

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Interconnexions et cybersécurité

Dumortier, Franck; Descamps, Benjamin

Published in:

Revue du Droit des Technologies de l'information

Publication date:

2018

Document Version

le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

Dumortier, F & Descamps, B 2018, 'Interconnexions et cybersécurité', *Revue du Droit des Technologies de l'information*, numéro 70, pp. 31-52.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Interconnexions et cybersécurité

Franck Dumortier¹ et Benjamin Descamps²

Dans cette contribution, après avoir brièvement décrit les interconnexions techniques qu'impliquent les architectures big data et avoir évoqué les principales normes réglementant la sécurité informationnelle au sein de celles-ci, nous rappelons que l'obligation de cybersécurité reste une obligation de moyens. Celle-ci a néanmoins été renforcée grâce au principe d'accountability qui impose, entre autres, la réalisation d'une analyse d'impact avant le traitement de mégadonnées considérées. Étant donné les risques techniques liés notamment à la masse de données traitées mais aussi au niveau élevé de stockage distribué et à l'externalisation fréquente des traitements, nous mettons l'accent sur certaines mesures de sécurité essentielles à l'ère du big data – dont le contrôle d'accès logique, l'authentification et la journalisation – permettant d'imputer adéquatement les responsabilités entre les divers acteurs en cas d'incident.

INTRODUCTION

La sécurité des données informatiques³ – en ce compris celle des données à caractère personnel au sens large⁴ – est devenue un enjeu majeur, non seulement pour tous les

aspects de notre vie privée⁵, mais également pour notre économie en ce qu'elles dépendent désormais considérablement de la *confidentialité*, de l'*intégrité* et de la *disponibilité* de traitements d'informations à grande échelle. La garantie de ces «trois critères de sécurité classiques»⁶ a récemment été légalement

¹ Maître de conférences. Chercheur au CRIDS.

² Commandant. Ministère de la défense.

³ Cette notion apparaît dans l'article 1^{er} de la Convention de Budapest (Convention sur la cybercriminalité STE n° 185 du Conseil de l'Europe, Budapest, 11, 2001) qui définit «données informatiques» comme toute «représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction». Voy. également l'article 2, b), de la directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.

⁴ Voy. la définition large de «données à caractère personnel» prônée par le Groupe 29 dans son Avis 4/2007 sur le concept de données à caractère personnel, WP136, 20 juin 2007. Voy. également Y. POULLET, «La protection des données : un nouveau droit constitutionnel – pour une troisième génération de réglementations de protection des données», in *Droit constitutionnel et vie privée*, Thunis, 2008 pp. 297-365.

⁵ Dans l'affaire *I. c. Finlande*, la Cour européenne des droits de l'homme a estimé que le défaut de garanties relatives à la sécurisation des données contre des usages non autorisés constituait une violation de l'obligation positive d'assurer le respect du droit à la vie privée consacré à l'article 8 de la Convention européenne des droits de l'homme (ci-après «CEDH»). Cour eur. D.H., 17 juillet 2008, *I. c. Finlande*, req. n° 20511/03. Dans cette affaire, la requérante, infirmière, dénonce la consultation illégale de son dossier médical confidentiel par ses collègues de travail. Dans son arrêt, la Cour conclut, à l'unanimité, qu'il y a eu violation de l'article 8, les autorités internes n'ayant pas, au moment des faits, mis les données médicales de la requérante à l'abri d'un accès non autorisé.

⁶ Groupe 29, Avis 03/2014 sur la notification des violations de données à caractère personnel, WP213, 25 mars 2014, p. 5. Le Groupe s'inspire clairement de l'ISO/CEI 27001 qui insiste particulièrement sur le triptyque «Disponibilité – Intégrité – Confidentialité». L'ISO/CEI 27001 est une norme internationale de sécurité des systèmes d'information dont le titre est «Technologies de l'information – Techniques de



renforcée, notamment suite à l'élévation de l'obligation de sécurité au rang de principe de base⁷ dans le RGPD⁸ et l'adoption de la directive NIS⁹. Dans le contexte du big data¹⁰, dont l'une des caractéristiques principales est l'*interconnexion* de quantités sans cesse croissantes de données de type et de qualité variables, réparties dans différents supports traditionnels, mobiles ou dans le Cloud, l'on ne peut que féliciter le législateur d'avoir pris la mesure de l'importance de la cybersécurité. Nous regrettons toutefois qu'outre la reconnaissance des trois critères de sécurité classiques, l'occasion ne fut pas saisie afin de formaliser de manière non équivoque les fonctions *d'imputabilité*¹¹,

*d'authenticité*¹² et de *non-répudiation*¹³ des données, lesquelles nous semblent essentielles pour assurer l'effectivité de la sécurité informationnelle à l'ère du big data. En effet, étant donné le nombre d'acteurs, d'équipements et de processus impliqués dans l'environnement des mégadonnées, les mesures de contrôle d'accès, d'authentification et de journalisation apparaissent comme étant fondamentales, non seulement à des fins de transparence vis-à-vis des personnes concernées, mais également afin d'être en mesure d'imputer adéquatement les responsabilités en cas d'incident.

I. BIG DATA ET INTERCONNEXIONS « TECHNIQUES »

Selon le National Institute of Standards and Technology, le paradigme du big data consiste en la distribution de systèmes de données à travers des ressources indépendantes couplées horizontalement pour atteindre la « scalabilité » nécessaire au traitement efficace de datasets étendus¹⁴. En d'autres mots, le concept désignerait l'ensemble des technologies, infrastructures et services permettant la collecte, le stockage et l'analyse de données recueillies et produites en nombre croissant. Dans ce contexte, les objets connectés jouent un rôle déterminant en termes de *vélocité* et de *variété* en générant constamment des données – structurées ou non – en temps réel. La solu-

sécurité – Systèmes de gestion de sécurité de l'information – Exigences». Elle fait partie de la suite ISO/CEI 27000 et permet de certifier des organisations.

⁷ Au même titre que les traditionnels principes de qualité des données (licéité, loyauté, transparence, finalité, minimisation, exactitude et limitation de la conservation des données). À ce sujet, voy. F. DUMORTIER, «La sécurité des traitements de données, les analyses d'impact et les violations de données», in *Le règlement général sur la protection des données: Analyse approfondie*, sous la coordination de K. ROSIER et C. DE TERWANGNE, Bruxelles, Larcier, 2018, à paraître.

⁸ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

⁹ Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (ci-après «directive NIS»).

¹⁰ Selon le National Institute of Standards and Technology (NIST) big data Public Working Group, «*big data consists of extensive dataset primarily in the characteristics of volume, variety, velocity, and/or variability that require a scalable architecture for efficient storage, manipulation, and analysis*». Voy. NIST big data Interoperability Framework: Volume 1, Definitions, version 2, juin 2018, p. 6, disponible à l'adresse https://bigdatawg.nist.gov/_uploadfiles/NIST.SP.1500-1r1.pdf.

¹¹ Selon la Commission de la protection de la vie privée devenue l'Autorité de protection des données (ci-après «APD») depuis l'entrée en application du RGPD, «l'imputabilité est la propriété qui garantit que les actions

d'une entité sont tracées et attribuées à cette seule entité». APD, «Note relative à la sécurité des données à caractère personnel», p. 2, disponible à l'adresse https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/note_securite_des_donnees_a_caractere_personnel.pdf.

¹² Selon l'APD, «l'authenticité est la propriété d'une entité d'être bien celle qu'elle prétend être», *Ibidem*.

¹³ Selon l'APD, «la non-répudiation est la propriété d'une action ou d'un événement d'avoir bien eu lieu et de ne pouvoir être nié ou nié ultérieurement», *Ibidem*.

¹⁴ Voy. NIST big data Interoperability Framework: Volume 1, Definitions, version 2, juin 2018, *op. cit.*, p. 6.



tion pour faire face au *volume* de données ainsi collectées est le stockage distribué, entraînant la conservation à différents endroits desdites données. Cela revient souvent à une forme de stockage dans le Cloud¹⁵ à partir duquel ou dans lequel les données – de sources et de types divers – sont ingérées par des plateformes d'analyse¹⁶ et/ou de partage en streaming¹⁷ afin d'en extraire de la *valeur*, c'est-à-dire du sens.

De manière non exhaustive, ce type d'architecture intéresse évidemment les entreprises privées qui poursuivent des fins de profilage publicitaire – pensons, par exemple, au succès croissant des enceintes connectées¹⁸ –, les administrations publiques – notamment pour détecter diverses formes de fraude grâce à l'analyse de données générées par des capteurs « intelligents »¹⁹ – mais également

les services de police dans l'exercice de leurs missions. En témoigne la récente modification de la « loi caméras »²⁰ dans laquelle une attention particulière a été apportée à la définition d'un cadre pour l'utilisation de caméras de reconnaissance automatique de plaques d'immatriculation (ANPR) et leur interconnexion avec des banques de données policières – dont notamment la BNG²¹ –, ou encore le projet « i-Police » dont l'implémentation dans un but de « prédictive policing » est prévue pour 2020²². Enfin, depuis les révélations d'Edward Snowden à propos des programmes PRISM et Upstream, l'on sait également que les services de renseignements ne sont pas en reste en la matière²³.

Outre les multiples finalités pour lesquelles les entreprises privées et les autorités publiques font usage du big data, l'ENISA²⁴ considère que l'un des domaines les plus prometteurs est son utilisation à des fins de gestion des événements

¹⁵ Selon le NIST : « *Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction* ». Voy. <http://www.nist.gov/itl/cloud/>.

¹⁶ Une structure logicielle populaire en la matière est *Apache Hadoop*, une implémentation open-source de la structure MapReduce, permettant le traitement parallèle et distribué de données à grande échelle.

¹⁷ Un exemple d'un tel type de plateforme est *Apache Kafka*. Il s'agit d'un outil d'échange de données en streaming conçu pour remplacer les courtiers de message traditionnels. De nombreuses firmes l'ont adopté, à tel point que Kafka est aujourd'hui considéré comme une plateforme standard pour les pipelines de traitement de données.

¹⁸ À ce sujet, voy. CNIL, « Enceintes intelligentes : des assistants vocaux connectés à votre vie privée », 5 décembre 2017, disponible à l'adresse <https://www.cnil.fr/fr/enceintes-intelligentes-des-assistants-vocaux-connectes-votre-vie-privee>.

¹⁹ Un exemple parmi d'autres est le contrôle énergétique. À ce sujet, voy. F. GREVISSE et V. VAN DER PLANCKE, « La fraude sociale à l'épreuve des consommations énergétiques », *Revue Démocratie*, septembre 2015, disponible à l'adresse http://www.socialenergie.be/wp-content/uploads/article_democratie-1.pdf. Tout récemment, le secrétaire d'État fédéral Philippe De

Backer annonçait employer les données des prélèvements kilométriques et des caméras ANPR dans le cadre de la lutte contre la fraude sociale. Voy. https://www.rtf.be/info/belgique/detail_de-backer-veut-utiliser-le-big-data-pour-lutter-contre-la-fraude-sociale?id=9887321.

²⁰ Loi du 21 mars 2018 modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière, *M.B.*, 16 avril 2018, p. 33691.

²¹ Au sujet de la BNG, voy. F. DUMORTIER, « La banque de données nationale générale : l'œil de Sauron ? », 2016, *Kairos*, n° 24, pp. 10-11.

²² Voy. « La police va prévoir la criminalité grâce à des algorithmes », *Le Soir*, 30 août 2018.

²³ À cet égard, voy. le récent arrêt Cour eur. D.H., 13 septembre 2018, *Big brother watch and others v. the United Kingdom*, req. nos 58170/13, 62322/14 et 24960/15.

²⁴ Pour rappel, l'ENISA est l'Agence européenne chargée de la sécurité des réseaux et de l'information, telle que régie par le règlement (UE) n° 526/2013.



et des incidents de sécurité²⁵. Ainsi, les SIEM²⁶ de seconde génération ont recours aux outils du big data pour offrir aux professionnels de la cybersécurité la capacité d'assurer le stockage, la corrélation et l'analyse en temps réel de logs²⁷ en provenance de sources diverses dans le but d'augmenter l'efficacité de la détection de menaces et de la gestion d'incidents²⁸.

Quel que soit l'objectif poursuivi par ses exploitants, l'utilisation d'une architecture big data a fatalement pour conséquence une *intensification d'interconnexions techniques* souhaitées mais présente également des risques accrus de tsunamis de données non autorisées. Qui plus est, selon la finalité poursuivie et/ou la qualification juridique de la personne physique ou morale responsable de la sécurité du traitement de mégadonnées, différents régimes juridiques peuvent trouver à s'appliquer, et ce parfois de manière cumulative, avec pour

conséquence un *accroissement d'interconnexions légales*.

II. BIG DATA ET INTERCONNEXIONS « LÉGALES »

Des obligations de cybersécurité découlent tout d'abord des législations assurant le respect du droit à la vie privée dès lors qu'il y a traitement de « données à caractère personnel ». Ce concept mérite une interprétation large dans le contexte du big data puisque son objectif intrinsèque est la corrélation d'informations grâce auxquelles il est « parfois relativement facile d'identifier des individus de manière unique à partir de données apparemment anonymes »²⁹. En cette matière, les articles 32 et suivants du RGPD s'appliquent tant aux entreprises privées qu'aux administrations publiques lorsqu'elles agissent comme « responsables du traitement » ou « sous-traitants »³⁰, tous deux considérés comme débiteurs de l'obligation de sécurité sous l'empire du règlement. Des dispositions spécifiques sont prévues pour les activités de traitement effectuées par les

²⁵ ENISA, « Big data Security: Good Practices and Recommendations on the Security of big data Systems », décembre 2015, p. 10, disponible à l'adresse https://www.enisa.europa.eu/publications/big-data-security/at_download/fullReport.

²⁶ SIEM signifie Security Information and Event Management ou gestion des informations et des événements de sécurité. On peut définir le SIEM comme la collecte d'événements en temps réel, la surveillance, la corrélation et l'analyse des événements à travers des sources disparates.

²⁷ Un « log », « logfile » ou encore « fichier journal » est un fichier contenant des événements se produisant au sein des systèmes d'information et réseaux d'une organisation. Ces logs peuvent être générés par de multiples applications, comme par exemple un système d'exploitation, un antivirus, un firewall, un système de détection d'intrusion ou de prévention, et, de manière plus générale, par n'importe quel programme installé sur un serveur, un poste de travail ou un équipement de réseautique. NIST, Guide to Computer Security Log Management, septembre 2006, p. 9.

²⁸ Pour un aperçu de ce type de technologies, voy. ENISA, « Big data Threat Landscape and Good Practice Guide », janvier 2016, pp. 56 à 59, disponible à l'adresse https://www.enisa.europa.eu/publications/bigdata-threat-landscape/at_download/fullReport.

²⁹ APD, « Rapport big data », 2017, p. 9, disponible à l'adresse https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Rapport_Big_Data_2017.pdf. L'ENISA cite les exemples suivants: « *The AOL data breach already in 2006 was one of the first widely known cases of re-identification: the company's release of users' search logs allowed singling out certain users based on their searches. The Netflix case followed in 2007 when researchers identified individual users by matching data sets with film ratings on the Internet Movie Database. In 2012 the retail company Target, using behavioural advertising techniques, managed to identify a pregnant teen girl from her web searches and sent her relevant vouchers at home* ». ENISA, « Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics », décembre 2015, p. 13, disponible à l'adresse https://www.enisa.europa.eu/publications/big-data-protection/at_download/fullReport.

³⁰ Sur ces concepts, voy. Groupe 29, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », WP169, adopté le 16 février 2010.



«autorités compétentes»³¹ dans le domaine de la prévention et la détection des infractions pénales³², à savoir les articles 29 et suivants de la directive 2016/680/UE³³ (ci-après «directive Police & Justice»). Dans la même logique, dans l'exercice de leurs missions, les services de renseignement et de sécurité sont soumis à un régime dérogatoire inscrit au titre III de la loi d'implémentation belge³⁴. En sus d'exigences en matière de sécurité informationnelle proprement dite, les trois instruments susmentionnés (ci-après «le RGPD et les textes liés») imposent à

leurs débiteurs une discipline d'*accountability*³⁵ concrétisée par la tenue d'un registre³⁶ – devant contenir, dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles –, et, à l'exception notable des services de renseignements, l'obligation pour le responsable du traitement d'effectuer une analyse d'impact relative à la protection des données (ci-après «AIPD») lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques³⁷. Ces documents sont une source non négligeable d'informations utiles pour les autorités afin de jauger la prudence et la diligence dont doivent faire preuve les débiteurs de l'obligation de sécurité à l'ère du big data. Enfin, ces trois

³¹ Les «autorités compétentes» visées ne sont pas uniquement les autorités publiques telles les autorités policières ou judiciaires, mais comprennent de manière large tout organisme ou entité publique et/ou privé disposant en vertu d'une base légale, de prérogatives de puissance publique dans le cadre des finalités visées par la directive. À propos du champ d'application matériel de la directive Police & Justice, voy. C. FORGET, «La protection des données dans le secteur de la "police" et de la "justice"», in *Le règlement général sur la protection des données: Analyse approfondie*, sous la coordination de K. ROSIER et C. DE TERWANGNE, Bruxelles, Larcier, 2018, à paraître.

³² Selon le considérant 27 de la directive Police & Justice, la «prévention des infractions pénales» vise les données collectées dans le cadre d'une enquête spécifique mais aussi les données traitées par les autorités au-delà de ce cadre, pour acquérir une meilleure compréhension de certains phénomènes. Ainsi, l'étude de facteurs sociaux, psychologiques et économiques permettant d'établir des statistiques relatives au comportement menant au crime organisé et au terrorisme par exemple, tombe dans le champ d'application de la directive.

³³ Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

³⁴ Voy. les articles 88 et suivants du titre III de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018, p. 68616.

³⁵ Selon le Groupe 29, «En français, le texte du RGPD utilise le terme «responsabilité». En anglais, on utilise le terme «accountability», issu du monde anglo-saxon où il est d'usage courant et où il existe un vaste consensus sur le sens à lui donner – bien qu'il soit difficile d'en définir avec précision le sens dans la pratique. Globalement, on peut toutefois dire qu'il met l'accent sur la manière dont la responsabilité (responsability) est assumée et sur la manière de le vérifier. En anglais, les termes «responsability» et «accountability» sont comme l'avert et le revers d'une médaille et sont tous deux des éléments essentiels de la bonne gouvernance. On ne peut inspirer une confiance suffisante que s'il est démontré que la responsabilité (responsability) est efficacement assumée dans la pratique. Dans la plupart des autres langues européennes, du fait, essentiellement, de la diversité des systèmes juridiques, il est difficile de traduire le terme «accountability». Groupe 29, Avis n° 3/2010 sur le principe de la responsabilité, WP173, 13 juillet 2010, p. 8.

³⁶ Les articles 30 du RGPD et 24 de la directive Police & Justice imposent la tenue d'un «registre des activités de traitement». Par contre, l'article 90 de la loi d'implémentation belge contraint à la tenue d'un «registre des banques de données» des services de renseignement et de sécurité, celui-ci étant par ailleurs classifié au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, *M.B.*, 7 mai 1999, p. 15752.

³⁷ Voy. les articles 35 du RGPD et 27 de la directive Police & Justice. Le titre III de la loi du 30 juillet 2018 ne prévoit pas cette contrainte à l'égard des services de renseignement et de sécurité.



régimes enjoignent aux responsables de traitements de notifier les violations de données à caractère personnel à leurs autorités de protection des données respectives³⁸, ainsi que, dans certaines hypothèses prévues par le RGPD et la directive Police & Justice³⁹, la communication de ces fuites aux personnes concernées⁴⁰.

Parallèlement à ces dispositions protectrices des droits fondamentaux, la directive NIS – laquelle est en voie de transposition en droit belge – a pour objectif d'affermir *la résilience* des réseaux et des systèmes d'information dans un but de fonctionnement harmonieux du marché intérieur⁴¹, qu'il y ait ou non traitement de données à caractère personnel. Les articles 14 et 16 de cette directive imposent aux «opérateurs de services essentiels»⁴² (ci-après «OSE») et aux «fournisseurs de services numériques»⁴³ (Digital service providers, ci-après

«DSP») des obligations de cybersécurité pour éviter les «incidents»⁴⁴ et réduire au minimum l'impact de ceux-ci sur la continuité de leurs services. De plus, les OSE et les DSP doivent notifier les incidents ayant un impact significatif sur la continuité de leurs services à l'autorité compétente⁴⁵ ou au CSIRT⁴⁶. Certes, la notification des incidents dans le contexte de la directive NIS poursuit un objectif différent de celui que se sont fixés le RGPD et les textes liés. Néanmoins, dans de nombreux cas, des données à caractère personnel seront impliquées à la suite d'incidents au sens de la directive susmentionnée: «dans de telles circonstances, les autorités compétentes [en matière de cybersécurité] et les autorités chargées de la protection des données devraient coopérer et échanger des informations sur tous les aspects pertinents de la lutte contre toute atteinte aux données à caractère personnel à la suite d'incidents»⁴⁷.

³⁸ Dans les circonstances prévues aux articles 33 du RGPD, 30 de la directive Police & Justice et 89 de la loi d'implémentation belge. Selon les mêmes articles, les sous-traitants ont, quant à eux, une obligation de notification aux responsables de traitements.

³⁹ Voy. les articles 34 du RGPD et 31 de la directive Police & Justice.

⁴⁰ Le titre III de la loi du 30 juillet 2018 ne prévoit pas cette obligation pour les services de renseignement et de sécurité.

⁴¹ Voy. les considérants 1 à 3 de la directive NIS.

⁴² Voy. l'article 4, 1), de la directive NIS selon lequel un OSE est défini comme: a) une entité publique ou privée qui fournit un service qui est essentiel au maintien d'activités sociétales et/ou économiques critiques; b) la fourniture de ce service est tributaire des réseaux et des systèmes d'information; c) un incident aurait un effet disruptif important sur la fourniture dudit service. Pour le 9 novembre 2018 au plus tard, les États membres ont l'obligation d'identifier les OSE ayant un établissement sur leur territoire pour chaque secteur et sous-secteur visé à l'annexe II de la directive NIS (énergie, transports, banques, infrastructures de marchés financiers, secteur de la santé, fourniture et distribution d'eau potable, infrastructures numériques).

⁴³ Les types de fournisseurs de services numériques sont repris à l'annexe III de la directive NIS. Sont ainsi visés les «places de marché en ligne», les «moteurs de recherche en ligne» et «les services d'informatique

en nuage» ayant leur établissement principal (siège social) ou un représentant désigné sur le territoire d'un État membre. En effet, un DSP qui n'est pas établi dans l'Union mais qui fournit des services susmentionnés à l'intérieur de l'Union doit désigner un représentant dans l'un des États membres dans lesquels les services sont fournis.

⁴⁴ Dans le contexte de la directive NIS, un «incident» est défini comme étant «tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information», même en l'absence de traitements de données à caractère personnel.

⁴⁵ Voy. l'article 8 de la directive NIS selon lequel chaque État membre désigne une ou plusieurs autorités nationales compétentes ainsi qu'un point de contact national unique en matière de sécurité des réseaux et des systèmes.

⁴⁶ Un CSIRT est un centre de réponse aux incidents de sécurité informatique – également connu sous la dénomination de centre de réponse aux urgences informatiques (CERT) – chargé de la gestion des incidents et des risques selon un processus bien défini. En vertu de l'article 9 de la directive NIS, chaque État membre doit désigner un ou plusieurs CSIRT, se conformant aux exigences énumérées à l'annexe I, point 1) de ladite directive.

⁴⁷ Considérant 63 de la directive NIS.



Les deux cadres légaux susmentionnés s'appliquent de manière cumulative lorsque leurs champs d'application matériels se rencontrent. Ainsi, un opérateur de Cloud considéré comme « sous-traitant » au sens du RGPD sera aussi qualifié de DSP et devra, par conséquent, également respecter les prescrits de la directive NIS à moins qu'il ne s'agisse d'une microentreprise ou d'une petite entreprise telle que définie dans la recommandation 2003/361/CE de la Commission⁴⁸. Dans le contexte du big data, cet exemple illustre d'ailleurs une certaine aberration, l'importance d'un incident n'étant pas forcément liée au chiffre d'affaires ou au nombre de personnes occupées par une société⁴⁹. Heureusement, l'opérateur dudit Cloud ne pourra toutefois pas écarter sa responsabilité découlant de l'application du RGPD en arguant du simple fait qu'il n'a pas connaissance du traitement des données à caractère personnel qu'il héberge⁵⁰. Par conséquent, il sera tenu de notifier au responsable du traitement toute violation de données à caractère personnel « dans les meilleurs délais après en avoir pris connaissance »⁵¹. Dans le cas d'espèce, une clause contractuelle précisant un délai plus précis de notification au responsable du traitement est donc fortement recommandée au risque pour ce dernier de ne pouvoir se conformer au délai « maximum » de 72 heures⁵² en ce qui concerne sa propre notification à l'autorité de protection des données.

III. NATURE DE L'OBLIGATION DE SÉCURITÉ

Il va de soi que les obligations de notification et, le cas échéant, de communication en cas de violations de données et/ou d'incidents doivent être analysées comme étant des obligations de résultat engageant automatiquement la responsabilité de leurs débiteurs en cas de non-respect. À l'inverse, étant donné que l'utopie du risque nul est un mythe⁵³, l'obligation légale de sécurisation proprement dite doit être considérée comme *une obligation de moyens* ne mettant en jeu la responsabilité de ses débiteurs que s'il est prouvé que ces derniers ont commis une faute en n'utilisant pas tous les moyens nécessaires et proportionnés pour l'éviter. Il en résulte qu'en cas de violation de l'obligation légale de sécurité, la charge de la preuve échoit au créancier qui devra démontrer que le débiteur n'a pas été suffisamment prudent ou diligent dans la mise en œuvre de moyens qui auraient été nécessaires pour l'éviter. À cet égard, les deux frameworks légaux de cybersécurité prévoient que les mesures techniques et organisationnelles doivent garantir un niveau de sécurité *adapté aux risques*⁵⁴ tout en prenant en compte l'état des connaissances⁵⁵. De plus, le RGPD et

⁴⁸ Article 16, § 11, de la directive NIS.

⁴⁹ Notons néanmoins que l'article 20 de la directive NIS prévoit la possibilité de notifications volontaires.

⁵⁰ La simple conservation de données est expressément listée par l'article 4(2) du RGPD comme exemple de traitement.

⁵¹ Article 33, § 2, du RGPD.

⁵² Selon le Groupe 29, « *the contract between the controller and processor should specify how the requirements expressed in Article 33(2) should be met in addition to other provisions in the GDPR. This can include requirements for early notification by the processor that in turn support the controller's obligations to report to the supervisory authority within 72 hours* ». Groupe 29,

« Guidelines on Personal data breach notification under Regulation 2016/679 », WP250, p. 14.

⁵³ APD, « Note relative à la sécurité des données à caractère personnel », *op. cit.*, p. 8.

⁵⁴ À cet égard voy. les articles 32, § 1^{er}, du RGPD, 29, § 1^{er}, de la directive Police & Justice, 88, § 2 de la loi du 30 juillet 2018 ainsi que 14, § 1^{er} et 16, § 1^{er}, de la directive NIS.

⁵⁵ La prise en compte de l'état des connaissances doit se lire comme une obligation de « s'informer des diverses techniques de sécurité présentes sur le marché et à les évaluer à l'aune des risques décelés ». Y. POULLET, « La sécurité informatique, entre technique et droit », *Cahiers du CRID*, n° 14, 1998, p. 43. Le Conseil de l'Europe précise, quant à lui, que « les mesures de sécurité devraient prendre en considération les méthodes et techniques de pointe en matière de sécurité des données dans le cadre du traitement de données ».



les textes liés imposent de prendre en considération les coûts de mise en œuvre⁵⁶, la nature, la portée, le contexte et les finalités du traitement⁵⁷.

Outre le fait que les coûts ne sont pas expressément un facteur pour évaluer le niveau de sécurité approprié sous l'empire de la directive NIS, la référence aux risques n'a pas la même signification dans les deux cadres légaux. En effet, contrairement à la directive NIS dont la notion de risque est axée autour de l'impact négatif potentiel sur la sécurité des réseaux et des

systèmes d'information⁵⁸, le RGPD et les textes liés se placent sous l'angle du risque «pour les droits et libertés des personnes concernées»⁵⁹ afin de déterminer le niveau de sécurité approprié. Sous ces régimes, un «risque» est un scénario hypothétique qui décrit un événement redouté et toutes les menaces qui permettraient qu'il survienne, pouvant provoquer un impact sur la vie privée des personnes concernées⁶⁰. Par exemple, selon l'APD, «lorsque le traitement de données envisagé recourt au profilage ou à ce qu'on appelle les analyses "big data", le risque de traitement de données inexactes et/ou de discrimination indirecte peut augmenter. Dans de tels cas, le responsable du traitement doit recourir à des procédures mathématiques et statistiques appropriées et prendre des mesures techniques et organisationnelles qui permettent de corriger les facteurs induisant des inexactitudes dans les données à caractère personnel et de minimiser le risque d'erreurs. Le responsable du traitement doit en outre éviter que le traitement ait des conséquences discriminantes sur la base de l'origine raciale ou ethnique, des opinions politiques, de la religion ou des

Conseil de l'Europe, Projet de rapport explicatif de Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 2016, p. 11.

⁵⁶ En ce qui concerne la référence légale aux coûts, Y. Pouillet insiste sur le fait que celle-ci «ne peut se concevoir en fonction des ressources financières du responsable du traitement. Les frais doivent être suffisants et raisonnables compte tenu des précédents critères. Il serait inacceptable qu'un responsable des traitements limite la sécurité de son système d'information nonobstant les risques encourus pour les personnes concernées au seul motif que les techniques disponibles sont trop onéreuses au regard de ses ressources financières». Y. POUILLET, *op. cit.*, p. 43. L'APD va dans le même sens en estimant que «le coût des mesures envisagées ne peut pas en soi constituer une raison de réaliser un traitement sans garanties suffisantes. Si le responsable du traitement n'est pas en mesure de prévoir des garanties suffisantes et de ramener le risque à un niveau acceptable, au vu de la technologie disponible et des frais d'exécution, il doit le cas échéant soit renoncer au traitement, soit réaliser une consultation préalable de l'autorité de contrôle». APD, «Recommandation d'initiative concernant l'analyse d'impact relative à la protection des données», n° 01/2018, p. 25.

⁵⁷ Parmi les éléments pertinents pour déterminer la nature, la portée, le contexte et les finalités des traitements, l'APD cite «les catégories de personnes concernées, l'échelle du traitement de données, l'origine des données, la relation entre le responsable du traitement et les personnes concernées, les éventuelles conséquences pour les personnes concernées et le degré de facilité avec lequel on peut identifier ces dernières». Voy. APD, Recommandation n° 01/2018, *op. cit.*, p. 17.

⁵⁸ L'article 4(7) de la directive NIS définit le «risque» comme étant «toute circonstance ou tout événement raisonnablement identifiable ayant un impact négatif potentiel sur la sécurité des réseaux et des systèmes d'information».

⁵⁹ Quant à la nature des droits à prendre en compte, le Groupe 29 indique que la référence aux «droits et libertés» des personnes concernées ne renvoie pas uniquement au droit à la vie privée ou au droit à la protection des données, «mais s'entend également, le cas échéant, pour d'autres droits fondamentaux, tels que la liberté de parole, la liberté de pensée, la liberté de circulation, l'interdiction de toute discrimination, le droit à la liberté ainsi que la liberté de conscience et de religion». Groupe 29, «Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est "susceptible d'engendrer un risque élevé" aux fins du règlement (UE) 2016/679», WP248, 4 avril 2017, p. 7.

⁶⁰ CNIL, «Analyse d'impact relative à la protection des données: la méthode», mai 2018, p. 8.



convictions, de l'appartenance syndicale, du statut génétique ou de l'état de santé, ou de l'orientation sexuelle, ou ait des conséquences qui se traduisent par des mesures produisant un tel effet. Pour éviter de telles conséquences, il convient également de vérifier s'il existe une possibilité qu'un risque déterminé soit fortement susceptible de se produire chez certaines minorités ou groupes protégés»⁶¹.

Cette distinction à propos de la notion de «risque» a notamment pour conséquence que, dès lors que des données à caractère personnel sont traitées – ce qui sera presque toujours le cas dans le contexte du big data –, l'exigence d'*accountability* a pour effet de renforcer cette obligation de moyens en imposant au responsable du traitement d'être en mesure de démontrer l'efficacité des mesures *sur demande de l'autorité de contrôle*⁶². Ainsi que nous l'avons déjà rappelé, cette obliga-

tion documentaire prend notamment corps, dans le cadre du RGPD et de la directive Police & Justice, avec l'obligation du responsable du traitement de réaliser une AIPD pour les traitements «susceptibles d'engendrer un risque élevé».

La notion de «risque élevé» n'est pas définie en détail dans le RGPD⁶³ mais selon le Groupe 29, il s'agit d'évaluer le risque «inhérent»⁶⁴ afin de déterminer si le traitement de données envisagé est *susceptible d'avoir des incidences négatives sensibles* pour les libertés et droits fondamentaux des personnes physiques⁶⁵. Pour déterminer s'il est ou non probable qu'un traitement envisagé puisse donner lieu à un risque inhérent élevé, les lignes directrices élaborées par le Groupe 29 sont particulièrement importantes puisqu'elles identifient neuf critères qui doivent être pris en considération⁶⁶. Parmi ceux-ci en figurent certains qui seront souvent rencontrés dans le contexte du big data: données traitées à grande échelle, croisement

⁶¹ *Ibid.*, p. 24.

⁶² Articles 58, § 1^{er}, a), du RGPD et 47, § 1^{er}, de la directive Police & Justice. Cependant, il convient de rappeler que si le registre doit être mis à disposition de l'autorité de contrôle sur demande, il n'est par contre pas destiné aux personnes concernées ni au public en général. De même, il n'y a pas d'obligation légale de publier une AIPD. C'est le responsable du traitement qui décide lui-même de la publier ou non, quand bien même cette publication est encouragée par le Groupe 29: «La publication peut accroître la confiance dans les opérations de traitement du responsable du traitement et donner des gages de transparence. Il est notamment de bonne pratique de publier une AIPD lorsque des citoyens sont affectés par l'opération de traitement. Tel peut en particulier être le cas lorsqu'une autorité publique réalise une AIPD. L'AIPD publiée n'a pas besoin d'inclure l'intégralité de l'analyse, notamment lorsque celle-ci pourrait donner des informations spécifiques relatives à des risques en matière de sécurité concernant le responsable du traitement ou divulguer des secrets d'affaires ou des informations commercialement sensibles. Dans pareille situation, la version publiée peut consister simplement en un résumé des principales constatations de l'AIPD, ou même uniquement en une déclaration selon laquelle une AIPD a été effectuée». Groupe 29, WP248, *op. cit.*, p. 22.

⁶³ La directive Police & Justice prévoit également une obligation de réaliser une AIPD dans certaines circonstances. La présente section de cette contribution, qui s'inspire des dispositions du RGPD, s'applique *mutatis mutandis* pour l'interprétation des dispositions pertinentes de cette directive.

⁶⁴ Selon l'APD, «le risque "inhérent" renvoie à la probabilité qu'un impact négatif se produise lorsqu'aucune mesure de protection n'est prise. Le risque "résiduel" renvoie au contraire à la probabilité qu'un impact négatif se produise, malgré les mesures qui sont prises pour influencer (limiter) le risque (inhérent)». APD, Recommandation n° 01/2018, *op. cit.*, p. 20.

⁶⁵ Selon l'APD, «l'expression "susceptible de" ne signifie pas qu'il existe une lointaine possibilité d'incidence sensible. L'incidence sensible doit être plus probable qu'improbable. En revanche, cela signifie également qu'il n'est pas nécessaire que les personnes soient réellement affectées: la probabilité qu'elles soient sensiblement affectées suffit. Une «conséquence négative sensible» signifie que, dans le cas où le risque inhérent se produirait, la personne concernée serait sensiblement affectée dans l'exercice ou la jouissance de ses libertés et droits fondamentaux». *Ibid.*, p. 8.

⁶⁶ Groupe 29, WP248, *op. cit.*, pp. 10-13.



ou combinaison d'ensembles de données, évaluation ou notation (y compris activités de profilage et de prédiction). Dans le même sens, l'APD considère, par exemple, qu'une AIPD sera toujours requise «lorsqu'il est question d'un traitement à grande échelle de données générées au moyen d'appareils dotés de capteurs qui envoient des données via Internet ou via un autre moyen (applications de "l'Internet des objets" [ci-après "IoT"], comme les télévisions intelligentes, les appareils ménagers intelligents, les jouets connectés, les smart cities, les compteurs d'énergie intelligents, etc.) et que ce traitement sert à analyser ou prédire la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements de personnes physiques»⁶⁷. De même, l'APD estime qu'une AIPD doit toujours être réalisée «lorsqu'il est question de traitements de données à caractère personnel à grande échelle où le comportement de personnes physiques est observé, collecté, établi ou influencé, y compris à des fins publicitaires, et ce de manière systématique via un traitement automatisé»⁶⁸.

Lorsqu'une AIPD est requise, les principes de «privacy-by-design» et de «privacy-by-default» imposent au responsable du traitement de la réaliser *avant le traitement*⁶⁹, le cas échéant, avec l'aide du ou des sous-traitant(s) ayant l'obligation de lui fournir toutes les informations nécessaires⁷⁰. Cette analyse doit notamment contenir «une identification des

données à caractère personnel traitées, les destinataires de celles-ci, leur durée de conservation ainsi que les actifs sur lesquels elles reposent (par exemple matériels, logiciels, réseaux, personnes, etc.)»⁷¹. En matière de cybersécurité, ce premier exercice de «cartographie» s'avèrera particulièrement utile dans le contexte du big data, d'une part, afin de délimiter le périmètre et la variété des actifs à sécuriser, et, d'autre part, pour évaluer les risques du traitement considéré dans le but d'identifier les mesures techniques et organisationnelles appropriées.

IV. BIG DATA ET RISQUES TECHNIQUES

Bien que la notion de «risques» dans le cadre d'une AIPD dépasse de loin des considérations purement techniques, dans cette section nous décrivons brièvement ceux qui, du point de vue de la sécurité de l'information, engendrent soit des menaces, soit des vulnérabilités envers la confidentialité, l'intégrité ainsi que la disponibilité des données. En matière d'évaluation de ces risques, l'ISO 27005⁷² est un référentiel incontournable qui fixe un cadre et une approche pour la gestion de ceux-ci. Dans un rapport de 2016 dédié au paysage de risques dans les environnements big data, l'ENISA pointe tout d'abord un risque significatif au niveau de la disponibilité des données en avertissant que «les menaces, telles que les pannes de réseau ou les dysfonctionnements

⁶⁷ APD, Recommandation n° 01/2018, *op. cit.*, p. 43.

⁶⁸ *Ibid.*, p. 44.

⁶⁹ Selon le Groupe 29, une telle analyse est toutefois «un processus continu, en particulier lorsque l'opération de traitement est dynamique et soumise à de constants changements. La réalisation d'une AIPD relève d'un processus continu et n'est pas un exercice ponctuel». Groupe 29, WP248, *op. cit.*, p. 17.

⁷⁰ À cet effet, l'article 28, § 3, f), du RGPD impose que le contrat de sous-traitance mentionne obligatoirement cette collaboration «compte tenu de la nature du trai-

tement et des informations à la disposition du sous-traitant».

⁷¹ APD, Recommandation n° 01/2018, *op. cit.*, p. 17.

⁷² L'ISO/CEI 27005:2011 «Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information» contient des lignes directrices relatives à la gestion des risques en sécurité de l'information. Elle vient en appui des concepts généraux énoncés dans l'ISO/CEI 27001; elle est conçue pour aider à la mise en place de la sécurité de l'information basée sur une approche de gestion des risques.



de l'infrastructure de support peuvent affecter fortement les architectures big data du fait que celles-ci traitent des millions de données qui peuvent se trouver dans des emplacements physiques distincts entraînant une dépendance accrue vis-à-vis des interconnexions entre les serveurs»⁷³. De plus, au niveau de l'intégrité et de la confidentialité des données, l'ENISA identifie quatre groupes de risques inhérents à ces architectures qui peuvent être matérialisés par différentes «sources» telles que des sociétés/organisations tierces, des employés, des cybercriminels, des script kiddies ou encore des hacktivistes.

Le premier groupe de risques englobe la perte accidentelle d'informations ou d'actifs informatiques en raison d'erreurs humaines, d'une intervention involontaire, d'une utilisation erronée de l'administration de systèmes ou encore de la perte de périphériques. Celles-ci sont dues «à des erreurs de gestion et à des erreurs administratives (par exemple en appuyant sur le mauvais bouton), à une mauvaise application des règles (mauvaise gestion des correctifs, noms d'utilisateur et mots de passe par défaut ou mots de passe faciles à deviner) ou à d'autres erreurs de base (mises à jour et pannes de logiciels, problèmes d'intégration, défauts de procédure)»⁷⁴. À cet égard, une étude citée par l'agence s'étonne que «les paramètres par défaut de certaines technologies ne prévoient de configuration pour l'authentification, le chiffrement, l'auto-risation ou tout autre type de contrôle de sécurité que nous tenons pour acquis. Certains d'entre elles n'ont même pas de contrôle d'accès intégré»⁷⁵. De plus, étant donné que les

applications big data reposent sur des modèles de services Web, des fuites de données via des API insécurisées sont également à craindre⁷⁶. Enfin, «la fusion de sources de données hétérogènes augmente la redondance de la représentation des données, générant des copies mal protégées. En d'autres termes, si le stockage big data réplique dix fois les enregistrements de données et distribue les copies à dix nœuds de stockage pour une raison quelconque (par exemple, pour accélérer le pipeline d'analyse), les dix nœuds peuvent atteindre différents niveaux de sécurité (par ex. différentes versions du logiciel de sécurité), ce qui augmentera la probabilité de fuites de données»⁷⁷.

Le second groupe de risques identifié par l'agence concerne les menaces d'écoute, d'interception et de détournement de données dues aux vulnérabilités intrinsèques à ces architectures. À cet égard, le principal danger est que des acteurs malveillants puissent intercepter les communications entre les nœuds en ciblant les liens de communications. Selon l'agence, diverses sources affirment que la communication inter-nœuds dans les outils big data est souvent non sécurisée suite à l'absence, par défaut, de protocoles garantissant la confidentialité et l'intégrité des données entre les applications communicantes (TLS et SSL, par exemple)⁷⁸.

Le troisième type de risques à prendre en considération sont les attaques malveillantes élaborées et spécialisées pour exploiter les faiblesses des applications big data. Ainsi, ces

⁷³ ENISA, «Big data Threat Landscape and Good Practice Guide», *op. cit.*, p. 18.

⁷⁴ ENISA, «Big data Threat Landscape and Good Practice Guide», *op. cit.*, p. 19.

⁷⁵ Voy. l'étude de BinaryEdge réalisée en 2015 à propos de Redis, «MongoDB, Memcache, and Elasticsearch», disponible à l'adresse [https://blog.binaryedge.](https://blog.binaryedge.io/2015/08/10/data-technologies-and-security-part-1/)

[io/2015/08/10/data-technologies-and-security-part-1/](https://blog.binaryedge.io/2015/08/10/data-technologies-and-security-part-1/).

⁷⁶ Voy. l'étude de Securosis réalisée en 2012 et intitulée «Securing big data: Security Recommendations for Hadoop and NoSQL Environments», disponible à l'adresse https://securosis.com/assets/library/reports/SecuringBigData_FINAL.pdf.

⁷⁷ ENISA, «Big data Threat Landscape and Good Practice Guide», *op. cit.*, p. 21.

⁷⁸ *Ibid.*, p. 22.



systèmes seront plus probablement la cible d'attaques visant le vol d'identité puisque souvent ces architectures stockent et gèrent non seulement des informations d'identification mais également des données de profilage pouvant décrire en détail le comportement, les préférences, les habitudes ou encore les déplacements d'individus pouvant aider les cybercriminels à élaborer des formes plus élaborées d'usurpation ou de fraude. Dans ce contexte, le *social engineering*⁷⁹ est également un vecteur d'attaques à prendre en considération. L'agence énumère d'autres exemples de menaces – parmi lesquelles des kits d'exploitation qui permettent des infections par des virus et des logiciels malveillants; des vers qui peuvent être distribués en utilisant le réseau pour envoyer des copies à d'autres nœuds; des chevaux de Troie qui facilitent l'accès non autorisé; des backdoors qui sont des points d'entrée non documentés dans un programme informatique généralement insérés par un programmeur pour permettre un accès à distance au programme; des attaques par injection de code, etc. – dont les effets sont multipliés dans le contexte du big data puisqu'après le déploiement du code, l'attaquant peut manipuler les périphériques infectés, envoyer des commandes ciblées à d'autres serveurs et perturber ou manipuler leurs opérations⁸⁰. En outre, l'ENISA signale que la signature de périphériques et le chiffrement des médias peuvent être gravement compromis par l'uti-

lisation de certificats non autorisés permettant aux attaquants d'accéder aux ressources big data et aux liens de communications. De même, il s'agit de prendre en considération le risque de divulgation d'identifiants d'accès utilisés lors d'audits et par conséquent leur abus dès lors que l'étendue et la granularité de ces audits sont évidemment amplifiés dans un contexte big data⁸¹.

Le dernier ensemble de risques identifiés par l'ENISA renvoie à l'anonymisation inadéquate de données à caractère personnel. Même lorsque des techniques d'anonymisation sont utilisées, les utilisateurs individuels peuvent être réidentifiés en exploitant d'autres ensembles de données disponibles, par exemple, dans le domaine public. Il s'agit d'un phénomène inhérent au big data qui a la capacité d'individualiser des personnes physiques à partir de jeux de données anonymisés en corrélation avec des informations publiques apparemment inoffensives. Ce phénomène a par ailleurs été largement étudié par l'APD dans le cadre de son rapport relatif au big data⁸².

Au-delà de ces quatre groupes de risques liés notamment à la masse de données traitées mais aussi «au niveau élevé de réplication (stockage distribué) et à l'externalisation fréquente des traitements»⁸³, l'ENISA considère que les différents acteurs de la chaîne de traitement big data – «propriétaires de données, transformateurs de données, opérateurs de traitements et fournisseurs de services de stockage»⁸⁴ – sont susceptibles d'avoir des intérêts divergents, voire en conflit les uns avec les autres. Le tout aboutissant à «un écosystème complexe où les contre-mesures de sécurité

⁷⁹ Le social engineering est une technique qui a pour but d'extirper des informations à des personnes sans qu'elles ne s'en rendent compte. Contrairement aux autres attaques, elle ne nécessite pas de logiciel. La seule force de persuasion est la clé de voûte de cette attaque. Il y a quatre grandes méthodes de social engineering : par téléphone, par lettre, par internet et par contact direct. L'article suivant illustre cette notion de manière succincte <https://www.securiteinfo.com/attaques/divers/social.shtml>.

⁸⁰ ENISA, «Big data Threat Landscape and Good Practice Guide», *op. cit.*, p. 24.

⁸¹ *Ibid.*, p. 25.

⁸² APD, «Rapport big data», *op. cit.*

⁸³ ENISA, «Big data Threat Landscape and Good Practice Guide», *op. cit.*, p. 4.

⁸⁴ *Ibidem.*



doivent être précautionneusement planifiées et mises en place»⁸⁵.

V. BIG DATA ET MESURES DE SÉCURITÉ

À titre liminaire, rappelons que – contrairement à la directive NIS – le RGPD et les textes liés ne s'appliquent pas au traitement de données anonymes, à savoir «les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable»⁸⁶. Toutefois, le processus d'anonymisation en lui-même constitue un traitement de données à caractère personnel; et à ce titre, il est soumis aux exigences de ces législations jusqu'au moment où les données sont effectivement rendues anonymes⁸⁷. Les principales techniques d'anonymisation, telles que l'agrégation, la randomisation et la généralisation ont été décrites par le Groupe 29⁸⁸. Dans le contexte du big data, certains argumentent parfois que ces techniques d'anonymisation peuvent être utilisées afin de réduire ou même d'exclure le risque d'individualisation (*singling out*) ou de ré-identification. Toutefois, «lorsque le résultat de l'anonymisation est ensuite utilisé à l'égard de personne (par exemple lors de l'utilisation de corrélations – les corrélations peuvent être considérées comme une forme d'informations résumées ou agrégées), il y a (à nouveau) un (autre) traitement de données à caractère personnel. La législation relative à la protection des données s'appliquera à nouveau dans ce cas, même s'il est (partiellement) question de l'utilisation de données anonymes ou agrégées»⁸⁹. Par conséquent,

à défaut d'être absolument certains d'avoir à faire à des données réellement anonymes, nous recommandons aux débiteurs de l'obligation de sécurité de les considérer comme restant «à caractère personnel».

De manière générale, lorsque des données à caractère personnel sont traitées, les mesures de sécurité appropriées incluent, selon l'APD, la rédaction d'une politique de sécurité de l'information, l'organisation des aspects humains – en ce compris la désignation d'un délégué à la protection des données lorsque cela est requis⁹⁰ –, la gestion de la sécurité physique et de l'environnement, la sécurité applicative, la sécurisation des réseaux, la sécurisation logique des accès, la journalisation, le traçage et l'analyse des accès ainsi que la gestion des incidents de sécurité et de la continuité; ces mesures devant être documentées, implémentées, auditées et améliorées aussi souvent que nécessaire⁹¹. Dans les sections suivantes, sans souhait d'exhaustivité, nous examinons brièvement certaines de ces mesures qui nous paraissent particulièrement importantes dans le contexte du big data.

A. Politique de sécurité, sous-traitance et sous-traitance de second rang

Pour tout organisme traitant des données, une première étape de sécurisation consiste à «rédiger un document écrit – la politique de sécurité de l'information – précisant les stratégies et mesures retenues pour sécuriser ces

⁸⁵ *Ibidem*.

⁸⁶ Considérant 26 du RGPD.

⁸⁷ Groupe 29, Avis 05/2014 sur les techniques d'anonymisation, WP216, adopté le 10 avril 2014, p. 3.

⁸⁸ *Ibidem*.

⁸⁹ APD, «Rapport big data», *op. cit.*, p. 21.

⁹⁰ Article 37 du RGPD. Voy. également Groupe 29, «Lignes directrices concernant les délégués à la protection des données», WP243, 5 avril 2017.

⁹¹ APD, «Mesures de référence applicables à tout traitement de données à caractère personnel – version 1.0, disponible à l'adresse https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/mesures_de_reference_en_matiere_de_securite_applicables_a_tout_traitement_de_donnees_a_caractere_personnel_0.pdf.



données»⁹². Or, dans le contexte des mégadonnées, il est souvent question d'un grand nombre d'acteurs, ce qui rend l'attribution des responsabilités en matière de cybersécurité évidemment plus complexe. En cas de sous-traitance, l'organisation doit notamment veiller au respect des règles et politiques de sécurité applicables au traitement de l'information par son (ses) sous-traitant(s), tout en clarifiant les rôles et responsabilités de chaque intervenant⁹³. Nous avons déjà souligné que, sous le régime du RGPD, le responsable du traitement et le sous-traitant sont tous deux débiteurs de l'obligation de sécurité. Par conséquent, en cas de manquement, leur responsabilité solidaire pourra être éventuellement engagée conformément aux articles 82 et 83 du règlement. Sur le plan administratif, la répartition des éventuelles amendes⁹⁴ dépendra notamment de leur degré de responsabilité respectif dans la violation de l'obligation, compte tenu des mesures techniques et organisationnelles qu'ils ont chacun mises en œuvre⁹⁵. Sur le plan civil, la personne lésée pourra, au choix, demander réparation du préjudice subi à l'un ou à l'autre⁹⁶, lequel pourra ensuite se retourner contre le partenaire contractuel en ce qui concerne sa part de responsabilité dans le dommage⁹⁷. À cet égard, le contrat de sous-traitance doit notamment obligatoirement prévoir que le sous-traitant aide le responsable du traitement à garantir le respect de l'obliga-

tion de sécurité⁹⁸ et qu'il mette à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect de son obligation de sécurité, ainsi que pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et qu'il contribue à ces audits⁹⁹.

Non seulement plusieurs parties peuvent intervenir en tant que sous-traitants mais il est également habituel que des sous-traitants confient des activités à des sous-traitants de second rang. Dans ce cas, le RGPD prévoit que le sous-traitant ne peut pas recruter un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement¹⁰⁰. De plus, le contrat régissant les relations entre le sous-traitant et le sous-traitant de second rang doit contenir les mêmes obligations en matière de protection de données que celles fixées dans le contrat entre le responsable du traitement et le sous-traitant, en particulier pour ce qui est de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées¹⁰¹. Lorsque cet autre sous-traitant ne remplit pas ses obligations en matière de protection des données, le sous-traitant principal demeure pleinement responsable devant le responsable du traitement de l'exécution par l'autre sous-traitant de ses obligations¹⁰².

⁹² *Ibid.*, p. 2.

⁹³ *Ibid.*, p. 6.

⁹⁴ En Belgique, l'article 221, § 2, de la loi du 30 juillet 2018 précitée prévoit, en principe, l'absence d'amendes administratives pour les autorités publiques. Il se lit comme suit: «l'article 83 du Règlement ne s'applique pas aux autorités publiques et leurs préposés ou mandataires sauf s'il s'agit de personnes morales de droit public qui offrent des biens ou des services sur un marché».

⁹⁵ Article 83, § 2, d), du RGPD.

⁹⁶ Article 82, § 1^{er}, du RGPD.

⁹⁷ Article 82, § 5, du RGPD.

⁹⁸ Article 28 § 3, f), du RGPD.

⁹⁹ Article 28, § 3, f) et h), du RGPD.

¹⁰⁰ Article 28, § 2, du RGPD. Dans le cas d'une autorisation écrite générale, le sous-traitant informe le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements.

¹⁰¹ Article 28, § 4, du RGPD.

¹⁰² *Ibidem*.



Autant dire qu'en cas de sous-traitance ou de sous-traitance de second rang, des dispositions conventionnelles détaillées en matière de sécurité sont d'une importance cruciale pour assurer à l'un ou l'autre acteur la possibilité de prouver que le fait qui a provoqué le dommage lui est partiellement ou nullement imputable et ainsi être exonéré de responsabilité, en tout ou en partie. En effet, dans les contrats de sous-traitance, le principe de convention-loi ne s'oppose pas à ce que ceux-ci contiennent des obligations additionnelles de *résultat* en matière de sécurité informationnelle (par exemple en matière de contrôle des accès physiques et logiques, de journalisation, de techniques cryptographiques spécifiques, d'interdiction du BYOD¹⁰³, etc.). Ces contrats peuvent également exiger l'adhésion à des codes de conduite ou une certification par un tiers indépendant.

B. Certifications en cascade

L'ENISA considère que le respect de codes de conduites et la certification de tous les intervenants peuvent fortement contribuer à assurer l'interopérabilité entre les applications, tout en garantissant que la sécurité soit maintenue à niveau requis à tous les maillons de la chaîne¹⁰⁴. L'article 32, § 3, du RGPD stipule quant à lui que «l'application d'un code de conduite approuvé [...] ou d'un mécanisme de certification approuvé [...] peut servir d'élément pour démontrer le respect des exigences prévues [en matière de sécurité]». Sans entrer dans

le détail de cette disposition¹⁰⁵, un code de conduite essentiel est la norme ISO/CEI 27002, laquelle est une sorte de boîte à outils proposant un ensemble de 114 mesures de sécurité aussi bien techniques qu'organisationnelles qui permettent de traiter les risques identifiés. Les organisations qui adoptent l'ISO/CEI 27002 doivent évaluer leurs propres risques de sécurité de l'information et appliquer les contrôles appropriés en utilisant la norme pour orienter l'organisme. Outre le respect d'un code de conduite, une certification d'un sous-traitant ou d'un sous-traitant de second rang par un tiers indépendant agréé par l'organisme national de certification¹⁰⁶ peut offrir un moyen fiable pour ceux-ci de convaincre du respect de leurs obligations et de gagner la confiance de responsables du traitement (et vice-versa). Une certification indique au moins que les mesures en matière de sécurité de l'information ont été soumises à un audit indépendant à l'égard d'un certain nombre de critères. D'éventuelles certifications pertinentes en la matière sont notamment celles réalisées sur la base des normes ISO/IEC 27001 et ISO/IEC 27018¹⁰⁷.

¹⁰³ Le Bring Your Own Device est une pratique consistant à autoriser les employés à utiliser, dans un contexte professionnel, leurs propres terminaux personnels. Les smartphones en sont l'exemple le plus commun, mais le BYOD peut également recouvrir les tablettes, les ordinateurs portables, ou encore les clés USB. Groupe 29, Avis 2/2017 sur le traitement des données sur le lieu de travail, WP249, 8 juin 2017, p. 16.

¹⁰⁴ ENISA, «Big data Security Good Practices and Recommendations on the Security of big data Systems», *op. cit.*, p. 21.

¹⁰⁵ À cet égard, nous renvoyons à EDPB, «Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679», mai 2018 ainsi qu'à ENISA, «Recommendations on European Data Protection Certification», version 1.0, novembre 2017, disponible à l'adresse https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification/at_download/fullReport.

¹⁰⁶ En droit belge, BELAC est l'organisme national d'accréditation désigné conformément au règlement (CE) 765/2008 du Parlement européen et du Conseil, conformément à la norme EN-ISO/IEC 17065/2012 et aux exigences supplémentaires établies par l'autorité de contrôle en vertu de l'article 55 ou 56 du RGPD.

¹⁰⁷ La norme ISO/CEI 27018 concerne la protection des données à caractère personnel dans l'informatique en nuages. Elle a été publiée en août 2014 par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI) sous le titre en français: «Technologies de l'information, Techniques de sécurité – Code de bonnes



C. Architecture, sécurisation des réseaux et chiffrement

En cas d'interconnexion, tout organisme doit «s'assurer que les réseaux auxquels sont connectés les équipements impliqués dans le traitement des données à caractère personnel garantissent la confidentialité et l'intégrité de celles-ci»¹⁰⁸. Dans une version minimale, l'APD recommande de séparer le réseau local des machines accessibles depuis Internet, par exemple en mettant en œuvre une DMZ¹⁰⁹. Un système permettant le filtrage des flux entre ces zones doit être implémenté et ses alertes doivent être suivies et traitées dans des délais raisonnables grâce à un système de détection (et de prévention) d'intrusion («IDS/IPS») permettant de repérer des activités anormales ou suspectes. L'ENISA ajoute qu'il importe de concevoir les bases de données en application du principe de pseudonymisation¹¹⁰ de telle manière que les données considérées comme «sensibles» puissent être contenues dans des

champs séparés afin qu'elles puissent être facilement filtrées et/ou cryptées¹¹¹ lorsqu'elles sont transmises. En effet, selon le principe de *Self Protecting CIS*¹¹², chaque système devrait considérer tous les autres systèmes extérieurs comme étant non sécurisés et par conséquent, prendre les mesures nécessaires pour s'en protéger. Dans ce contexte, il va de soi que le chiffrement est une mesure d'atténuation clé pour garantir que seules les personnes et entités autorisées aient accès aux données¹¹³. Pour cette raison, l'ENISA recommande, dans la mesure du possible, de chiffrer les données tant au repos qu'en transit¹¹⁴ et de se munir d'une solution de gestion de clés de chiffrement appropriée, en tenant compte du grand nombre de périphériques à couvrir. Toutefois, dans la pratique, l'agence relève que dans le contexte de l'IoT, il est fréquent qu'aucun chiffrement ne soit utilisé pour le transport des données, car tous les appareils connectés n'offrent pas de telles capacités¹¹⁵. Une telle mesure est pourtant dans l'intérêt du responsable du traitement qui, en rendant les données incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, est dispensé

pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII». La norme constitue un complément aux mesures telles que définies dans la norme ISO/IEC 27002 afin de tenir compte de la nature répartie des risques et de l'existence de la relation contractuelle entre le client de services cloud et le Cloud Service Provider.

¹⁰⁸ APD, «Mesures de référence», *op. cit.*, p. 4.

¹⁰⁹ APD, «Recommandation d'initiative n° 01/2013 relative aux mesures de sécurité à respecter afin de prévenir les fuites de données», 21 janvier 2013, p. 4, disponible à l'adresse https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2013.pdf.

¹¹⁰ La «pseudonymisation» est définie par l'article 4, 5), du RGPD comme étant «le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable».

¹¹¹ ENISA, «Big data Security Good Practices and Recommendations on the Security of big data Systems», *op. cit.*, p. 20.

¹¹² CIS signifie «Communication and Information System». À l'origine, le principe du self protecting CIS provient de l'OTAN mais il peut être applicable pour toute interconnexion. Voy. OTAN, Security Committee, Primary Directive on CIS Security, AC/35-D/2004-REV3, 15 novembre 2013.

¹¹³ Pour rappel, l'article 48 de la loi du 13 juin 2005 relative aux communications électroniques dispose que «l'emploi de la cryptographie est libre».

¹¹⁴ Dans certaines situations assez courantes, il peut se trouver des canaux de communication qui ne sont par essence pas chiffrés (le protocole Telnet pour la gestion distante de systèmes par le service informatique ou encore le protocole HTTP couramment utilisé dans les navigateurs pour les pages Web).

¹¹⁵ ENISA, «Big data Security Good Practices and Recommendations on the Security of big data Systems», *op. cit.*, p. 20.



de son obligation de communiquer une violation de telles données aux personnes concernées¹¹⁶ et est par conséquent davantage à l'abri d'une perte de confiance de celles-ci.

D. Classification, séparation des rôles et sécurisation logique des accès

Afin d'assurer la confidentialité, l'intégrité et la disponibilité des données, tout organisme «doit s'assurer que [celles-ci] ne soient accessibles, conformément à leur classification, qu'aux personnes et aux applications qui en ont explicitement l'autorisation»¹¹⁷. En premier lieu, il importe donc de mettre en place des procédures de classification de l'information permettant d'inventorier et de localiser toutes les données à caractère personnel traitées, et ce quel qu'en soit le support, ainsi que de maintenir à jour une liste actualisée des différentes personnes habilitées à accéder et traiter ces données et de leurs pouvoirs respectifs (création, consultation, modification, destruction). Ce principe (plus communément nommé sous son acronyme anglais, *SoD*, c'est-à-dire *Segregation of Duties*) consiste à compartimenter les responsabilités des différents acteurs en leur assignant des rôles permettant de définir *qui peut faire quoi* ou encore *qui a accès à quoi*. Assez fortement liée au principe précédent, la limitation des privilèges consiste à limiter les droits selon les différents rôles. En effet, trop de privilèges sur les systèmes d'information peuvent conduire à des fraudes ou à des erreurs. En matière de rôles et de privilèges, en particulier pour le personnel du service informatique, il est également important de toujours distinguer l'utilisation normale de l'administration des systèmes¹¹⁸. Afin d'assurer

le respect de ces règles, l'APD recommande de compléter l'identification des intervenants par une procédure d'authentification¹¹⁹. La CNIL¹²⁰ va dans le même sens en affirmant que «pour assurer qu'un utilisateur accède uniquement aux données dont il a besoin, il doit être doté d'un identifiant qui lui est propre et doit s'authentifier avant toute utilisation des moyens informatiques»¹²¹.

Selon l'ENISA, le respect de ces différents préceptes est un défi majeur dans le contexte du big data qui consiste à collecter une grande diversité de données (allant de structurées à semi-structurées et non structurées) ayant différents niveaux de confidentialité et provenant de nombreuses sources. De plus, avec les nouvelles technologies telles que l'IoT, des appareils et des capteurs ayant besoin d'accéder aux données ne disposent pas toujours de la puissance de traitement ni de la capacité nécessaire pour offrir des contrôles d'accès avancés. À cet égard, afin de valider et de filtrer efficacement les sources, l'agence indique qu'une des mesures d'atténuation consiste à utiliser uniquement des périphériques pouvant fournir le niveau d'authentification requis, et, lorsque cela n'est pas possible, d'avoir recours à des processus solides de test des équipements ainsi que de suivi et de maintenance de

et un compte administrateur (avec tous les privilèges pour modifier le système). Il travaille sur son compte administrateur et décide d'ouvrir son navigateur afin d'aller regarder ses derniers mails, tout en ne se connectant pas au préalable sous son compte d'utilisateur normal afin de gagner du temps. Il ouvre une pièce jointe infectée et, étant dans une session sous un compte qui a tous les privilèges, le logiciel malicieux contenu dans la pièce jointe s'installe et infecte le système.

¹¹⁹ APD, «Mesures de référence», *op. cit.*, p. 4.

¹²⁰ La CNIL est l'autorité de protection des données en France.

¹²¹ CNIL, «La sécurité des données personnelles», *Les guides de la CNIL*, édition 2017, p. 7, disponible à l'adresse https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf.

¹¹⁶ Article 34, § 3, a), du RGPD.

¹¹⁷ APD, «Mesures de référence», *op. cit.*, p. 4.

¹¹⁸ Un exemple d'erreur humaine typique est celui d'un administrateur ayant bien deux comptes différents sur sa station de travail : un compte d'utilisateur normal (non privilégié, ne pouvant pas installer d'application)



l'inventaire du système¹²². Test, suivi et maintenance restent par ailleurs des mesures fondamentales, le problème du manque de mise à jour des systèmes étant encore toujours très fréquent et permettant à des attaques d'exploiter des failles non corrigées alors même que des correctifs sont disponibles. Bien que des systèmes opératoires tels que Windows ou des applications disposent de mécanismes capables d'automatiser les mises à jour, il en est encore souvent qui ne sont pas configurés correctement et dont les mises à jour ne se font pas régulièrement voire simplement pas du tout¹²³.

E. Journalisation, traçage et analyse des accès

Traditionnellement, il importe de rappeler que les trois critères de sécurité classiques (intégrité, confidentialité, disponibilité) sont compris comme étant des «finalités de base auxquelles s'ajoutent des fonctions de sécurité qui contribuent à confirmer d'une part la véracité, l'authenticité d'une action, entité ou ressource (notion d'authentification) et, d'autre part, l'existence d'une action (notion de non-répudiation d'une transaction, voire d'imputabilité)»¹²⁴. L'APD va dans le même sens en affirmant que «dans le contexte normatif, la sécurité de l'information recouvre par définition l'obtention et la conservation de la confidentialité, de l'intégrité, de la disponibilité, de l'imputabilité, de l'authenticité, de la fiabilité et de la non-répudiation de l'information et

des équipements de traitement de l'information»¹²⁵. De plus, il découle d'éclaircissements jurisprudentiels intéressants sur la portée du principe de sécurité «que les mesures de sécurité doivent non seulement empêcher les accès non autorisés [et accidentels] mais également permettre aux personnes concernées de contrôler les accès aux données qui ont eu lieu. Seul cet accès aux données sur les personnes ayant accédé aux données permet en effet à la personne concernée de vérifier l'effectivité des mesures de sécurité et lui permet d'exercer son contrôle ou sa maîtrise sur ses propres informations»¹²⁶. Dans la même ligne, la Cour de justice de l'Union européenne a rappelé dans son arrêt *Rijkeboer*¹²⁷ que pour assurer un effet

¹²⁵ APD, «Note relative à la sécurité des données à caractère personnel», *op. cit.*, p. 1.

¹²⁶ Ainsi que C. de Terwangne le souligne, c'est en ce sens qu'a jugé la Cour européenne des droits de l'homme dans l'affaire *I c. Finlande*, condamnant cet État pour avoir laissé un hôpital public mettre en place un système de sécurité des données qui ne conserve en mémoire que les traces des cinq derniers accès aux données et qui, de surcroît efface toute trace d'accès une fois les données versées aux archives. Dans le cas d'espèce, la Cour avait estimé que ce qui était requis en premier lieu est une protection réelle et effective qui exclut toute possibilité d'accès non autorisé afin d'obtenir une indemnisation pour le dommage causé par une divulgation non autorisée de données à caractère personnel. C. DE TERWANGNE, «La réforme de la convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel», in *Quelle protection des données personnelles en Europe?*, Bruxelles, Larcier, 2015, p. 113.

¹²⁷ C.J.U.E., 7 mai 2009, *College van burgemeester en wethouders van Rotterdam c. M. E.E. Rijkeboer*, C-553/07 «Dans cette affaire, M. Rijkeboer avait demandé au Collège de Rotterdam de l'informer de tous les cas où des informations le concernant et provenant de l'administration communale avaient été communiquées à des personnes tierces au cours des deux années précédant sa demande. Il désirait connaître l'identité de ces personnes et le contenu de l'information qui leur avait été transmise. Il avait déménagé dans une autre commune et souhaitait savoir, en particulier, à qui son ancienne adresse avait été communiquée. Il n'a reçu de réponse que pour l'année précédant sa demande, les données antérieures ayant été auto-

¹²² ENISA, «Big data Security Good Practices and Recommendations on the Security of big data Systems», *op. cit.*, pp. 20-23.

¹²³ Comme exemple de conséquence d'une mauvaise application des mises à jour, on mentionnera Wanna-Crypt, un rançongiciel réputé avoir touché près de 100.000 systèmes à travers le globe et dont la propagation a été possible parce qu'il exploitait une faille non mise à jour sur ces systèmes.

¹²⁴ S. GHERNAOUTI, *Sécurité informatique et réseaux*, Dunod, 2013, p. 1.



utile, le droit d'accès concerne nécessairement le passé: « cela implique l'obligation de conservation pendant une certaine durée des renseignements relatifs aux personnes destinataires des données ainsi qu'aux données précisément consultées ou transmises »¹²⁸.

Ces fonctions d'*authenticité*, d'*imputabilité* et de *non-répudiation* sont d'ailleurs implémentées dans le cadre de la directive Police & Justice, l'article 29, § 2 de celle-ci prévoyant que le responsable du traitement ou le sous-traitant met en œuvre, à la suite d'une évaluation des risques, des mesures destinées au contrôle de l'accès aux installations, au contrôle des supports de données, au contrôle de la conservation, au contrôle des utilisateurs, au contrôle de l'accès aux données, au contrôle de la transmission, au contrôle de l'introduction et au contrôle du transport. De plus, l'article 25 de ladite directive régule spécifiquement la journalisation en prévoyant que « les États membres prévoient que des journaux sont établis au moins pour les opérations de traitement suivantes dans des systèmes de traitement automatisé: la collecte, la modification, la consultation, la communication, y compris les transferts, l'interconnexion et l'effacement. Les journaux des opérations de consultation et de communication permettent d'établir le motif, la date et l'heure de celles-ci et, dans la mesure du possible, l'identification de la personne qui a consulté ou communiqué les données à caractère personnel, ainsi que l'identité des destinataires de ces données à caractère personnel »¹²⁹. De manière

analogue, en ce qui concerne l'utilisation des données à caractère personnel par les institutions et organes de l'UE, l'article 22 du règlement 45/2001¹³⁰ prévoit que des mesures sont prises lorsqu'elles sont nécessaires au regard des risques encourus et énumère le même type de mesures de contrôle¹³¹.

Il est dès lors particulièrement étonnant de relever que ni le RGPD ni la directive NIS n'imposent explicitement des mesures de contrôle

fins de procédures pénales». Le paragraphe 3 dudit article précise, quant à lui, que « le responsable du traitement et le sous-traitant mettent les journaux à la disposition de l'autorité de contrôle, sur demande ».

¹³⁰ Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

¹³¹ Telles des mesures prises « dans le but: a) d'empêcher toute personne non autorisée d'avoir accès aux systèmes informatiques de traitement des données à caractère personnel; b) d'empêcher que des supports de stockage puissent être lus, copiés, modifiés ou déplacés sans autorisation; c) d'empêcher toute introduction non autorisée de données dans la mémoire ainsi que toute divulgation, toute modification ou tout effacement non autorisés de données à caractère personnel mémorisées; d) d'empêcher des personnes non autorisées d'utiliser des systèmes de traitement de données au moyen d'installations de transmission de données; e) de garantir que les utilisateurs autorisés d'un système de traitement des données ne puissent accéder qu'aux données à caractère personnel que leur droit d'accès leur permet de consulter; f) de garder une trace des données à caractère personnel qui ont été communiquées, du moment où elles l'ont été et de leur destinataire; g) de garantir qu'il sera possible de vérifier *a posteriori* quelles données à caractère personnel ont été traitées, à quel moment et par quelles personnes; h) de garantir que des données personnelles qui sont traitées pour le compte de tiers ne peuvent l'être que de la façon prévue par l'institution ou l'organe contractant; i) de garantir que, lors de la communication de données à caractère personnel et du transport de supports de stockage, les données ne puissent être lues, copiées ou effacées sans autorisation; j) de concevoir la structure organisationnelle interne d'une institution ou d'un organe de manière à ce qu'elle réponde aux exigences propres à la protection des données ».

matiquement effacées conformément à la loi des Pays-Bas relative aux données personnelles détenues par les administrations communales». Voy. J. HERVEG, « L'accès du patient aux log files de son dossier informatisé », *D.C.C.R.*, 2011, liv. 90 p. 49.

¹²⁸ C. DE TERWANGNE, *op. cit.*

¹²⁹ Pour le surplus, l'article 25, § 2, de la directive Police & Justice précise que « les journaux sont utilisés uniquement à des fins de vérification de la licéité du traitement, d'autocontrôle, de garantie de l'intégrité et de la sécurité des données à caractère personnel et à des



d'accès, d'authentification et de journalisation à leurs débiteurs. Cela dit, selon le Comité européen de la protection des données, «*logging in considered required as part of the security obligation of controllers (article 32), as well as the obligation and in order to be able to demonstrate compliance with the GDPR (accountability) (article 5(2))*»¹³². L'APD va dans le même sens en recommandant à tous les débiteurs de l'obligation de sécurité de mettre en œuvre des mécanismes «qui doivent permettre de retrouver, en cas de nécessité, l'identité de l'auteur de tout accès aux données à caractère personnel ou de toute manipulation de celles-ci. L'enregistrement de ces informations de contrôle peut concerner, suivant les cas, l'accès physique, l'accès logique ou les deux»¹³³. Paradoxalement, afin de garantir la protection des données à caractère personnel, l'obligation de sécurité aurait donc pour conséquence d'imposer un traitement de données à caractère personnel additionnel ou accessoire ayant pour finalité l'imputabilité des actions réalisées sur les traitements initiaux. Les logs étant eux-mêmes des données à caractère personnel, l'APD considère que la «granularité des enregistrements, la localisation et la durée de conservation de ceux-ci, la fréquence et le type des manipulations effectuées sur ceux-ci dépendent du contexte»¹³⁴. La CNIL adopte le même type de recommandation en estimant qu'«afin de pouvoir identifier un accès frauduleux ou une utilisation abusive de données personnelles, ou de déterminer l'origine d'un incident, il convient d'enregistrer certaines des actions effectuées sur les systèmes informatiques. Pour ce faire, un dispositif de gestion des traces et des incidents doit être mis en place. Celui-ci doit enregistrer les événements

pertinents et garantir que ces enregistrements ne peuvent être altérés. Dans tous les cas, il ne faut pas conserver ces éléments pendant une durée excessive»¹³⁵. Dans le même document, la CNIL énumère les précautions nécessaires à prendre en compte lors de la mise en œuvre de la journalisation¹³⁶. Enfin, il s'agit de ne pas confondre la finalité de journalisation avec celle de la surveillance des employés en utilisant, par exemple, les logs pour évaluer leur rentabilité. Une telle autre finalité poserait en effet la délicate question de «l'équilibre entre l'intérêt légitime de l'employeur à protéger ses activités et les attentes raisonnables des

¹³⁵ CNIL, «La sécurité des données personnelles», *op. cit.*, p. 10.

¹³⁶ *Ibidem*. Selon la CNIL, «il s'agit de «prévoir un système de journalisation (c'est-à-dire un enregistrement dans des "fichiers journaux" ou "logs") des activités des utilisateurs, des anomalies et des événements liés à la sécurité : ces journaux doivent conserver les événements sur une période glissante ne pouvant excéder six mois (sauf obligation légale, ou risque particulièrement important) ; la journalisation doit concerner, au minimum, les accès des utilisateurs en incluant leur identifiant, la date et l'heure de leur connexion, et la date et l'heure de leur déconnexion ; dans certains cas, il peut être nécessaire de conserver également le détail des actions effectuées par l'utilisateur, les types de données consultées et la référence de l'enregistrement concerné. Il faut informer les utilisateurs de la mise en place d'un tel système, après information et consultation des représentants du personnel ; protéger les équipements de journalisation et les informations journalisées contre les accès non autorisés, notamment en les rendant inaccessibles aux personnes dont l'activité est journalisée ; établir des procédures détaillant la surveillance de l'utilisation du traitement et examiner périodiquement les journaux d'événements pour y détecter d'éventuelles anomalies ; assurer que les gestionnaires du dispositif de gestion des traces notifient, dans les plus brefs délais, toute anomalie ou tout incident de sécurité au responsable de traitement ; et enfin notifier toute violation de données à caractère personnel à la CNIL et, sauf exception prévue par le RGPD, aux personnes concernées pour qu'elles puissent en limiter les conséquences».

¹³² EDPB, «Letter to ICANN», 5 juillet 2018, p. 5, disponible à l'adresse https://edpb.europa.eu/sites/edpb/files/files/file1/icann_letter_en.pdf.

¹³³ APD, «Mesures de référence», *op. cit.*, p. 4.

¹³⁴ *Ibidem*.



personnes concernées, à savoir les employés, en matière de respect de la vie privée»¹³⁷.

Pour ce qui concerne le fondement de licéité de la journalisation, le considérant 49 du RGPD indique que «le traitement de données à caractère personnel dans la mesure strictement nécessaire et proportionnée aux fins de garantir la sécurité du réseau et des informations [...] constitue un intérêt légitime du responsable du traitement concerné». La notion de «sécurité du réseau et des informations» y est par ailleurs définie comme étant «la capacité d'un réseau ou d'un système d'information de résister, à un niveau de confiance donné, à des événements accidentels ou à des actions illégales ou malveillantes qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité de données à caractère personnel conservées ou transmises». Sont également considérés comme relevant de l'intérêt légitime, «la sécurité des services connexes offerts ou rendus accessibles via ces réseaux et systèmes, par des autorités publiques, des équipes d'intervention en cas d'urgence informatique (CERT), des équipes d'intervention en cas d'incidents de sécurité informatique (CSIRT), des fournisseurs de

réseaux et de services de communications électroniques et des fournisseurs de technologies et services de sécurité». L'objectif serait, entre autres, «d'empêcher l'accès non autorisé à des réseaux de communications électroniques et la distribution de codes malveillants, et de faire cesser des attaques par DDoS et des dommages touchant les systèmes de communications informatiques et électroniques»¹³⁸.

Selon l'ENISA, la journalisation n'est toutefois pas à prendre à la légère dans le contexte du big data où le «grand volume de transactions effectuées a pour conséquence que les journaux eux-mêmes deviennent trop nombreux. Une mesure d'atténuation consiste à ne conserver que certains journaux requis. Une autre consiste à stocker les journaux compressés et à utiliser uniquement les métadonnées extraites de ceux-ci. Si nécessaire, seuls les journaux requis peuvent être décompressés et utilisés»¹³⁹. Du point de vue de la protection de la vie privée, cette dernière recommandation permettra aux débiteurs de

¹³⁷ Groupe 29, WP249, *op. cit.*, p. 4. Voy. aussi Cour eur. D.H., 3 avril 2007, *Copland c. Royaume-Uni*, req. n° 62617/00. Dans cette affaire, la Cour a déclaré que les courriers électroniques envoyés à partir de locaux professionnels et les informations découlant de la surveillance de l'utilisation de l'internet pouvaient faire partie de la vie privée et de la correspondance d'un employé, et que la collecte et la conservation de ces informations à l'insu de l'employé constitueraient une atteinte à ses droits, bien que la Cour n'ait pas statué qu'une telle surveillance ne serait jamais nécessaire dans une société démocratique. Voy. également Cour eur. D.H., 5 septembre 2017, *Bărbulescu c. Roumanie*, req. n° 61496/08. Dans cet arrêt, la Cour précise les critères que doivent appliquer les autorités nationales lorsqu'elles apprécient si une mesure prise pour surveiller les communications des employés est proportionnée au but poursuivi et si l'employé concerné est protégé contre l'arbitraire.

¹³⁸ Dans le même esprit, le considérant 50 du RGPD stipule que «le fait, pour le responsable du traitement, de révéler l'existence d'éventuelles infractions pénales ou de menaces pour la sécurité publique et de transmettre à une autorité compétente les données à caractère personnel concernées dans des cas individuels ou dans plusieurs cas relatifs à une même infraction pénale ou à des mêmes menaces pour la sécurité publique devrait être considéré comme relevant de l'intérêt légitime du responsable du traitement». Pour ce qui est des interactions entre les débiteurs de l'obligation de sécurité et les autorités susmentionnées, la Convention de Budapest prévoit des méthodes d'enquêtes spécifiques pour les forces de l'ordre dans le contexte digital, dont notamment la saisie de données informatiques et la recherche dans un système informatique. De plus, en Belgique, la collaboration d'un responsable du traitement ou d'un sous-traitant en vue de la production de logs peut être demandée sur base d'une ordonnance du juge d'instruction conformément à l'article 88quater du Code d'instruction criminelle.

¹³⁹ ENISA, «Big data Security: Good Practices and Recommendations on the Security of big data Systems», *op. cit.*, p. 24.



l'obligation de sécurité de se conformer au principe de minimisation des données¹⁴⁰.

CONCLUSION

Étant donné les risques techniques inhérents au big data découlant notamment de la masse de données traitées, de l'utilisation de périphériques dotés de capacités limitées, du niveau élevé de réplication et de l'externalisation fréquente des traitements, des mesures de sécurité effectives ainsi que de notification des incidents paraissent indispensables à tous les maillons de la chaîne. Dans ce contexte, l'on ne peut que saluer l'adoption de la directive NIS et le renforcement de l'obligation de sécurité dans le RGPD imposant notamment la réalisation d'une AIPD avant le traitement de mégadonnées considéré ainsi que la notification obligatoire à tous les niveaux en cas de fuites des données. Toutefois, même si elle se trouve ainsi consolidée, l'obligation de sécurisation des données reste, dans les textes légaux, une obligation de moyens. En cas de sous-traitance et de sous-traitance de second rang, des dispositions conventionnelles additionnelles prévoyant des obligations de résultat entre les différents acteurs paraissent essentielles afin de garantir une répartition adéquate des responsabilités lors de mésaventures. Afin de répercuter en cascade le contenu d'une politique de sécurité cohérente, ces dispositions contiendront utilement des exigences contractuelles d'adhésion de tous les intervenants à des codes de conduite précis en matière de cybersécurité, de certification par des auditeurs indépendants agréés, des précisions quant aux mesures de sécurité garantissant la confidentialité, l'intégrité et la disponibilité des données mais également, nous semble-t-il, des impératifs en matière d'imputabilité, d'authenticité et de non-répudiation des traite-

ments opérés sur celles-ci. Il va sans dire que la *mise en œuvre strictement nécessaire et proportionnée* de ces trois fonctions de sécurité s'avèrera utile à des fins probatoires dans le cadre de potentielles procédures civiles, disciplinaires, administratives ou pénales, notamment lorsque la licéité d'un accès aux données est contestée ou lorsqu'une violation de données à caractère personnel est en jeu. À cet égard, un cadre légal régissant de manière explicite la journalisation dans le RGPD aurait été le bienvenu afin, d'une part, d'offrir une garantie de transparence supplémentaire aux personnes concernées qui exerceraient leur droit d'accès pour le passé et, d'autre part, de procurer une certaine sécurité juridique aux débiteurs qui y auraient recours afin de se réserver des preuves vis-à-vis de leurs co-contractants. Heureusement, l'absence de mentions expresses relatives aux fonctions d'imputabilité, d'authenticité et de non-répudiation des données dans les textes légaux est compensée par la jurisprudence européenne et par les recommandations des autorités de contrôle nationales qui préconisent fortement la mise en place de politiques d'authentification, de gestion des accès logiques et de journalisation. Ces dernières confortent la *ratio legis* du RGPD selon laquelle sécurité des données et *accountability* vont de pair: une obligation de moyens n'a de réelle puissance que lorsqu'elle est accompagnée de mesures permettant de vérifier si ses débiteurs ont été suffisamment prudents et diligents dans sa mise en œuvre.

¹⁴⁰ Article 5, § 1^{er}, c), du RGPD.