti à cet égard) ne pourrait rencontrer son obligation de sécurité. Cette interprétation est confirmée notamment par la jurisprudence de la Cour européenne des droits de l'homme et par l'affaire SNCB que nous aborderons dans la section ci-dessous.

Dès lors, le niveau de protection à assurer est fonction notamment de la sensibilité des données traitées et des risques liés à l'utilisation de ces données. Ainsi certaines dispositions spécifiques permettent de se rendre compte que des données médicales, par nature plus sensibles, bénéficient d'un régime renforcé de sécurité[3]. Ainsi, une interprétation possible pour le responsable de traitement des critères permet une proportionnalité quand les données en cause sont sensibles et les risques pour les personnes concernées sont élevés. Les mesures d'une plus grande importance devront être

3 Recommandation n° R(97)5 du Comité des ministres du Conseil de l'Europe relative la protection des données médicales, point 9 : « *en matière de données médicales, les mesures techniques et organisationnelles doivent assurer un niveau de sécurité approprié compte tenu dune part de l'état de la technique et d'autre part de la nature sensible des données médicales et de l'évaluation des risques potentiels.* »

prises compte tenu de cette évaluation *in concreto*. De plus, le risque étant fortement lié à l'état de la technique, celui-ci sera un critère permettant d'évaluer si des mesures de sécurité effectives ont été prises. Dans le cas d'une fuite de données (*data breach*), le juge devra prendre en compte les différents critères et se situera au jour de la faille de sécurité afin d'évaluer si les mesures prises étaient d'un niveau adéquat.

En termes de responsabilité la loi dispose que « *le responsable de traitement est responsable du dommage causé par un acte contraire aux dispositions déterminées par ou en vertu de la présente loi. Il est exonéré de cette responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable* »[4].

La loi prévoit ainsi une présomption réfragable de responsabilité pour le responsable de traitement. La charge de la preuve repose ainsi sur les épaules de ce dernier. Afin de dégager sa responsabilité il devra prouver que les faits survenus ne pourraient lui être imputables.

Étant donné que le responsable de traitement est tenu à l'obligation de sécurité, il devra prouver que les mesures prises étaient d'un niveau adéquat compte tenu de l'état de la technique, du risque et de la nature des données. Les frais consentis devrait être proportionnés à ces critères et ne pourraient à eux-seuls justifier un niveau inadéquat de sécurité (niveau faible par rapport aux risques exposés), à défaut il verrait sa responsabilité engagée.

III. Affaires et jurisprudence entourant la question du niveau de sécurité adéquat

3.1. L'affaire MOBIB

L'affaire concernant la carte MOBIB de la STIB, du point de vue de la sécurité, posait la question suivante : l'utilisation de la technique de chiffrement obsolète lors de la conception du système permet-elle de rencontrer un niveau adéquat de sécurité compte tenu de l'état de la technique ? Des chercheurs en sécurité considèrent que cela ne permet pas de répondre de manière adéquate à l'obligation de sécurité de la loi[5]. Ainsi, selon David Morelli, responsable de communication à la Ligue des droits de l'homme[6] : « La carte MoBIB a été présentée comme anonyme et inviolable. Or des chercheurs de l'UCL sont parvenus à la craquer en 14 minutes. Ils ont réussi à décrypter les informations contenues sur celles-ci via un lecteur disponible sur le Web à moins de 100 euros. Pour

4 Article 15 bis, alinéas 2 et 3 la loi vie privée.
5 http://www.ieb.be/Carte-MoBIB-un-bon-exemple-de.
6 http://www.cesep.be/ANALYSES/TECHNOLOGIES/2010/orwel.html

nous, le système mis en place par la STIB révèle de -trop- nombreuses carences. D'une part, les informations ne sont pas protégées : n'importe quel quidam équipé d'un lecteur adéquat peut lire et copier les informations personnelles des voyageurs : nom, code postal, date de naissance et lieu et heures des trois derniers voyages effectués par l'usager. C'est inquiétant et contraire à la loi sur la protection de la vie privée. D'autre part, la quantité et la nature des données récoltées sont excessives au regard des objectifs annoncés par la STIB, à savoir lutter contre la fraude et gérer la clientèle. On ne demande pas le retrait de cette carte : on invite simplement la STIB à respecter toute une série d'éléments légaux qui semblent absents. » En outre, les chercheurs ayant travaillé sur la question notent que « *la protection de la lecture, et donc de l'anonymat des utilisateurs du métro, avec les mêmes techniques que celles choisies pour protéger l'écriture, n'aurait engendré aucun coût supplémentaire pour la STIB. L'absence de ce mécanisme minimum dans la carte MoBIB actuellement déployée relève donc de la négligence gratuite.* »[7]
La STIB a d'ailleurs reçu un prix Big Brother Award pour sa mauvaise gestion des questions en matière de sécurité des données personnelles et d'anonymat via la carte MoBIB[8]

3.2. L'affaire de la SNCB

La question des mesures techniques de sécurité s'est posée de manière encore plus prégnante par rapport à la fuite de données dans le cas de la SNCB. Aucune mesure n'avait été prise pour protéger l'accès aux données personnelles (de plus d'un million d'usagers) que traitait la SNCB. Celles-ci étaient en libre disposition via une simple recherche sur un moteur de recherche standard tel que Google[9]. La Commission vie privée a ainsi décidé de saisir le parquet et a transféré le dossier au procureur[10]. En effet l'article 32 §2 dispose que « § 2. Sauf si la loi en dispose autrement, la Commission dénonce au procureur du Roi les infractions dont elle a connaissance. ». La CPVP n'avait pas encore eu recours à cette disposition par le passé malgré l'utilisation de la voix affirmative par la loi.

3.3. La Cour européenne des droits de l'homme

Finalement nous relevons aussi que la Cour européenne des droits de l'homme s'est prononcée sur le sujet dans une affaire opposant une infirmière à l'administration

7 http://www.ieb.be/Carte-MoBIB-un-bon-exemple-de
8 http://www.liguedh.be/espace-presse/116-communiques-de-presse-2011/1358-big-brother-awards-prix-du-public
9 http://nurpa.be/actualites/2012/12/SNCB-fuite-donnees-personnelles
10 http://datanews.levif.be/ict/actualite/fuite-de-donnees-a-la-sncb-la-commission-de-la-vie-privee-a-transmis-le-dossier-au-parquet-de-bruxelles/article-normal-288907.html

hospitalière où elle était employée[11]. Elle a vu son contrat de travail non renouvelé du fait de divulgation de données à caractère personnel la concernant. Ayant échoué à faire réparer son dommage devant les juridictions finlandaises nationales, l'affaire a été portée devant la CEDH. La haute juridiction a dit pour droit que si l'établissement en question avait mieux protéger l'accès aux dossiers médicaux en restreignant l'accès aux personnes directement impliquées, la requérante aurait été dans une position moins défavorable lors de son recours via la responsabilité aquilienne devant l'ordre judiciaire national. L'indemnisation du fait du dommage subi n'est pas suffisante. « *Ce qui est demandé est une protection réelle et effective excluant toute possibilité d'accès non autorisé* »[12].

La Cour a aussi considéré dans un arrêt du 25 février 1997, que la confidentialité et la sécurité sont des éléments fondamentaux de la protection de la vie privée. Elle a affirmé en substance que « la législation interne doit ménager des garanties appropriées pour empêcher toute communication ou divulgation de données à caractère personnel relatives à la santé qui ne serait pas conforme aux garanties prévues à l'article 8 de la Convention »[13].

3.4. Cour de Justice de l'Union

La Cour de Justice de l'Union européenne a affirmé dans l'arrêt Rijkeboer[14], que la protection des données implique que la personne concernée puisse s'assurer que ses données à caractère personnel sont orientés vers des destinataires autorisés. Afin de pouvoir effectuer les vérifications nécessaires, la personne concernée pouvoir disposer d'un droit d'accès à l'information sur ces catégories de destinataires des données, ainsi qu'au contenu de l'information communiquée non seulement pour le présent, mais aussi pour le passé.

Ces différents exemples illustrent la différence entre la mise en œuvre technique et les exigences de la loi concernant le niveau adéquat de sécurité. En effet, étant donné qu'il est techniquement possible de mettre en place des traitements larges, mais dont on n'assure pas de dispositifs de sécurité d'un niveau adapté, il semble que certains acteurs considèrent que la mise en place d'un niveau de sécurité faible (non proportionné au risque) comme suffisant pour rencontrer l'obligation de sécurité (les différents cas finlandais mentionnés ou l'affaire MOBIB) ou ne prennent pas en compte la sécurité (cas SNCB).

---

11 CEDH, 17 juillet 2008, n° 20511/03.

12 F. Villefagne, C. De Terwangne, J. Herveg, C. Gayrel, *Chronique de jurisprudence*, RDTI. n°35/2009, p. 107.

13 Arrêt Z c. Finlande du 25 févier 1997, Recueil des arrêts et décisions 1997-I, p. 347, § 5.

14 C.J.U.E., 7 mai 2009 (Rijkeboer), aff. C-553/07 ; C. De Terwangne, « *l'étendue dans le temps du droit d'accès aux informations sur les destinatairs de données à caractère personnel* » note sosu CJUE , 7 mai 2009, RDTI, 2011, numéro 43, pp. 65 à 81.

IV. Les recommandations de la Commission vie privée

La Commission de la protection de la vie privée (CPVP) s'est déjà penchée sur la question de ce qui constitue un niveau de sécurité adéquat via des mesures de sécurité. Ainsi, ces mesures rassemblent les mesures techniques et organisationnelles sous la catégorie de « mesures de sécurité ». Elle considère que « *Les mesures de sécurité, appelées aussi "mesures de protection" ou "contrôles de sécurité" sont des procédés ou dispositifs susceptibles de réduire les risques. Les mesures de sécurité peuvent être efficaces de différentes manières : en diminuant les possibilités d'une menace, en corrigeant les vulnérabilités ou encore en limitant les opportunités de conséquences directes ou d'impacts indirects. Il est aussi possible d'agir sur le facteur temps. En effet, en détectant mieux et plus tôt les incidents, il est possible d'agir avant une dégradation significative.* »[15]

Dans cette perspective, la CPVP a émis un certain nombre de recommandations, notamment suite à l'affaire SNCB. Elle considère ainsi que ce sont les « *règles de l'art à respecter par tout responsable du traitement afin d'assurer une sécurité de l'information optimale et partant, de garantir la sécurisation des données à caractère personnel des personnes concernées* »[16]. La recommandation du 21 janvier 2013 relative aux mesures de sécurité à respecter afin de prévenir les fuites de données considère que « les mesures de sécurité publiées par la Commission et la norme ISO/IEC 27002 peuvent offrir à cet égard un cadre de référence général adéquat »[17].
Ce standard fait partie de la norme ISO 27001.

Si ces recommandations basées sur des référentiels pouvaient aider à interpréter ce qui pourrait éventuellement constituer l'état de la technique du point de vue de la CPVP, il semblerait que certains acteurs de terrains doutent de l'efficacité de ces référentiels.

Nous relevons ainsi que Selon Laurent Bloch, certifié Lead Auditor ISO 27001, directeur du Système d'information de l'Université Paris-Dauphine et chercheur associé à la chaire Castex de Cyberstratégie de l'Institut des Hautes Études de Défense nationale (IHEDN), il existe plusieurs problèmes quant à la place de l'ISO dans la sécurité informatique et

15 CPVP, *Note sur la sécurité des données à caractère personnel*, 26 septembre 2012, p. 7, consultable à l'adresse suivante : http://www.privacycommission.be/sites/privacycommission/files/documents/note_securite_des_donnees_a_caractere_personnel.pdf.

16 CPVP, recommandation n° 01/2013 du 21 janvier 2013 relative aux mesures de sécurité à respecter afin de prévenir les fuites de données.

17 CPVP, recommandation n° 01/2013 du 21 janvier 2013 relative aux mesures de sécurité à respecter afin de prévenir les fuites de données. p.3.

l'organisation de celle-ci.
Cet auteur n'est « *pas convaincu que les normes évoquées à la section précédente (ISO 27001) soient un remède à l'insécurité ; ces méthodes sont d'une grande lourdeur, leur seul apprentissage est d'une ampleur propre à absorber une énergie considérable, or une fois que l'on connaît par cœur les critères communs et que l'on sait appliquer EBIOS les pieds au mur, on n'a pas mis en place une seule mesure concrète de SSI, on est seulement capable, en principe, d'évaluer les mesures que d'autres auront éventuellement mises en place.* (...) *Ce qui frappe le lecteur de ces normes, c'est que la vérification formelle de conformité à leur texte peut presque être effectuée par un auditeur dépourvu de compétence technique : il suffit de lire les documents obligatoires et de vérifier que les mesures mentionnées ont bien été appliquées, ce qui doit être écrit dans un autre document. On pourrait presque imaginer un audit par ordinateur : il serait sans doute mauvais, mais formellement conforme*[18]. (...) *Une autre faiblesse de ces démarches, c'est leur déterminisme : la lecture de leurs documentations suggère que l'univers des risques et des menaces qu'elles sont censées conjurer est parfaitement ordonné et prévisible, alors que justement ses caractéristiques premières sont le chaos et la surprise.* (…) *Les procédures destinées à évaluer des travaux techniques deviennent une charge de travail plus lourde que l'objet de l'évaluation, les procédures de gestion demandent plus de travail que les activités qu'elles servent à gérer, bref ce qui devrait être une aide pour l'action devient un fardeau, de surcroît ennuyeux.* (...) *Les règles de sécurité complexes ou trop contraignantes seront simplement inappliquées, parce que trop difficiles à comprendre. La simple lecture des critères communs (ISO 15408) et des manuels EBIOS représente des milliers de pages : autant dire que leur étude détaillée est antinomique de toute politique réelle de sécurité*.»

Selon George Quigley, sénior chez KPMG pour les pratiques de cybersécurité et ISO[19], la question que les acteurs se posent est la suivante :

« *That begs the question, if ISO27001 is so good, why are we still seeing security breaches? The answer as with all of these issues is complex. Firstly the standard is a management standard, not necessarily a security standard. To take an extreme example, an organisation might decide that its risk appetite is high risk. It, therefore, takes a cavalier approach to security, leaving itself open to a high risk of a breach occurring, but still complying with the standard.* (...) *When compared with financial based assurance reports such as AAF/0106, SAS70 (now SSAE16), etc, it is apparent that the 27001 certification process does not include detailed testing nor a disclosure of the results of that testing.*[20]»

Dans le cas où les critiques des acteurs de terrain étaient avérées, il serait nécessaire de

18 L. Bloch, *Sécurité informatique, Principes et méthodes à l'usage des DSI, RSSI et administrateurs*, Eyrolles, 2011, p. 22.
19 http://www.kpmg.com/uk/en/issuesandinsights/articlespublications/newsreleases/pages/senior-appointment-for-kpmg-s-cyber-security-practice.aspx.
20 http://www.ion.icaew.com/itcounts/post/ISO27001-Certifications-Worth-the-paper-they-are-written-on-.

réévaluer la place de ce référentiel en particulier concernant sa capacité à pouvoir refléter le niveau réel de l'état de la technique en tant que critère d'évaluation d'un niveau de sécurité adéquat.

V. Résolution du Parlement européen concernant le programme de surveillance de la NSA et les incidences sur les droits fondamentaux des citoyens européens

Le Parlement européen a adopté le même jour (12 mars 2014) la Résolution concernant le programme de surveillance de la NSA[21], (...) et les incidences sur les droits fondamentaux des citoyens européens et le Projet de règlement européen concernant la protection des données à caractère personnel.

La résolution concernant la surveillance de masse de la NSA (ci-nommée résolution NSA/vie privée) fait suite aux différentes révélations portées à la presse par Edward Snowden, l'ex-contractant de l'Agence gouvernementale de renseignements américaine.

Bien que les résolutions du Parlement européen soient des actes non contraignants, elles expriment la position de l'institution sur un problème donné. Elles peuvent éclairer la Cour de justice en lui permettant d'apprécier la portée d'un acte communautaire contraignant (via l'interprétation téléologique).

Cette résolution permet de remettre en contexte la question des mesures de sécurité d'une part, et d'autre part, d'éclairer certains points quant au projet de règlement européen concernant la protection des données à caractère personnel. Nous allons parcourir certains points intéressant les questions de mesures de sécurité pour la protection des données à caractère personnel.

En premier lieu rappelons ce qu'est la NSA. NSA est l'acronyme de National Security Agency (Agence nationale de la sécurité) c'est un organisme gouvernemental du département de la Défense des États-Unis, responsable du renseignement d'origine électromagnétique et de la sécurité des systèmes d'information et de traitement des données du gouvernement américain[22].

Dans le contexte des différentes missions qu'elle se donne pour but de remplir, un ancien contractuel de l'agence (Edward Snowden) a décidé de révéler à partir du 6 juin 2013 les différentes opérations (nommés « programmes ») qui sont mis en œuvre par cette agence. Ces programmes sont massivement tournés vers la surveillance de tout un chacun

21 Résolution du Parlement européen du 12 mars 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 (2013/2188(INI)).

22 http://fr.wikipedia.org/wiki/National_Security_Agency.

utilisant un dispositif électronique (ordinateur portable, GSM, tablette, réseaux sociaux, email…). Ce faisant, cette surveillance de masse viole les différentes législations, conventions et constitutions (y compris américaine) concernant la protection de la vie privée dont notamment le Pacte international relatif aux droits civils et politiques, les différentes Constitutions des différents États surveillés, la Convention européenne des droits de l'homme et bien entendu la loi « vie privée » belge de 1992. Dans ce contexte, le Parlement européen a diligenté une enquête et pris une résolution quant à ces révélations. La résolution « NSA / vie privée » emporte notamment la position du Parlement européen sur la question de la protection des données à caractère personnel. Le même jour était aussi voté par le Parlement européen le projet de règlement européen concernant la protection des personnes physiques à l'égard du traitement des données à caractère personnel[23]. Nous parcourrons les points concernant la position de l'institution concernant les mesures de sécurité permettant de renforcer la protection des données.

En premier lieu, nous remarquons que la résolution « *appelle plus particulièrement l'attention sur les programmes de renseignement de la NSA permettant la surveillance de masse des citoyens de l'Union européenne grâce à l'accès direct aux serveurs centraux des grandes entreprises américaines du secteur de l'internet (programme PRISM), à l'analyse de contenus et de métadonnées (programme Xkeyscore), au contournement du cryptage en ligne (BULLRUN), et à l'accès aux réseaux informatiques et téléphoniques et aux données de localisation, mais aussi sur les systèmes de l'agence de renseignement britannique GCHQ, notamment son activité de surveillance en amont (programme Tempora) et son programme de décryptage (Edgehill), les attaques ciblées de l'homme du milieu" sur des systèmes informatiques (programmes Quantum et Foxacid) et la collecte et la conservation de quelque 200 millions de SMS par jour (programme Dishfire)* ».

Sans rentrer dans les détails, le programme BULLRUN pose particulièrement question pour les responsables de traitement souhaitant mettre en place un niveau de sécurité adéquat. En effet, la cryptographie est l'une des méthodes mathématiques permettant d'assurer la sécurité et la confidentialité de données électroniques. Le programme BULLRUN est conçu pour déchiffrer les transmissions électroniques. La NSA travaille sur ces questions en collaboration avec la GCHQ britannique. D'après les propres documents de la NSA, celle-ci serait capable de déchiffrer les transits internet en temps réel. L'une des approches utilisées a été l'introduction de logiciels espions (appelés *backdoors* ou portes dérobées) dans les protocoles de cryptographie standardisés, ainsi que l'affaiblissement du niveau de sécurité assuré par ces protocoles. Après les révélations du 5 septembre 2013 par les articles du *Guardian*[24], du *New York Times* et de *ProPublica*, l'organisme de normalisation technique américain NIST qui avait accepté le

23 Résolution législative du Parlement européen du 12 mars 2014 sur la 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)0011 – C7-0025/2012 – 2012/0011(COD)).

24 James BALL, Julian BORGER et Glenn GREENWALD, "Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security", *The Guardian*, 6 septembre 2013: http://www.thegardian.com/wolrd/2013/sep/05/nsa-GCHQ-encryption-codes-security.

standard « Dual Elliptic Curve Deterministic Random Bit Generator » (Dual_E_DRBG), a recommandé de ne plus l'utiliser le 8 septembre 2013. De son côté la société RSA Security (leader mondial en cryptographie) recommandait officiellement de ne plus utiliser ses produits B-Safe à la suite d'installation de « porte dérobée » implémentée dans la conception du standard par l'agence américaine.

En second lieu, tirant les conclusions de l'enquête qu'il a diligentée après les révélations, le Parlement européen « *observe qu'il n'existe aucune garantie, que ce soit pour les institutions publiques européennes ou pour les citoyens, que leur sécurité informatique ou leur vie privée puisse être protégée des attaques d'intrus bien équipés* (…) ; *note que pour pouvoir jouir d'une sécurité informatique maximale, les Européens doivent accepter de consacrer suffisamment de moyens, humains et financiers, à la préservation de l'indépendance et de l'autosuffisance de l'Europe dans le domaine des technologies de l'information* ».[25]

Concernant la protection des données à caractère personnel, l'institution propose les réformes suivantes :

- *« invite la présidence du Conseil et les États membres à accélérer leurs travaux sur l'ensemble du paquet relatif à la protection des données en vue de permettre son adoption en 2014, afin que les citoyens de l'Union puissent bénéficier d'un niveau élevé de protection des données dans un avenir très proche ; souligne qu'un engagement réel et un soutien sans faille de la part du Conseil sont une condition nécessaire pour prouver la crédibilité et la fermeté de l'Union à l'égard des pays tiers*[26]
- *souligne que le règlement relatif à la protection des données et la directive relative à la protection des données sont tous deux nécessaires pour protéger les droits fondamentaux des individus et qu'ils doivent dès lors être traités comme un tout à adopter simultanément afin de s'assurer que l'ensemble des activités de traitement de données dans l'Union prévoient un niveau élevé de protection en toutes circonstances ; souligne qu'il n'adoptera des mesures de coopération en matière répressive que lorsque le Conseil aura entamé les négociations avec le Parlement et la Commission au sujet du paquet relatif à la protection des données*[27]
- *rappelle que les notions de "prise en compte du respect de la vie privée dès la conception" et de "respect de la vie privée par défaut" participent au*

25 Résolution du Parlement européen du 12 mars 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 (2013/2188(INI)), conclusion point 2.

26 Résolution du Parlement européen du 12 mars 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 (2013/2188(INI)), p. 33, point 59.

27 *Ibidem,* point 60.

renforcement de la protection des données et devraient avoir le statut de norme pour tous les produits, services et systèmes proposés sur l'internet[28] *;* ».

Concernant la sécurité informatique le Parlement prend les positions suivantes :

- « *condamne vivement le fait que des services de renseignement cherchent à assouplir les normes de sécurité informatique et à installer des "portes dérobées" ("backdoors") dans toute une série de systèmes informatiques ; demande à la Commission de présenter une proposition législative visant à interdire le recours aux portes dérobées par les services répressifs ; recommande en conséquence le recours aux logiciels ouverts à chaque fois que la sécurité informatique est un enjeu important*[29] *;*
- *estime que les révélations en matière de surveillance de masse qui ont provoqué cette crise peuvent être l'occasion pour l'Europe de prendre l'initiative pour mettre en place, en tant que mesure stratégique prioritaire, une capacité autonome de ressources informatiques clés ; souligne que pour regagner la confiance, une telle capacité informatique européenne devrait se fonder autant que possible sur des normes ouvertes, des logiciels et, si possible, du matériel ouverts, rendant toute la chaîne d'approvisionnement transparente et contrôlable, de l'architecture de processeur jusqu'à la couche application*[30] *;*
- *invite la Commission à présenter, avant décembre 2014, des propositions législatives pour encourager les fabricants de logiciels et de matériel à renforcer la sécurité et la vie privée au moyen de fonctions dès la conception et par défaut dans leurs produits, y compris en proposant des mesures pour décourager la collecte excessive et disproportionnée de données à caractère personnel en masse et en introduisant une responsabilité légale pour les fabricants pour les vulnérabilités connues non corrigées, les produits défectueux ou non sûrs, ou l'installation de portes dérobées secrètes permettant d'accéder sans autorisation aux données et de les traiter ; à cet égard, demande à la Commission d'évaluer la possibilité de mettre en place un système de certification ou de validation pour le matériel informatique, y compris des procédures de test au niveau de l'Union européenne pour garantir l'intégrité et la sécurité des produits* ; »[31].

Nous nous apercevons que l'optique prise par le Parlement européen est d'une part d'assurer un haut niveau de sécurité concernant la protection des données à caractère personnel, d'autre part de prendre en compte la notion de vie privée à la conception (*privacy by design*). Le *privacy by design* s'oppose directement au logiciel espion (*backdoor*) qui aurait été implémenté lors de la conception (tel que le programme BULLRUN de la NSA sur la conception de standards cryptographiques). La maîtrise de la chaine d'approvisionnement et l'usage de protocoles, méthodes, logiciels ouverts (*open source*), ainsi que des méthodes de certification permettant de s'assurer de la sécurité, de

28 *Ibidem,* point 61.
29 *Ibidem,* point 92.
30 *Ibidem,* point 91.
31 *Ibidem,* point 94.

la fiabilité du système qui est acquis et mis en œuvre, sont aussi fortement préconisés. Nous examinerons une réponse apportée par ces méthodes ouvertes à la questions des logiciels espions implémentés à la conception.

VI. La réponse des logiciels ouverts (open source) à l'implémentation de « backdoors » lors de la conception de système d'information et son articulation par rapport au concept de « privacy by design »

Après l'onde de choc des révélations de Snowden, la communauté des développeurs des logiciels ouverts (*open source* ou aussi appelés logiciels libres) a commencé à élaborer des réponses pour parer à ces attaques sophistiquées.

Le fait d'implémenter dès la conception des *backdoors* est particulièrement problématique quant à la sécurité des données. En effet, dans ce cas de figure le détournement de finalité est inscrit aux cœur même du dispositif de traitement de données. Cette pratique s'oppose frontalement à la conception de « *privacy by design* » (nous nommerons cette pratique le « *backdoor by design* »).

Une des réponses à l'implémentation de *backdoor*, a été élaborée via la réintroduction de la notion de reproductibilité. Nous allons brièvement explorer l'articulation de cette réponse notamment au concept de « *privacy by design* ».

Afin de faire face au scénario de détournement de finalité par l'implémentation de *backdoor* lors de la phase de conception, la communauté s'est ainsi tournée vers le principe scientifique de la reproductibilité. La reproductibilité est la faculté pour une expérience ou une étude de pouvoir être reproduite soit par le chercheur lui-même (répétabilité)[32] ou par n'importe quelle personne qui travaille dessus de manière indépendante lorsque les mêmes conditions sont réunies. Cela vient du principe *ceteris paribus* (toutes choses égales par ailleurs) les mêmes conditions expérimentales donnent les mêmes résultats scientifiques. Ceux-ci dès lors peuvent être reproduits afin d'en vérifier l'exactitude et la véracité de manière indépendante. La reproductibilité dans le cas de l'informatique consiste à pouvoir arriver à la même empreinte (aussi dénommée sous l'anglicisme « *hash* ») de logiciels à partir d'une compilation des mêmes sources via la même chaine de compilation (outils de développement).

Ainsi, le logiciel libre met à disposition à la fois le code source et les conditions de développement via la chaine de compilation. D'une part, il est ainsi possible d'auditer le code source des logiciels résultant de n'importe quel développement ainsi que la chaine de compilation, de manière indépendante. D'autre part, dès lors que les mêmes conditions sont disponibles, il est possible de reproduire à partir du code source les logiciels en les recompilant de manière indépendante (tout utilisateur final ou tout homme de l'art). Ceci permet de faire la correspondance entre un code source donné et le logiciel spécifique qui en est le résultat.

32 http://fr.wikipedia.org/wiki/Reproductibilit%C3%A9.

Ainsi, la reproductibilité fait référence au fait qu'un même code source compilé avec la même chaine de compilation doit arriver à un résultat en tout point identique. La livraison du code source du logiciel et la reproduction du processus de compilation via le code source par tout tiers indépendant doit permettre d'arriver à la même empreinte[33]. Dans le cas de divergence, cela pourrait être un premier indice sérieux de compromission dans la conception du logiciel[34]. Si cette compromission est avérée, cela irait *ipso facto* à l'encontre du principe « *privacy by design* » et l'on reviendrait au scénario du « *backdoor by design* ».

Il est à noter que le régime juridique même de certaines licences libres permet de favoriser cette reproductibilité. Ainsi, la notion de code source complet et correspondant est inscrite dans certaines licences libres[35] . Ce concept signifie que le code source qui est publié correspond effectivement au logiciel qui a été distribué. Dans le cas d'une absence de *backdoor* dans le code source, et d'une absence de *backdoor* dans la chaine de compilation le code source correspondant au logiciel qui serait complet permettrait d'arriver à un résultat identique au logiciel fournis. De ce fait si ce code source correspond effectivement au logiciel, il sera considéré comme ayant satisfait à la condition de code source complet et correspondant de la licence. Les logiciels *open source* via leurs licences libres donnent des droits[36] à leurs destinataires qui permettent d'exercer les actes de reproductibilité. Cette reproductibilité, outre la vérification indépendante, permet aussi la vérification croisée par tous les acteurs de la chaine de développement et par tout utilisateur final de manière transparente. Cette méthode technologiquement neutre peut s'appliquer à n'importe quel logiciel (du plus anodin jusqu'au système d'exploitation).

Les projets *open source* phares ont déjà mis en place ces méthodes (citons Linux Debian, Fedora, Redhat, Mozilla Firefox, Tor[37]). À ce jour le système d'exploitation Linux Debian[38] a atteint 80 % de reproductibilité sur l'ensemble de ses logiciels[39].

Ces pratiques de vérifications croisées et indépendantes sont à même de donner un début de réponse permettant de fiabiliser la chaine de conception du logiciel[40]. Cela permettra à terme, d'identifier les logiciels et systèmes qui auront été victimes ou auteurs d'une

33 https://blog.torproject.org/blog/deterministic-builds-part-one-cyberwar-and-global-compromise ;
34 https://blog.torproject.org/blog/deterministic-builds-part-two-technical-details
35 Article 2§ 2 de la GPL 2 et GPL 3 – GNU general public licence-
36 traditionnellement dénommés les 4 libertés. Celles-ci sont : la liberté d'exécuter le logiciel, pour n'importe quel usage ; la liberté d'étudier le fonctionnement d'un programme, la liberté de l'adapter à ses besoins, ce qui passe par l'accès aux codes sources ; la liberté de redistribuer des copies : http://www.gnu.org/philosophy/free-sw.fr.html
37 http://media.ccc.de/browse/congress/2014/31c3_-_6240_-_en_-_saal_g_-_201412271400_-_reproducible_builds_-_mike_perry_-_seth_schoen_-_hans_steiner.html#video&t=286
38 https://wiki.debian.org/ReproducibleBuilds/About
39 https://lwn.net/Articles/630074/; https://people.debian.org/~lunar/blog/posts/eighty_percent/
40 https://blog.torproject.org/blog/deterministic-builds-part-one-cyberwar-and-global-compromise ; https://www.schneier.com/blog/archives/2006/01/countering_trus.html

attaque de type « *backdoor by design* » (tels que les scénarios du programme BULLRUN) et ainsi de les écarter. Cela permet d'augmenter la fiabilité des logiciels et systèmes en augmentant l'assurance que ceux-ci reposent bien sur le principe du « *privacy by design* » et qu'ils n'ont pas été détournés en « *backdoor by design* ».

Dans cette perspective, cette propriété de reproductibilité pourra avantageusement s'intégrer dans les différents aspects prévus par le projet de règlement européen. Nous y voyons particulièrement la disposition concernant la certification de l'article 39, 1 decies du règlement que nous aborderons en section infra. Ainsi, des logiciels dont le régime juridique aménage la propriété de reproductibilité[41] pourraient recevoir une certification correspondante afin de les distinguer de ceux ne permettant pas une vérification par tout tiers indépendant (en ce compris l'utilisateur final lui-même) via le mécanisme prévu à l'article 39 du projet de règlement européen concernant les données à caractère personnel.

Cette réponse aux portes dérobées lors de la conception de logiciel rentre dans la droite ligne de l'état d'esprit émanant de la résolution du Parlement européen concernant la NSA.

En outre, Le Conseil National du Logiciel Libre (CNLL) est l'instance représentative en france, des associations et groupements d'entreprises (plus de 400 entreprises françaises spécialisées ou avec une activité significative dans le logiciel libre du logiciel libre en France.) a publié une enquête en avril 2014 touchant 139 entreprises du secteur concernant les révélations de Snowden et leur positionnement, ainsi que l'impact de ces informations. D'une part, le constat tiré est identique au observation de Parlement européen dans sa résolution NSA/vie privée. D'autre part, il semble avoir une unanimité quant à la crise de confiance soulevée par ces révélations. Ainsi, « *Ils sont 94% à estimer que certains logiciels propriétaires répandus ont des portes dérobées intégrées sous la contrainte des services d'espionnage. Ils jugeraient sans doute très étonnant que le Ministère de la Défense français ait choisi de confier une immense partie de son informatique à Microsoft dans le cadre d'un grand contrat dit « open bar*[42][43] ». L'étude continue quant à l'impact pour la sécurité informatique et celui du logiciel libre en tant que facteur d'adoption pour un renforcement du controle de la chaine de conception, de distribution et d'usage. Ainsi « *Seulement 59 % d'entre eux pensent que les révélations de Edward Snowden vont conduire à une attractivité accrue des logiciels open source. Sans doute perçoivent-ils que la gravité extrême de logiciels corrompus n'est pas encore bien comprise, tant du grand public que de bon nombre de décideurs.*[44]». Finalement, « *70 % (...) rapportent que leurs clients sont soucieux de conserver leurs données dans un centre d'hébergement situé en France.* »[45] Cette étude confirme largement les positions du

41 Article 2 §2 de la GPL 2 et GPL 3 - GNU general public licence.

42 http://www.april.org/open-bar-microsoftdefense-renouvele-jusquen-2017-quand-des-changements

43 http://www.cnll.fr/news/resultats-etude-2014/ ; http://www.cnll.fr/static/pdf/CNLL-Survey-2014-F.pdf p. 22

44 *Ibidem*

45 *Ibidem*

Parlement européen en tant que reflets des préoccupations actuels. Elle consolide la tendance au renforcement d'une protection effective des données à caractère personnel via des mesures de sécurité transparentes et vérifiables.

Nous allons examiner le règlement européen afin d'une part d'analyser la manière dont il envisage la question sur les mécanismes de protection et de sécurité mis en place utiles à la reproductibilité et d'autre part nous élargirons le champ afin de faire le tour des autres mécanismes de sécurité renforcée prévus par le règlement.

VII. Les mesures de sécurité prévues par le projet de règlement européen concernant la protection des données à caractère personnel

Ce règlement prévoit un certain nombre d'innovations par rapport aux textes précédents réglant la matière (directive vie privée). D'une part, au niveau du champ d'application, étant un règlement européen, celui-ci sera d'effet direct sans nécessité de transposition dans les États membres. Cela permettra d'harmoniser les règles relatives à la protection de la vie privée dans l'ensemble des États membres de l'Union européenne.

En second lieu, notons que les innovations apportées par ce texte pourraient avoir des conséquences importantes sur la question des mesures techniques et organisationnelles de sécurité pour la protection des données personnelles. En effet, les obligations imposées sont consécutivement plus précises dans leurs objectifs et moyens et plus larges dans leur étendue. Cela nous amène à considérer les recommandations formulées plus haut comme une préparation en adéquation avec le projet de règlement européen. Nous allons examiner les différents aspects concernant l'obligation de sécurité à charge du responsable de traitement.

7.1. Mécanismes de protection des données dès la conception et des données par défaut

L'article 23 du règlement fait écho à la résolution NSA/vie privée qui « rappelle que les notions de "prise en compte du respect de la vie privée dès la conception" et de "respect de la vie privée par défaut" participent au renforcement de la protection des données et devraient avoir le statut de norme pour tous les produits, services et systèmes proposés sur l'internet ».

L'article 23 en son premier paragraphe dispose ainsi que :

« *Compte tenu des techniques les plus récentes, des connaissances techniques actuelles, des meilleures pratiques internationales et des risques représentés par le traitement des données , le responsable du traitement et le sous-traitant éventuel appliquent, tant lors de la définition des objectifs et des moyens de traitement que lors du traitement proprement dit, des mesures et procédures techniques et organisationnelles appropriées et proportionnées, de manière à ce que le traitement soit conforme aux prescriptions du présent règlement et garantisse la protection des droits de la personne concernée, notamment en ce qui concerne les principes établis à l'article 5. La protection des données dès la conception tient compte en particulier de la gestion du cycle de vie complet des données à caractère personnel, depuis la collecte jusqu'à la suppression en passant par le traitement. Elle est systématiquement axée sur l'existence de garanties procédurales globales en ce qui concerne l'exactitude, la confidentialité, l'intégrité, la sécurité physique et la suppression des données à caractère personnel. Une fois que le responsable du traitement a procédé à une analyse d'impact relative à la protection des données, conformément à l'article 33, les résultats sont pris en compte lors de l'élaboration desdites mesures et procédures.* »

L'idée est d'utiliser les techniques les plus récentes pour mettre en œuvre des mécanismes qui vont garantir que dès la conception seules seront traitées les données à caractère personnel nécessaires à chaque finalité spécifique du traitement. Ces mécanismes devant ainsi assurer que les données ne sont pas collectées ou conservées au-delà de la durée nécessaire à ces finalités. Ces technologies vont faciliter le principe de minimisation. En cela, le « *privacy by design* » permettra en tant que principe d'écarter à priori l'intégration de portes dérobées lors de la conception. En outre le caractère par défaut permet de mettre en œuvre des paramètres, des fonctionnalités privilégiant et facilitant par défaut une configuration qui protège la vie privée des utilisateurs. Ainsi, en limitant par exemple les données collectées dès le départ, leur durée de vie ou les conditions d'accès et de traitements ou bien qui permettent de supprimer les corrélations entre les données de connexion et les données personnelles qui rendent possible l'identification de l'internaute.

7.2. Label européen et procédure de certification

Le considérant 77 dispose que « *Afin de favoriser la transparence et le respect du présent règlement, la création de mécanismes de certification, ainsi que de labels et de marques normalisées en matière de protection des données, devrait être encouragée pour permettre aux personnes concernées d'évaluer rapidement, de manière fiable et vérifiable, le niveau de protection des données offert par les produits et services en question. Un « label européen de protection des données » devrait être établi au niveau européen afin de générer un climat de confiance chez les personnes concernées et une sécurité juridique pour les responsables du traitement* ».

Ce considérant est la transposition de l'idée de certification et de label qui avait été déjà évoquée dans la résolution de procédure et de « marque » permettant d'augmenter la visibilité pour les acteurs de marché présentant le plus de garanties quant à la protection des données. Le caractère vérifiable se retrouve dans la disposition comme faisant référence à un contrôle possible par des tiers indépendants. Ce caractère se retrouve à l'article 39,1quiquies du règlement qui dispose comme suit que :

« *1 quinquies. Pendant la procédure de certification, l'autorité de contrôle peut agréer des auditeurs tiers spécialisés pour effectuer en son nom l'audit du responsable du traitement ou du sous-traitant. Les auditeurs tiers disposent de personnel suffisamment qualifié, sont impartiaux et libres de tout conflit d'intérêts par rapport à leurs fonctions. Les autorités de contrôle révoquent l'agrément lorsqu'il existe des raisons de croire que l'auditeur ne remplit pas correctement ses fonctions. La certification finale est octroyée par l'autorité de contrôle.* »

Les mécanismes de certification en matière de protection des données vont contribuer à la bonne application du cadre réglementaire. Elles peuvent prendre en compte les spécificités sectorielles qui peuvent exister. L'article 39 en tant que siège de la matière dispose que :

« *1 bis. Tout responsable du traitement ou sous-traitant peut demander à n'importe quelle autorité de contrôle dans l'Union de certifier, moyennant le paiement de frais raisonnables tenant compte des coûts administratifs, que le traitement des données à caractère personnel est exécuté conformément au présent règlement, notamment aux principes énoncés aux articles 5, 23 et 30, et dans le respect des obligations du responsable du traitement et du sous-traitant, ainsi que des droits des personnes concernées.*

1 ter. La certification est volontaire, abordable et disponible au travers d'un processus transparent et ne présentant pas de complications injustifiées. »

La validité du label européen venant du mécanisme de certification est de 5 ans (article 39;1 octies), l'agrément peut être retiré néanmoins dans le cas où la conformité ne serait

plus présente (article 39, 1 septies). Un registre public est établi afin de permettre aux acteurs de terrain de connaître la validité ou non d'un label en cours (article 39, 1 nonies).

L'article 39, 1 decies est particulièrement intéressant quant à la question de la reproductibilité évoquée dans la section concernant les pratiques de sécurité *open source*. Ainsi, l'article dispose que :

« *Le comité européen de la protection des données peut, de sa propre initiative, certifier qu'une norme technique renforçant la protection des données est conforme au présent règlement.* »

Ainsi, il serait possible de faire certifier des systèmes, logiciels et produits permettant de garantir les conditions de la reproductibilité et renforçant par là l'approche « *privacy by design* ».

Trois sanctions sont possibles en cas de violation du règlement à savoir[46] : un avertissement par écrit lors d'une première infraction non intentionnelle ; des vérifications périodiques régulières de la protection des données. Mais la sanction la plus importante prévoit que « *une amende pouvant atteindre 100.000.000 EUR ou au maximum 5 % du chiffre d'affaire annuel mondial dans le cas d'une entreprise, le montant le plus élevé devant être retenu* ». Il est prévu que dans le cas où le responsable de traitement avait obtenu un label qui est valide et qu'une infraction se produit néanmoins, une atténuation de la responsabilité de celui-ci est accordée. Ainsi l'article 2 ter dispose que « *Si le responsable du traitement ou le sous-traitant est détenteur d'un « label européen de protection des données » valable, conformément à l'article 39, l'amende prévue au point c) du paragraphe 2 bis) sera exclusivement appliquée dans les cas de manquement de propos délibéré ou par négligence.* ». Afin d'évaluer la sanction administrative, l'autorité compétente prend en compte une série de facteur énumérés à l'article 39, 2 quater dont « *le niveau des mesures et procédures techniques et d'organisation mises en œuvre conformément à*

- *l'article 23 – Protection des données dès la conception et protection des données par défaut ;*
- *l'article 30 – Sécurité des traitements ;*
- *l'article 33 – Analyse d'impact relative à la protection des données* ».

Ce mécanisme de certification et de labellisation permet à n'en pas douter un renforcement accru de l'effectivité de la protection des données à caractère personnel. Le pouvoir de sanction étant la pierre angulaire de cette configuration. Le pouvoir de certifier des normes techniques permettant d'atteindre et d'aider à atteindre les objectifs du règlement est particulièrement bienvenu et est en adéquation avec le contexte de la résolution NSA/vie privée du Parlement européen. Il semble ainsi que la mise en œuvre de normes d'excellence en ce qui concerne la labellisation et la certification, semble un des objectifs ambitieux du législateur européen. De manière générale, les systèmes, logiciels et méthodes ouvertes préconisés par la résolution semble être adaptés pour

46 Article 39, 2 bis c).

rencontrer les exigences du règlement promu par le législateur européen et de manière plus particulière quant à l'exigence de garantie entourant la notion de « privacy *by design* ». Finalement, la garantie d'indépendance des auditeurs est un autre gage allant dans cette voie

7.3. Obligation de sécurité via des mesures techniques et organisationnelles renforcées

L'article 30[47] du règlement dispose que :

« *Le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques présentés par le traitement, en tenant compte des résultats de l'analyse d'impact relative à la protection des données conformément à l'article 33, ainsi que des techniques les plus récentes et des coûts liés à leur mise en œuvre.* »

Un certain nombre de critères sont précisés au paragraphe suivant concernant notamment la politique de sécurité mise en œuvre. Ainsi, il dispose que « *Compte étant tenu des techniques les plus récentes et des coûts liés à leur mise en œuvre, cette politique de sécurité inclut :*

- *a) la capacité de garantir l'intégrité de la personne concernée ;*
- *b) la capacité de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement des données à caractère personnel ;*
- *c) la capacité de rétablir la disponibilité des données et l'accès à celles-ci, dans les plus brefs délais, en cas d'incident physique ou technique qui compromet la disponibilité, l'intégrité et la confidentialité des systèmes et des services d'information ;*
- *d) s'agissant de données à caractère personnel sensibles, au sens des articles 8 et 9, des mesures de sécurité supplémentaires afin d'assurer la prise de conscience pleine et entière des risques et la capacité de prendre des mesures de prévention, de correction et d'atténuation, presque en temps réel, contre les faiblesses et les incidents décelés qui pourraient présenter un risque pour les données ;*
- *e) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des politiques, des procédures et des plans de sécurité mis en place pour assurer une efficacité constante.* »

Le législateur européen a ainsi décidé d'amener des mesures plus précises et des

47 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//FR.

obligations plus concrètes quant à ces mesures afin de remplir de manière la plus effective possible l'objectif dudit règlement.

Nous relevons ainsi que le deuxième paragraphe assigne des objectifs précis au responsable de traitement. Il dispose que « *Les mesures visées au paragraphe 1 poursuivent au moins les objectifs suivants :*

- *a) garantir que seules des personnes autorisées peuvent avoir accès aux données à caractère personnel à des fins légalement autorisées ;*
- *b) protéger les données à caractère personnel stockées ou transmises contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelles et le stockage, le traitement, l'accès et la divulgation non autorisés ou illicites ; et*
- *c) assurer la mise en œuvre d'une politique de sécurité relative au traitement des données à caractère personnel.* »

7.4. Étude d'impact sur la vie privée ou PIA (Privacy Impact Assesment) - article 33, 32 bis

Le dispositif d'étude d'impact est prévu par l'article 32 bis et 33 du règlement. Lorsque le traitement présente des risques particuliers par rapport aux droits et libertés des personnes faisant l'objet de ce traitement, soit du fait de leur nature, de leur portée, ou du fait de la finalité, le responsable de traitement doit faire une étude d'impact. L'analyse doit contenir les mesures envisagées pour faire face à ces risques, les garanties, les mesures de sécurité mises en œuvre, ainsi que les mécanismes permettant d'apporter la preuve de la conformité du traitement.

Il s'agit d'une évaluation qui va se faire en amont de la mise en place du système de traitement automatisé avant de décider de sa mise en place réelle. Cette gestion doit se faire sur tout le cycle de vie du traitement des données à caractère personnel. Ainsi que le prévoit le point 3 de l'article 33 : « *L'analyse porte sur la gestion de la totalité du cycle de vie des données à caractère personnel, de la collecte à la suppression, en passant par le traitement* ».

Les mesures techniques et organisationnelles de sécurité de l'article 30 étant un volet de cette analyse de risque lors du traitement.

7.5. L'obligation de notification des failles de sécurité

La notification des failles de sécurité aux autorités de contrôle de données et aux personnes concernées devient une obligation légale prévue à l'article 31 du nouveau règlement européen.

Le projet de règlement pose l'obligation de notifier à l'autorité de contrôle « *la violation de données à caractère personnel sans retard injustifié après en avoir pris connaissance* ». Selon le considérant 67, cette notification devrait se faire « *soit dans un délai inférieur à 72 heures. Le cas échéant, la notification devrait être assortie d'une explication concernant ce retard*. » En outre, le responsable de traitement doit :

- « *c) recommander des mesures à prendre pour atténuer les éventuelles conséquences négatives de la violation de données à caractère personnel ;*
- *d) décrire les conséquences de la violation de données à caractère personnel ;*
- *e) décrire les mesures proposées ou prises par le responsable du traitement pour remédier à la violation de données à caractère personnel et en atténuer les effets.* »

Finalement le paragraphe 4 prévoit que : « *Le responsable du traitement conserve une trace documentaire de toute violation de données à caractère personnel, en indiquant son contexte, ses effets et les mesures prises pour y remédier. La documentation constituée doit être suffisante pour permettre à l'autorité de contrôle de vérifier le respect des dispositions du présent article et de l'article 30* ».

Ainsi, le responsable de traitement devra tracer l'ensemble des incidents de sécurité dans l'organisation (étant donné que ces incidents peuvent mener à une violation des données). Le responsable de traitement devra aussi exiger la même chose de ses sous-traitants.

7.6. Architecture documentaire et principe d'*accoutability*

Le principe d'*accoutability* signifie que les données à caractère personnel sont traitées de manière conforme et que le responsable de traitement peut apporter la preuve de la conformité de chaque opération. Le principe d'*accountability* n'est pas totalement nouveau car il figure déjà dans les lignes directrices de l'OCDE régissant la vie privée. De même la Conférence internationale des commissaires à la protection des données et de la vie privée en octobre 2010. Finalement le groupe de l'article 29 considère que ce principe est nouveau en ce sens qu'il oblige le responsable de traitement à apporter la preuve de la

bonne gestion au quotidien de la conformité des traitements[48].

Dans le projet de règlement européen cela se traduit par l'article 28 qui met à charge du responsable de traitement des obligations documentaires renforcées. Cet article dispose que : « *Chaque responsable de traitement et chaque sous-traitant conserve une trace documentaire régulièrement mise à jour nécessaire au respect des exigences établies dans le présent règlement.* » Elle doit comporter un certain nombre d'informations qui permettent la traçabilité (le nom, les coordonnées du responsable de traitement, les informations du délégué à la protection des données, les finalités du traitement et les intérêts légitimes poursuivis par le responsable de traitement…).

Cette documentation doit aussi comporter les délais impartis pour l'effacement des différentes catégories de données. La documentation doit aussi prévoir les mécanismes qui ont été mis en place pour vérifier l'efficacité des mesures prises. Le responsable de traitement doit pouvoir démontrer que le traitement est opéré de manière conforme avec le cadre règlementaire. Cette obligation vise aussi les sous-traitants.

Dès lors, il sera nécessaire de tracer matériellement le respect des obligations dans l'organisation et de maintenir l'architecture documentaire afférente à cette obligation. De plus, dans le cas de sous-traitance, il sera nécessaire de prévoir une clause concernant la mise en œuvre de cette documentation.

Conclusion

Ce rapide tour d'horizon des mesures de sécurité prévues par la loi « vie privée » belge et renforcées dans le futur projet de règlement européen concernant la protection des données à caractère personnel nous a permis de mesurer l'état du droit sur la question et sa mise œuvre, ainsi que les perspectives futures quant à un renforcement des mesures de sécurité via le règlement européen. Ce règlement a pour but notamment d'apporter une réponse effective à la violation massive de la vie privée permise par les programmes de surveillance indiscriminés de la NSA. La résolution du Parlement européen sur la question préconise une approche renforcée qui a pour but d'apporter une réponse à la radicalité même des révélations de Snowden. À ce titre, les logiciels, systèmes, normes ouverts permettant une vérification par tout tiers indépendant est privilégiée par l'institution. En outre l'idée de la « *privacy by design* » permet aussi de s'opposer au détournement de finalité permis par le « *backdoor by design* ». Les systèmes ouverts ont proposé en réponse à la surveillance de masse notamment la notion de reproductibilité

48 Http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_fr.pdf.

qui permet d'assurer que les conditions du « *privacy by design* » puissent être rencontrées. Ainsi, dès la conception d'un système de traitement informatique celui-ci n'est pas détourné de sa finalité par l'implémentation de portes dérobées. Une certification de la reproductibilité serait souhaitable afin que les acteurs de terrain (entreprises, administrations etc.) puissent reconnaitre les composants informatiques proposant l'attribut de reproductibilité. À coté de ces avancées, le règlement prévoit aussi des mesures de sécurité à différents niveaux permettant d'accompagner de manière globale et effective l'objectif d'un haut niveau de protection des données à caractères personnel. La résolution du Parlement européen concernant la NSA a permis de renforcer l'optique d'une protection accrue, et l'on ne peut que se réjouir qu'elle trouve enfin une expression dans un règlement. Ainsi, différents instruments ont été mis en place, et concourent tous à une augmentation de la sécurité et de la fiabilité dès la conception d'un système faisant un traitement de données à caractère personnel.

Nous ne pouvons que saluer cette tendance à rendre effective la protection des données à caractère personnel, rendue indispensable dans un monde ou l'évolution technologique permet une surveillance de masse de plus en plus efficace, qui actualise la figure de *Big Brother*. Cette vigilance doit être doublée, lorsque l'on sait que des catégories de données que l'on croyait hier sans intérêt, permettent aujourd'hui, par l'intermédiaire du croisement massif de données (*Big* data), d'arriver à donner des images très précises des gens, et que ces développements s'accélèrent de jour en jour[49].

Cette question cruciale est en train de déterminer le type de société dans laquelle nous souhaitons vivre dans les prochaines décennies. À la lumière d'une actualité révélant régulièrement un mépris de notre droit fondamental à la vie privée et à l'autodétermination permise par celui-ci[50], il serait coupable ou naïf de fermer les yeux sur ces questions qui orientent le devenir de nos sociétés démocratiques hyper-connectées.

---

49 Citons une étude établissant qu'il est possible d'identifier 90 % des Américains à partir de 3 données : date de naissance, code postal, et âge (http://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/). Il serait donc possible, au sein d'une étude en principe anonymisée et ne recourant qu'à ces 3 informations, de savoir qui y a répondu. De la même manière, l'on peut établir l'orientation politique d'un individu à partir de ses goûts musicaux (http://www.zdnet.fr/actualites/pandora-dis-moi-ce-que-tu-ecoutes-je-te-dirai-pour-qui-tu-votes-39797826.htm) ou de ses goûts en matière d'alcool (http://www.slate.fr/life/81849/electeurs-gauche-preferent-vodka-electeurs-droite-whisky), identifier une personne à partir de 3 achats (http://www.slate.fr/story/97453/carte-credit-identifier-achats), ou encore établir un profil de personnalité à partir de ses like sur Facebook (http://geeko.lesoir.be/2013/04/08/liker-sur-facebook-revele-votre-personnalite/).

50 Arrêt de la Cour constitutionnelle allemande du 15 décembre 1983, *Volkszählungsurteil*, BVerfGE Bd. 65, S. 1 ff.).

Table des matières