36

La protection des données dans un monde globalisé

Alexandre Fiévée
Avocat au barreau de Paris
Elvinger, Hoss & Prussen

Patrick Santer
Elvinger, Hoss & Prussen

Table des matières

Introduction

1. La globalisation est l'acte qui consiste à concevoir et appréhender quelque chose comme un tout. D'un point de vue économique, elle se traduit par le développement de stratégies à l'échelle planétaire, conduisant à la mise en place d'un marché mondial unifié. Cette notion renvoie ainsi inévitablement à celle de mondialisation. D'ailleurs, étymologiquement, leur racine respective – « globe » et « monde » – est suffisamment proche pour que « globalisation » et « mondialisation » soient considérées comme synonymes. Toutefois, chacun s'accorde à voir dans la globalisation soit une nouvelle forme de mondialisation (également appelée la « mondialisation contemporaine »), soit une forme de dépassement de la mondialisation. Alors que la mondialisation peut s'appréhender comme un processus de généralisation des échanges (de capitaux, de biens, d'informations, etc.) entre les acteurs économiques localisés dans différentes parties du monde, la globalisation se caractérise en outre par la capacité des acteurs à se connecter, à interagir et à coordonner leurs actions en temps réel grâce aux progrès technologiques.

2. Ces progrès ont constitué, en effet, un élément déterminant, sinon décisif, dans le développement du processus de globalisation. Il est indéniable que la période récente a été marquée par des avancées majeures :

– tout d'abord, la mise au point d'algorithmes puissants de compression des données permettant l'informatique multimédia, et donc la généralisation de l'utilisation des techniques numériques rendant ainsi possible le transport – de plus en plus important –de tout type de données à travers des supports variés vers des récepteurs universels ;
– ensuite, le protocole internet qui permet à des routeurs placés aux nœuds des réseaux de télécommunication du monde entier de transporter de plus en plus rapidement des paquets de données vers n'importe quelle destination.

3. L'acheminement d'un volume de données quasi illimité pour un coût très faible ne pose donc plus de problème, expliquant ainsi, d'un point de vue technique, notamment la constitution de ces bases de données géantes, (appelées *Big data*), la pratique de l'*e-mailing* ou encore le recours à la délocalisation. Tout le monde s'accorde ainsi pour considérer les nouvelles technologies de l'information « comme étant à la base des processus de globalisation »[1].

[1] C. Milani, « Les différentes dimensions de la globalisation et l'essai d'une régulation par le marché », *Cahiers du Brésil contemporain*, 2000, nº 41/42.

4. Si les progrès technologiques ont été déterminants, l'existence d'un environnement politique et réglementaire propice y a également contribué. Selon le STATEC (Institut national de la statistique et des études économiques), « si le progrès technique est une condition nécessaire du processus de globalisation, il n'est pas suffisant ». Ainsi, « à partir du début des années 1970, des mesures de libéralisation, de déréglementation dans le secteur financier, d'abord, dans les domaines des transports et des communications, ensuite, ont largement favorisé le processus de globalisation »[2].

5. Le STATEC ajoute que « l'extension de ce développement à une multitude de domaines et sa quasi-généralisation au niveau de la planète ont bien sûr été accélérées après l'effondrement du mur de Berlin et l'intégration de presque toutes les nations dans le système économique mondial »[3].

6. Par ailleurs, et indépendamment de cet environnement favorable, plusieurs circonstances d'ordre économique doivent être appréhendées comme des éléments moteurs du processus de globalisation : si la recherche d'un profit au niveau mondial par les acteurs privés est l'un de ces éléments, la volonté de réaliser une économie en est un autre. Ainsi, la mise en œuvre d'une politique de réduction des coûts se traduit souvent par une délocalisation d'une infrastructure ou d'une fonction de l'entreprise dans des pays en voie de développement ou dans des pays dits « émergents », et ce, dans l'optique de bénéficier, à moindre coût, d'un environnement technologique favorable et/ou d'une main-d'œuvre qualifiée. Par ailleurs, la volonté des entreprises multinationales et des groupes d'entreprises de rationaliser les tâches a contribué également à entretenir le processus de globalisation, dans la mesure où elle conduit à une centralisation des traitements des différentes entités dans un pays donné.

7. Il convient de noter que cette tendance à la délocalisation n'est pas nouvelle. Elle s'est développée, en effet, dans les années 1980 en Europe avec notamment l'*outsourcing IT* (également appelée « infogérance informatique »), qui a permis aux entreprises de se recentrer sur leur activité principale (*core business*) en délocalisant leur infrastructure informatique et en confiant à des prestataires informatiques externes la gestion et l'exploitation de leur système d'information. La complexité de ces opérations et l'importance des coûts associés à une telle gestion expliquent généralement le choix opéré en faveur d'une telle délocalisation.

---

2 STATEC, « Le Luxembourg 1960-2010 – Une économie de petit espace face aux mutations du monde », 29 avril 2013.

3 STATEC, « Le Luxembourg 1960-2010 – Une économie de petit espace face aux mutations du monde », 29 avril 2013.

8. Ainsi, si l'*outsourcing* n'est pas nouveau, en revanche, de nouvelles formes d'externalisation sont apparues avec, notamment, le *Business Process Outsourcing* (ou *BPO*), qui consiste dans l'externalisation non pas de l'infrastructure informatique, mais de l'intégralité d'une opération métier ou d'un processus de l'entreprise (telle que la comptabilité, la gestion des contrats commerciaux ou encore la gestion administrative des ressources humaines). En 2009, selon l'ITIDA (Information Technology Industry Developmement Agency), l'*outsourcing* (*IT* et *BPO*) représentait un marché mondial compris entre 92 et 96 milliards de dollars avec, comme principaux « consommateurs », le secteur de la finance et de l'assurance (40 %)[4]. En 2011, le marché mondial de l'*outsourcing IT* était estimé, par le cabinet Gartner, à lui seul à 246,6 milliards de dollars[5] grâce notamment au développement du *cloud computing* (encore appelé nuage informatique ou l'informatique dématérialisée).

9. Le *cloud computing*, qui repose sur les technologies de la virtualisation, s'analyse en effet comme une forme d'externalisation en ce que l'entreprise, au lieu d'investir dans des équipements informatiques qui lui sont propres, va consommer, en fonction de ses besoins, des services proposés par un tiers et accessibles à distance (selon les protocoles et standards internet). Quatre offres de services se partagent actuellement le marché : l'offre *SaaS* (*Software as a service*), qui concerne principalement des applications d'entreprise et consiste dans la mise à disposition à distance d'une fonction opérationnelle standardisée ; l'offre *PaaS* (*Platform as a service*), qui porte sur des environnements de tests et de production et consiste dans la mise à disposition d'une plate-forme prête à l'emploi en vue notamment d'y développer des applications ; l'offre *IaaS* (*Infrastructure as a service*), qui porte principalement sur des serveurs, des processeurs et des capacités de stockage, et consiste dans la mise à disposition de ressources informatiques ; enfin, l'offre BPaaS (*Business Process as a service*), qui pourrait remplacer à terme le *BPO*. À cet égard, le cabinet Gartner estime que le marché du *BPaaS* pourrait atteindre 144,7 milliards de dollars en 2016 et suivre un taux de croissance annuel moyen de 15 %[6].

10. Au Luxembourg, l'externalisation pour les entreprises du secteur financier repose sur un cadre juridique certain, avec notamment la loi modifiée du 5 avril 1993 relative au secteur financier et les circulaires de la Commission de

---

4 D. Filippone, « 61 % du marché européen de l'externalisation concerne l'informatique », 13 décembre 2010, http://www.journaldunet.com.

5 D. Barathon, « Le marché mondial de l'outsourcing a progressé de 7,8 % en 2011 », 21 mai 2012, http://www.distributique.com.

6 D. Filippone, « BPaaS ou la gestion des processus métiers dans le *Cloud* », 3 mai 2013, http://www.journaldunet.com.

surveillance du secteur financier (ci-après la « CSSF »)[7]. Le 12 décembre 2012, une circulaire 12/552 (modifiée par la circulaire 13/563 du 19 mars 2013) est venue préciser le cadre réglementaire, s'agissant notamment des conditions dans lesquelles les entreprises du secteur financier sont autorisées à recourir à l'*outsourcing* et, notamment, à la « sous-traitance dans le domaine informatique ».

11. Ce cadre favorable à l'*outsourcing* a tout récemment été complété par la loi du 9 juillet 2013 portant modification de l'article 567 du Code de commerce[8], qui prévoit désormais la possibilité pour l'entreprise cliente, en cas de faillite du prestataire, de récupérer, dans le cadre d'une action en revendication, ses données et fichiers, ce qui inclut les traitements qui ont été effectués et les résultats de ces traitements.

12. Dans ce contexte technique, économique et juridique, ce qui finalement caractérise le mieux la globalisation, c'est la nette accélération de la circulation des biens, des services…, mais aussi et surtout des données. Certains parlent même de « globalisation de l'information ». Selon Pierre-Noël Giraud, professeur d'économie à l'École des mines de Paris, la globalisation n'est autre qu'un processus qui rend désormais techniquement très difficile d'empêcher la copie et la circulation, à un coût dérisoire, des données et des fichiers[9]. D'ailleurs, dans un rapport réalisé à l'instigation du Conseil de l'Europe, il est clairement indiqué que cette globalisation des échanges d'informations constitue un « défi redoutable » pour la protection des données[10]. Mais de quelles données s'agit-il ?

13. Il s'agit de toutes les données privées collectées, utilisées, produites par l'entreprise dans le cadre de ses activités et qui, du fait de la globalisation, vont circuler et s'échanger, et ce, sans considération des frontières : données économiques et financières, données clients, données de ressources humaines, etc. Certaines, sur le plan juridique, sont qualifiées de données « confidentielles », d'autres sont soumises à un régime de protection particulier : les données à caractère personnel dites « sensibles » comme les données de santé ; les données financières ; les données judiciaires, etc. Sur le plan économique,

---

7 Les circulaires CSSF 05/178 et CSSF 06/240.

8 Loi du 9 juillet 2013 portant modification de l'article 567 du Code de commerce.

9 P.-N. Giraud, « Comment la globalisation façonne le monde », *Politique étrangère*, avril 2006.

10 J.-Ph. Walter, *Défis posés par les flux transfrontières de données à caractère personnel*, Rapport rédigé à l'instigation du Conseil de l'Europe, www.edsb.ch.

elles ont acquis une valeur marchande sans précédent. Elles sont devenues « des marchandises, des biens de consommation qui s'achètent, se vendent et s'échangent », au risque parfois de mettre en péril le droit au respect de la vie privée des individus[11].

14. Sur le plan juridique, la rapidité de l'évolution technologique est telle que le cadre légal a du mal à encadrer ou simplement aborder un domaine en constante mutation. Ainsi, si le Luxembourg a été parmi les premiers pays à se doter d'une législation en matière de protection des données à caractère personnel par la loi du 31 mars 1979, l'absence d'adaptation de celle-ci pendant les années 1980 et 1990 a rendu l'application de cette loi « illusoire »[12]. Le législateur luxembourgeois s'est efforcé de donner à la « société de l'information » des règles contraignantes et protectrices pour les consommateurs,[13] mais aussi d'adapter le cadre juridique à ces nouvelles technologies de l'information.[14] Il n'en demeure pas moins que cette intégration n'est pas évidente lorsqu'on tente de concilier des concepts juridiques remontant au XIX^e^ siècle avec l'environnement technologique du XXI^e^ siècle.

15. Dans ce contexte de globalisation, la protection des données est indispensable pour instaurer un climat de confiance. Cela passe par le respect scrupuleux par l'entreprise des règles en vigueur en matière de protection des données à caractère personnel (chapitre 1). Il s'agit également, pour l'entreprise, de protéger l'une de ses principales richesses, à savoir son « patrimoine informationnel ». Dans ce cadre, il lui appartient de veiller à garder une certaine maîtrise de ses données (chapitre 2) et de garantir leur confidentialité et leur sécurité (chapitre 3).

---

11 J.-Ph. Walter, *Défis posés par les flux transfrontières de données à caractère personnel*, Rapport rédigé à l'instigation du Conseil de l'Europe, www.edsb.ch.

12 Rapport de la Commission parlementaire des médias et des communications sur le projet de loi relatif à la protection des personnes à l'égard du traitement des données à caractère personnel, *Doc. parl.*, 4735-13, p. 3.

13 Par exemple, la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

14 Par exemple, la loi modifiée du 14 août 2000 relative au commerce électronique et le projet de loi 6543 relatif à l'archivage électronique. Ainsi, à propos de l'archivage électronique, les auteurs du projet de loi 6543 relèvent que « devenu obsolète, le cadre législatif actuel ne permet pas aux acteurs économiques de profiter pleinement des technologies de l'information et, du coup, pourrait pénaliser la place luxembourgeoise » (*Doc. parl.*, 6543, p. 2).

Chapitre 1

Le traitement licite des données

16. La collecte et l'exploitation des données à caractère personnel (section 1), mais aussi leur transfert (section 2), ont connu une augmentation spectaculaire, en raison principalement de la rapide évolution des technologies de l'information. Encadrées par des textes, ces opérations ne doivent pas se faire au détriment des intérêts des personnes physiques, qui doivent pouvoir assurer une maîtrise de l'utilisation qui est faite de leurs données.

Section 1
La collecte et l'exploitation

17. La Commission nationale de protection des données (CNPD) le constate aisément : « les progrès technologiques rapides et la globalisation sont des phénomènes qui ont modifié en profondeur la manière de collecter, de consulter et d'utiliser les données de l'individu »[15]. Il n'en demeure pas moins que ces traitements de données à caractère personnel doivent être réalisés dans le respect des principes édictés par la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. C'est notamment le cas de ces traitements réalisés dans le cadre de l'utilisation des *cookies*, du recours à la pratique de l'*IP Tracking* ou encore de l'*e-mailing*. Autant de pratiques qui se sont développées dans ce contexte de globalisation et qui doivent respecter ces principes généraux, ainsi que, pour certaines, des règles particulières édictées par des textes spécifiques.

Sous-section 1
Les principes généraux[16]

18. La collecte et l'exploitation des données des personnes physiques obéissent à des règles très strictes visées dans la loi modifiée du 2 août 2002 précitée.

19. Il appartient ainsi à toute entreprise qui prend l'initiative de collecter des données à caractère personnel pour des finalités qu'elle a déterminées, en sa qualité de responsable du traitement, de s'assurer que les données ont été

---

15 CNPD, *Rapport d'activité 2012*, juillet 2013.

16 Pour une analyse détaillée de ces principes, nous renvoyons à l'article de P. Santer et T. Hoss, « La loi du 2 août 2002 sur la protection des personnes à l'égard du traitement des données à caractère personnel : une nouvelle donnée pour la place financière », ALJB, *Droit bancaire et financier*, avril 2004.

collectées pour « des finalités déterminées, explicites et légitimes » et qu'elles ne seront pas traitées ultérieurement « de manière incompatible avec ces finalités »[17]. Ces données doivent être « adéquates, pertinentes et non excessives » au regard de ces finalités[18].

20. En tout état de cause, cette collecte et tout autre traitement ultérieur – entendu comme « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés » – ne peuvent être effectués que sous certaines conditions et notamment lorsqu'ils sont nécessaires à « l'exécution d'un contrat auquel la personne concernée est partie » ou lorsque celle-ci a donné « son consentement »[19].

21. Par ailleurs, ces traitements sont soumis à des formalités préalables auprès de la CNPD, à savoir soit, en principe, une notification préalable (sauf en cas d'exemptions légales), soit, dans les cas prévus par la loi, une demande d'autorisation préalable[20].

22. Enfin, le responsable du traitement – à savoir la personne qui détermine les finalités d'un traitement de données à caractère personnel – se doit de respecter les droits de la personne concernée[21] :

– le droit à l'information, qui permet à celle-ci de connaître, préalablement à la collecte, notamment l'identité du responsable du traitement, les finalités du traitement, les destinataires, l'existence de ses droits et la durée de conservation des données ;
– le droit d'accès, qui lui permet d'obtenir auprès du responsable du traitement confirmation que des données la concernant sont traitées et communication desdites données ;
– et le droit d'opposition, qui lui permet de s'opposer à tout moment, pour des raisons légitimes, à ce que des données la concernant fassent l'objet d'un traitement.

Sous-section 2

La pratique des cookies

23. Les *cookies* sont des fichiers textes au format alphanumérique déposés sur le disque dur de l'ordinateur par le serveur généralement du site internet

17 Loi modifiée du 2 août 2002, article 4.
18 Loi modifiée du 2 août 2002, article 4.
19 Loi modifiée du 2 août 2002, article 5.
20 Loi modifiée du 2 août 2002, articles 12 et s.
21 Loi modifiée du 2 août 2002, articles 26 et s.

visité. Cette pratique est réalisée en vue, d'une part, d'identifier l'internaute à chacune de ses nouvelles visites et, d'autre part, de consulter ses navigations antérieures. L'objectif affiché est de faciliter l'utilisation ultérieure du site internet par cet internaute. Le principe, qui connaît des exceptions, est celui du consentement préalable de l'internaute pour le stockage, dans son équipement terminal, de *cookies* par le responsable du site internet.

§ 1. Le principe du consentement préalable

24. L'utilisation des *cookies* est réglementée au niveau européen par la directive 2009/136/CE du 25 novembre 2009[22], qui a été transposée en droit luxembourgeois par la loi du 28 juillet 2011 modifiant la loi du 30 mai 2005 relative à la protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques.

25. L'article 4, (3),(e), de la loi du 30 mai 2005 précitée dispose ainsi que le stockage, par le responsable d'un site internet, d'informations ou l'obtention de l'accès à des informations déjà stockées dans l'équipement terminal d'un abonné ou d'un utilisateur est autorisé à condition, toutefois, de « l'accord » de ce dernier, et ce, « après avoir reçu une information claire et complète, entre autres sur les finalités du traitement ». Les législateurs national et européen n'ayant pas donné de définition de l'accord requis pour permettre au responsable d'un site internet de recourir licitement à la pratique des *cookies*, le groupe de travail « Article 29 » est venu, par un avis 02/2013 rendu le 2 octobre 2013, préciser les caractéristiques que doit revêtir cet accord. Ainsi, selon le groupe de travail « Article 29 », il appartient au responsable du site web de mettre en place un dispositif permettant :

– une information spécifique : le consentement de l'utilisateur doit être basé sur une information préalable, claire et compréhensible ; le groupe indique ainsi que cette information relative à l'utilisation des *cookies* doit être accessible sur la page d'accueil du site internet consulté par l'utilisateur et doit porter notamment sur le type et la finalité des *cookies*, leur durée de validité et, le cas échéant, les destinataires potentiels des informations recueillies au moyen de ces *cookies* ; les utilisateurs doivent également avoir connaissance des méthodes d'acceptation des *cookies*, ainsi que des éventuelles conséquences d'un refus sur la poursuite ou non de la navigation sur le site internet en question ;
– un consentement préalable : le groupe de travail « Article 29 » indique que le consentement doit être sollicité préalablement au placement des

[22] La directive 2009/136/CE modifie la directive 2002/58/CE.

cookies; les responsables de site internet doivent, en conséquence, s'assurer que la méthode d'acceptation des *cookies* ne nécessite pas en elle-même, l'installation ou la lecture de *cookies*;

– une action positive: selon le groupe de travail «Article 29», le consentement peut se manifester au moyen d'un clic sur un lien d'acceptation dédié ou dans une case à cocher qui notifiera ainsi cette acceptation; en tout état de cause, la case à cocher ou le lien d'acceptation doit être localisé à proximité de la mention d'information portant sur les *cookies* et ce, afin de garantir un consentement éclairé;
– un consentement libre et réel: le consentement doit résulter d'un véritable choix de l'utilisateur qu'il doit pouvoir effectuer dès son arrivée sur la page d'accueil du site internet; l'utilisateur doit, en conséquence, pouvoir accepter tous les *cookies* ou seulement certains; il doit également être en mesure de modifier les paramètres initialement choisis et de retirer à tout moment son consentement.

26. Si le législateur n'a ainsi pas donné de définition de l'«accord», il en donne une illustration en indiquant que cet «accord» peut être exprimé «par l'utilisation de paramètres appropriés d'un navigateur ou d'une autre application», dès lors que «cela est techniquement possible et effectif»[23]. Cela signifie donc qu'en utilisant les options proposées par le logiciel de navigation pour manifester son consentement à la pratique des *cookies,* l'utilisateur ou l'abonné donne, au sens de la loi du 30 mai 2005, son accord ou non à une telle pratique. Cet accord peut être également exprimé, selon le législateur, par l'utilisation «d'une autre application», sans qu'il soit précisé le type d'«application» couvert par la loi. En pratique, des plateformes interprofessionnelles dédiées à l'acceptation ou au refus des *cookies* se sont créées permettant, notamment, à l'utilisateur ou à l'abonné, en cliquant sur un lien de désactivation, de refuser les *cookies* de toutes les sociétés membres de la plateforme[24]. Il semble, dès lors, possible de considérer que les «applications» mentionnées par le législateur fassent référence à ce type de plateformes.

27. En tout état de cause, le consentement au placement de *cookies* donné au moyen de l'utilisation des paramètres de navigation ou d'une autre application ne peut constituer un consentement valable que sous réserve que celui-ci réponde à la définition donnée par la loi modifiée du 2 août 2002, à savoir une

---

23 Article 4, (3), (e), de la loi du 30 mai 2005 relative à la protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques.

24 Telles que la plate-forme européenne Youchoices.com proposée par les professionnels de la publicité digitale regroupés au sein de l'association européenne EDAA (European Digital Advertising Alliance).

manifestation de volonté libre, spécifique et informée se traduisant par un acte positif. À ce titre, le groupe de travail « Article 29 » souligne que « les personnes concernées ne sauraient avoir donné leur consentement simplement parce qu'elles ont acheté/utilisé un navigateur ou une autre application qui permet, par défaut, la collecte ou le traitement de leurs informations »[25]. Il constate, en effet, que très souvent les personnes concernées n'ont même pas connaissance du traçage de leurs informations et ne savent pas non plus comment paramétrer le navigateur pour refuser les *cookies* (et ce, nonobstant les informations figurant dans les politiques de confidentialité des émetteurs), ce qui rend ces personnes inaptes à donner leur accord. Le groupe de travail « Article 29 » relève, en conséquence, qu'il est difficile d'apprécier si l'absence de modification des paramètres du navigateur constitue une véritable manifestation de volonté d'accepter les *cookies* de la part de la personne concernée ou, au contraire, résulte simplement d'une ignorance de sa part. Ainsi, le groupe de travail « Article 29 » préconise aux créateurs de navigateurs et d'applications de configurer leurs navigateurs/applications pour que ces derniers refusent « par défaut les *cookies* tiers », de telle sorte que la personne concernée doive effectuer une action positive pour accepter les *cookies* et ainsi exprimer un consentement valable et effectif.

28. Le groupe de travail « Article 29 » rappelle, par ailleurs, la nécessité pour les créateurs de navigateurs, mais également les fournisseurs de réseaux publicitaires ainsi que les diffuseurs, de permettre, en tout état de cause, un consentement informé.

§ 2. Les exceptions au principe du consentement

29. En application de l'article 4, (3), (e), de la loi du 30 mai 2005, l'implantation de *cookies* peut échapper à l'obligation d'information et de recueil du consentement de l'utilisateur ou de l'abonné lorsqu'elle vise « exclusivement à effectuer ou à faciliter la transmission d'une communication par la voie du réseau de communications électroniques »[26]. En revanche, le législateur ne donne pas d'indication sur les cas dans lesquels un *cookie* peut se révéler indispensable à cette transmission. À ce titre, le groupe de travail « Article 29 » indique qu'un *cookie* possédant au moins l'une des trois caractéristiques suivantes peut être considéré comme strictement nécessaire à la transmission d'une communication entre deux parties par la voie d'un réseau, à savoir « la capacité d'acheminer l'information sur le réseau, la capacité d'échanger les

[25] Groupe de travail « Article 29 », *Avis 2/2010 sur la publicité comportementale*, 22 juin 2010.

[26] Directive 2002/58/CE, article 5, § 3 ; loi du 30 mai 2005 de l'article 4, (3).

données dans leur ordre prévu et la capacité de détecter les erreurs de transmission ou les pertes de données »[27]. Il précise également ce qu'il faut entendre par transmission d'une communication par la voie d'un réseau de communications électroniques « tout type d'échanges de données ayant lieu au moyen d'un réseau de communication électronique », étant précisé que le réseau de communication électronique correspond, au sens de la directive 2002/21/CE, à un système de transmission dont l'objet est de permettre l'acheminement de signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques[28]. Le contrôleur européen de la protection des données, au moment de l'élaboration de la directive « *e-privacy* »,[29] mentionnait, à titre d'illustration, le cas de l'accès à un site internet par un utilisateur : « [L]orsqu'un utilisateur souhaite accéder à un site web, il doit adresser une demande au serveur hébergeant le site en question. Celui-ci répondra s'il sait où envoyer l'information, c'est-à-dire s'il connaît l'adresse IP de l'utilisateur. En raison du mode de stockage de cette adresse, il faudra à nouveau que le site web sur lequel l'utilisateur souhaite se rendre accède à des informations sur l'équipement terminal des internautes. »[30] Cet accès au terminal de l'utilisateur, indispensable pour la transmission de la communication, rentrerait dès lors dans le champ d'application de l'exception au principe du consentement.

30. Une seconde exception à ce principe vise l'implémentation du *cookie* qui est « strictement nécessaire à la fourniture d'un service de la société d'information expressément demandé par l'abonné ou par l'utilisateur ». Aux termes de l'article 1er de la loi modifiée du 14 août 2000 sur le commerce électronique, il faut entendre par service de la société d'information « tout service presté, normalement contre rémunération, à distance par voie électronique et à la demande individuelle d'un destinataire de services ». Ces services englobent, dès lors, un large éventail d'activités économiques parmi lesquelles la vente de biens en ligne, mais également les services consistant à transmettre des informations par le biais des réseaux de communication ou encore à fournir un accès à un réseau de communication[31]. Selon le groupe de travail « Article 29 », seuls les *cookies* placés dans le cadre d'un service de la société d'information

---

27 Groupe de travail « Article 29 », *Avis 04/2012 sur l'exemption de l'obligation de consentement pour certains* cookies, 7 juin 2012.

28 Directive 2002/21/CE, article 2, a).

29 Directive 2002/58 CE.

30 Avis du contrôleur européen de la protection des données sur la proposition de directive du Parlement européen et du Conseil modifiant, entre autres, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

31 Voy. 18e considérant de la directive 2000/31/CE du 8 juin 2000 sur le commerce électronique.

demandé par l'utilisateur au moyen d'une action positive et sans lesquels le service ne pourra pas fonctionner rentrent dans le champ d'application de l'exception. Il pourra aussi bien s'agir, dans le cadre d'un service de commerce électronique, de *cookies* utilisés pour mémoriser le formulaire rempli par l'internaute ou un panier d'achat (« *user-input cookies* ») que, dans le cadre d'une souscription à un abonnement sur internet, de *cookies* utilisés pour identifier un utilisateur (« *authentification cookies* »)[32].

31. En d'autres termes, dès lors qu'elle est utile ou nécessaire à la transmission d'une communication ou à la fourniture d'un service, la pratique du *cookie* entre dans le périmètre des exceptions. En revanche, lorsque le recours aux *cookies* par le responsable du site internet est motivé par d'autres finalités – comme la gestion publicitaire, le profilage ou encore le traçage des internautes –, il est alors contestable[33].

Sous-section 3
*L'*IP *Tracking*

32. La pratique de *l'IP tracking* et la question de sa licéité ont récemment été placées sur le devant de la scène par le biais d'une question parlementaire posée à la Commission européenne. Cette pratique, qui se serait développée dans le secteur du transport aérien, mais qui peut être utilisée dans d'autres secteurs d'activités, consiste à proposer à un internaute, lors de ses connexions ultérieures au site de l'opérateur, pour une même recherche de billets, un prix supérieur à celui affiché lors de sa première visite. L'objectif serait ainsi d'inciter l'internaute à acheter un billet immédiatement en laissant supposer que le nombre de places disponibles diminue et donc que le prix augmente. D'un point de vue technique, une telle pratique est rendue possible par la collecte, lors de la première visite de l'internaute, de son adresse IP ainsi que de ses données de navigation, permettant alors son identification lors de ses visites ultérieures par le responsable du site.

33. Le 12 mars 2013, la commissaire européenne à la Société numérique, Viviane Reding, a répondu que les « adresses IP […] sont susceptibles de constituer des données à caractère personnel si elles laissent des traces qui, associées à d'autres informations reçues par les serveurs, peuvent être utilisées pour créer des profils et identifier ainsi, directement ou indirectement les

---

[32] Groupe de travail « Article 29 », *Avis 04/2012 sur l'exemption de l'obligation de consentement pour certains* cookies, 7 juin 2012.

[33] CNPD, *Rapport d'activité 2012*, juillet 2013.

personnes concernées […] ». Elle a considéré que « sans préjudice des compétences de la Commission […], les autorités de contrôle nationales chargées de la protection des données sont les organes compétents pour le suivi de l'application des mesures nationales de transposition de la directive 95/46/CE ». Il revient donc, selon la Commission européenne, aux autorités de contrôle nationales de s'assurer du respect des dispositions en vigueur en matière de protection des données.

34. Ainsi, selon la commissaire européenne, la licéité de la pratique de l'*IP Tracking* doit être appréciée en application « des mesures nationales de transposition de la directive 95/46/CE », et ce, dans la mesure où les adresses *IP* sont susceptibles de constituer des données à caractère personnel. Selon cette directive[34], un traitement de données à caractère personnel n'est licite que sous réserve que le responsable du traitement ait respecté certaines conditions. À cet égard, il convient de noter que s'analyse comme une « donnée à caractère personnel » toute information concernant une personne physique identifiée ou identifiable. Ainsi, il ne fait aucun doute que l'adresse *IP* – à savoir un numéro d'identification attribué de façon permanente ou provisoire à tout appareil connecté à un réseau informatique utilisant l'*Internet Protocol* – doit être considérée comme une donnée à caractère personnel. Dans ces conditions, le responsable d'un site internet, qui collecte l'adresse *IP* d'un visiteur, réalise un traitement soumis aux dispositions de la directive 95/46 et donc de la loi modifiée du 2 août 2002, lequel traitement est défini comme « toute opération ou ensemble d'opérations […] appliquées à des données à caractère personnel, telles que la collecte […] l'utilisation […] ». Le responsable du site internet se doit alors, comme indiqué ci-dessus, de respecter certains principes et certaines conditions dans la mise en œuvre de ce traitement. Ainsi, il lui appartient de collecter les données pour des finalités déterminées, explicites et légitimes et il ne doit pas les traiter ultérieurement de manière incompatible avec ces finalités. Par ailleurs, le traitement de ces données doit être loyal et licite. Le responsable du site internet se doit aussi d'obtenir le consentement de la personne concernée avant que le traitement (notamment la collecte) ne soit effectué, étant précisé que l'internaute doit avoir été informé notamment des finalités du traitement auquel les données sont destinées. Compte tenu notamment du principe selon lequel la finalité du traitement doit être légitime, il semble acquis que le responsable du site internet, qui se livrerait à la pratique de l'*IP Tracking* pour inciter les internautes à acheter des billets à un prix différent de celui

[34] Directive 95/46 CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Cette directive a été transposée par le Luxembourg par la loi modifiée du 2 août 2002.

proposé lors de la première visite, serait en infraction avec les dispositions de la directive 95/46/CE et de la loi modifiée du 2 août 2002.

35. Il convient de noter que la Commission européenne ne s'est intéressée à la question de la licéité de ces pratiques qu'au regard des dispositions de la directive 95/46/CE relative aux données à caractère personnel, alors qu'il est fort probable que de telles pratiques puissent s'analyser également, indépendamment de la problématique des données, comme étant déloyales au sens de la directive 2005/29/CE relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur[35].

Sous-section 4

Le marketing direct ou l'e-mailing

36. L'*e-mailing*, qui consiste en l'envoi massif de courriers électroniques à finalité commerciale ou publicitaire, constitue un véritable enjeu pour les entreprises dans le cadre d'une démarche de prospection. En effet, cette démarche commerciale représente un des moyens de marketing direct les plus efficaces, compte tenu de son faible coût et de son taux de réponses élevé. Conscientes de cet enjeu, les entreprises n'hésitent pas à réaliser des investissements conséquents pour la mise en œuvre de ce type de campagne, qui peut s'avérer toutefois problématique d'un point de vue juridique.

§ 1. Le respect du principe de l'« *opt-in* » sauf…

37. Il ressort de l'article 11(1) de la loi modifiée du 30 mai 2005 relative à la protection des données dans le secteur des communications électroniques que « l'utilisation de systèmes automatisés d'appel et de communication sans intervention humaine (automates d'appel), de télécopieurs ou de courrier électronique à des fins de prospection directe n'est possible que si elle vise l'abonné ou l'utilisateur ayant donné son consentement préalable ». En outre, « l'envoi de communications non sollicitées à des fins de prospection directe par d'autres moyens […] n'est possible que si l'abonné ou l'utilisateur" concerné a donné son consentement ».

38. En d'autres termes, l'entreprise ne peut recourir à la prospection directe au moyen d'un courrier électronique, d'un « short message service » (SMS) ou d'une communication téléphonique utilisant les coordonnées d'une personne

[35] Cette directive 2005/29/CE a été transposée en droit luxembourgeois par la loi du 29 avril 2009 relative aux pratiques commerciales.

physique sans avoir obtenu au préalable le consentement de cette dernière à recevoir de tels messages.

39. La circonstance selon laquelle l'entreprise aurait acquis les adresses électroniques d'une entreprise cédante, et donc n'aurait pas directement collecté les données auprès des personnes concernées, n'est pas de nature à l'exonérer de sa responsabilité. Il lui appartient, en effet, de s'assurer que le fichier acheté contient les coordonnées de personnes ayant donné leur consentement à recevoir des messages de prospection commerciale[36].

40. Toutefois, l'article 11, (2), de la loi susvisée du 30 mai 2005, précise que « le fournisseur qui, dans le cadre d'une vente d'un produit ou d'un service, a obtenu […] de ses clients leurs coordonnées électroniques en vue d'un courrier électronique peut exploiter ces coordonnées électroniques à des fins de prospection directe pour des produits ou services analogues […] ».

41. Toute la difficulté, pour se prévaloir du régime de l'exception, réside à déterminer, en l'absence de définition légale ou jurisprudentielle, les contours de la notion de « produits et services analogues ». Pour ce faire, il est possible de se référer à l'annexe du code de déontologie européen en matière d'utilisation de données à caractère personnel dans le marketing direct, validé en juin 2010 par le groupe de travail « Article 29 », qui indique que la personne concernée doit être informée à l'avance, lors de la collecte, de la signification des « produits et services analogues », afin de s'assurer que la prospection qui sera réalisée dans le cadre de cette exception portera bien sur des produits ou services correspondant aux « attentes légitimes du consommateur ». Il semble ainsi qu'il faille considérer que les « produits et services analogues » sont ceux qui correspondent à une « attente légitime du consommateur ». Il faudra donc se placer du point de vue du consommateur moyen pour apprécier si un nouveau produit ou service est « analogue » à celui qu'il a déjà acheté. Dans la mesure où l'adjectif « analogue » et l'expression « attente légitime du consommateur » ne font l'objet d'aucune définition à caractère juridique, il semble que la notion de « produits ou services analogues » puisse être rapprochée de celle de « produits ou services similaires », et ce, dans la mesure où ces deux notions sont notamment employées indistinctement dans la directive 2002/58/CE[37] fixant le régime de la prospection commerciale. En effet, dans cette directive, il est fait référence à deux reprises à l'exception à la règle du consentement

[36] CNIL, Délibération nº 2011-384, 12 janvier 2012.

[37] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

préalable, à l'article 13.2 et dans le considérant nº 41. Or, si le premier renvoie à la notion de « produits ou services analogues », le second mentionne, quant à lui, les « produits ou services similaires » en indiquant : « [i]l est raisonnable d'autoriser l'entreprise qui […] a obtenu les coordonnées électroniques […] à exploiter ces coordonnées électroniques pour proposer au client des produits et services similaires […]. »[38] De plus, la version anglaise de la directive ne vise, tant dans le considérant nº 41 qu'à l'article 13.2, que les « *similar products and services* »[39].

42. Par conséquent, afin de définir le périmètre de la notion de « produits ou services analogues », il semble légitime de se référer à la notion de « produits ou services similaires », mieux connue en droit luxembourgeois[40], notamment en matière de marques. Si les textes ne définissent pas la notion de « produits ou services similaires », en revanche les juridictions ont eu l'occasion de se prononcer à de nombreuses reprises sur son interprétation. Selon la Cour de justice de l'Union européenne, il convient, pour apprécier la similitude des produits ou services, « de tenir compte de tous les facteurs pertinents qui caractérisent le rapport entre les produits ou services. Ces facteurs incluent, en particulier, leur nature, leur destination, leur utilisation ainsi que leur caractère concurrent ou complémentaire »[41]. La Cour d'appel de Paris a, pour sa part, précisé que sont similaires des produits sur lesquels, « il existe un risque évident de confusion dans l'esprit du public, le consommateur d'attention moyenne […] étant enclin à les confondre, […] étant ajouté que les produits en cause sont destinés à une même clientèle, recherchant un produit similaire »[42]. À titre d'exemple, il a été considéré comme similaires les « services d'édition de revues, livres et maga-

---

38 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, considérant nº 41 : « Within the context of an existing customer relationship, it is reasonable to allow the use of electronic contact details but for the offering of similar products or services […] » et article 13.2 : « Notwithstanding paragraph 1n where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of a sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services […] ».

39 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, considérant nº41.

40 Loi du 16 mai 2006 portant approbation de la Convention Benelux en matière de propriété intellectuelle (marques et dessins ou modèles), signée à La Haye, le 25 janvier 2005, article 2.20.

41 CJCE, 29 septembre 1998, C-39/97, *Canon*.

42 CA Paris, 4e chambre, Section B, 26 janvier 2007 ; nº 05/06034.

zines» et les «émissions radiophoniques»[43]. Ont été également jugés comme similaires, les services «d'organisation de voyages et d'accompagnement des voyageurs» et les «activités culturelles»[44]. Les magistrats ont ainsi considéré que «les services d'accompagnement des voyageurs [...] sont [...] par leur nature et leur finalité des services complémentaires des activités culturelles; qu'il en résulte que ces services peuvent être attribués par le public à une même origine» et ont donc pu affirmer que les services des agences de tourisme sont similaires aux activités culturelles. Par un arrêt du 1er juin 2005[45], la Cour d'appel de Paris s'est prononcée sur la similarité des services d'assurance et des services bancaires dans les termes suivants : «[l]es services bancaires et les services d'assurances peuvent présenter la même finalité, être rendus par les mêmes prestataires et être systématiquement associés dans l'utilisation qu'en fait le consommateur; qu'il en résulte un risque de confusion pour ce dernier, qui les attribuera inévitablement à la même origine; qu'il s'agit donc de produits similaires.» Ainsi, dans l'ensemble, les produits d'assurances et services bancaires peuvent être considérés comme des produits ou services similaires permettant à l'assureur ou à l'établissement bancaire de bénéficier du régime de l'exception de l'article 11 (2) de la loi modifiée du 30 mai 2005 susvisée, et de ne pas ainsi avoir à recueillir le consentement de leur client pour l'envoi de courriers électroniques ou SMS de prospection commerciale.

§ 2. La garantie d'un droit d'opposition effectif et gratuit

43. Il ressort des termes de l'article 11, (2), de la loi susvisée, que les clients disposent du «droit de s'opposer, sans frais et de manière simple», à l'exploitation de leurs coordonnées électroniques.

44. Dans une délibération du 12 janvier 2012, l'autorité française de protection des données (la Commission nationale de l'informatique et des libertés, la CNIL) a sanctionné une entreprise dont le dispositif d'opposition ne répondait pas aux exigences légales d'effectivité et de gratuité :

– tout d'abord, parce que ce dispositif était payant, puisqu'il reposait sur l'envoi d'un SMS adressé au numéro payant mentionné dans le message ou sur un contact téléphonique payant ;
– ensuite, parce que, si le dispositif prévoyait également la possibilité de formuler une opposition au moyen d'un formulaire sur le site internet, celle-ci s'avérait purement théorique, dans la mesure où cette faculté n'était pas mentionnée dans le corps des messages ;

---

43 CA Paris, 25 juin 1999, *PIBD*, 2000, nº 689, III, p. 19.

44 CA Paris, 4e chambre, section B, 14 mars 2003, nº 2002/12264.

45 CA Paris, 4e chambre, Section A, 1 juin 2005, nº 04/21184.

– enfin, parce que, malgré les demandes formulées par certains prospects, leurs coordonnées restaient présentes dans la base de données du « démarcheur ».

45. En d'autres termes, s'il semble que le « démarcheur » ait le choix du mode d'exercice du droit d'opposition qu'il propose à ses prospects, il se doit de veiller, en revanche, à ce que celui-ci soit effectif et gratuit. Les personnes concernées, parfaitement informées de l'existence du dispositif d'opposition, doivent pouvoir ainsi l'utiliser aisément et sans coût, afin que l'envoi des messages de prospection commerciale cesse dès le moment où elles en auraient manifesté la volonté expresse.

Section 2
Le transfert

46. Le constat est simple : on ne peut envisager de globalisation sans d'incalculables transferts de données à caractère personnel de par le monde. De plus en plus d'entreprises collaborent, en effet, avec des partenaires localisés dans différentes parties du globe. La CNPD, qui a enregistré, en 2012, 48 demandes d'autorisation en vue d'un transfert de données vers des pays tiers (c'est-à-dire des pays qui ne sont pas des États membres de l'Union européenne), relève que « le développement des échanges et la mondialisation ont entraîné un accroissement spectaculaire des transferts de données à caractère personnel dans le cadre de projets de centralisation et d'*outsourcing* de la gestion du personnel, de la clientèle ou des fournisseurs, ainsi que lorsqu'elles externalisent leurs activités informatiques »[46]. Bien entendu, le *cloud computing* est ici directement visé…

47. Il convient de noter que seuls les « transferts de données vers des pays tiers » sont spécifiquement encadrés par la loi modifiée du 2 août 2002. Pour les autres, dès lors qu'ils constituent un traitement de données à caractère personnel, ils sont soumis aux règles en vigueur à tout traitement de données.

Sous-section 1
Au sein de l'Union européenne

48. Parce qu'il est nécessairement rattaché à un traitement principal « ayant une finalité plus globale que le simple fait de transférer des données à carac-

[46] CNPD, *Rapport d'activité 2012*, juillet 2013.

tère personnel »[47], un tel transfert fait l'objet d'une formalité dont la nature dépend du traitement principal : notification ou demande d'autorisation.

49. Il appartient, en tout état de cause, au responsable du traitement à l'origine du transfert, de s'assurer notamment que :

– le transfert a une finalité déterminée, explicite et légitime ;
– les données transférées ne seront pas traitées ultérieurement de manière incompatible avec cette finalité ;
– les données transférées sont adéquates, pertinentes et non excessives au regard de la ou des finalités pour lesquelles elles sont transférées ;
– la durée de conservation par l'importateur des données n'est pas excessive.

50. Par ailleurs, si l'importateur des données est un « sous-traitant » au sens de la loi modifiée du 2 août 2002[48], celui-ci ne peut agir que sur « la seule instruction du responsable du traitement »[49], et donc notamment dans les limites prévues par le contrat liant ces deux parties.

Sous-section 2

Hors de l'Union européenne

51. Le principe est posé à l'article 18, (1), de la loi modifiée du 2 août 2002 : « Le transfert vers un pays tiers de données faisant l'objet d'un traitement ou destinées à faire l'objet d'un traitement après leur transfert ne peut avoir lieu que si le pays en question assure un niveau de protection adéquat et moyennant respect des dispositions de la présente loi et de ses règlements d'exécution. » Bien entendu, la loi modifiée du 2 août 2002 prévoit un certain nombre de dérogations.

§ 1. Vers un pays assurant un niveau de protection adéquat

52. En principe, et comme indiqué ci-dessus, les données à caractère personnel ne peuvent être transférées vers un pays situé hors de l'Union européenne que sous réserve que ce pays soit considéré comme ayant un niveau adéquat de protection, c'est-à-dire présentant des garanties pour la protection des données similaires à celles de la directive 95/46 CE.

---

47 CNIL, *Les transferts de données à caractère personnel hors Union européenne*, www.cnil.fr.

48 Loi modifiée du 2 août 2002, article 2, (o). Par « sous-traitant », il faut entendre « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données pour le compte du responsable du traitement ».

49 Loi modifiée du 2 août 2002, article 22, (3).

53. En application de l'article 18, (2), de la loi modifiée du 2 août 2002, il appartient au responsable du traitement d'apprécier le caractère adéquat du niveau de protection offert par un pays tiers « au regard des circonstances relatives au transfert […], notamment la nature des données, la finalité et la durée du ou des traitements envisagés, le pays d'origine et le pays de destination finale, les règles de droit générales et sectorielles en vigueur dans le pays en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées ». En cas de doute, le responsable du traitement se voit reconnaître la faculté d'en informer la CNPD qui appréciera le niveau de protection offert par le pays en question. Lorsque la CNPD (ou la Commission européenne) constate qu'un pays tiers ne dispose pas d'un niveau de protection adéquat, le transfert est « prohibé » en principe, sauf à bénéficier de l'une des dérogations prévues par la loi modifiée du 2 août 2002[50].

54. À ce jour, la législation des pays suivants a été reconnue par la Commission européenne comme offrant une protection suffisante pour qu'un transfert soit réalisé à destination de ceux-ci : Andorre, l'Argentine, le Canada, les îles Féroé, l'île de Man, Guernesey, Jersey, l'Uruguay et la Suisse. Par ailleurs, sont considérées comme assurant un niveau de protection adéquat, les entreprises *Safe Harbor*, c'est-à-dire les entités établies aux États-Unis ayant adhéré aux conditions des accords de la sphère de sécurité conclus entre la Commission européenne et les autorités américaines figurant sur la liste tenue par la Federal Trade Commission[51]. Il convient de relever que seules les sociétés qui relèvent de la compétence de la Federal Trade Commission ou du ministère américain des Transports peuvent participer à la « sphère de sécurité ». Par conséquent, le secteur bancaire tout comme celui des télécommunications y échappent[52].

§ 2. Vers un pays n'assurant pas un niveau de protection adéquat

55. Par dérogation à ce qui précède, l'article 19, (1), de la loi modifiée du 2 août 2002, indique qu'un tel transfert vers un pays n'assurant pas un niveau de protection adéquat peut être réalisé à condition que : « (a) la personne concernée ait donné son consentement au transfert envisagé, ou (b) le transfert soit nécessaire à l'exécution d'un contrat auquel la personne concernée et le responsable du traitement sont parties ou à l'exécution de mesures précon-

---

50 Loi modifiée du 2 août 2002, article 18, (3).

51 CNPD, *Rapport d'activité 2012*, juillet 2013.

52 P. Santer, T. Hoss, « La loi du 2 août 2002 sur la protection des personnes à l'égard du traitement des données à caractère personnel : une nouvelle donnée pour la place financière, ALJB, *Droit bancaire et financier*, avril 2004.

tractuelles prises à la demande de la personne concernée, ou (c) le transfert soit nécessaire à la conclusion ou l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers, ou (d) le transfert soit nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice, ou (e) le transfert soit nécessaire à la sauvegarde de l'intérêt vital de la personne concernée, ou (f) le transfert intervienne depuis un registre public tel que prévu à l'article 12, paragraphe (2) lettre (b) ». Si le transfert est réalisé dans l'une de ces hypothèses, et bien que le transfert soit considéré comme licite, il appartient au responsable du traitement de notifier à la CNPD, à sa demande, un rapport établissant les conditions dans lesquelles il opère ledit transfert[53].

56. En tout état de cause, la CNPD peut, en application de l'article 19, (3), de la loi modifiée du 2 août 2002, autoriser, sur la base d'une demande dûment motivée, un transfert de données vers un pays n'assurant pas un niveau de protection adéquat, si le responsable du traitement offre « des garanties suffisantes au regard de la protection de la vie privée et des libertés des droits fondamentaux des personnes concernées, ainsi que l'exercice des droits correspondants ». À noter qu'en 2012, la majorité des demandes d'autorisation (48 au total, comme en 2011) émanaient d'entreprises du secteur financier et que les pays de destination étaient le plus souvent les États-Unis et l'Inde[54]. Les « garanties suffisantes », qui permettent au responsable du traitement d'obtenir une autorisation de la CNPD, peuvent résulter, en application du même article, de « clauses contractuelles appropriées ».

57. Il peut s'agir notamment des clauses contractuelles types (adoptées par la Commission européenne) signées par l'entité exportatrice de données et l'entité importatrice. Il existe deux catégories de clauses : celles encadrant les transferts de responsable de traitement à responsable de traitement (issues d'une décision de la Commission européenne du 15 juin 2001 : 2001/497/CE, modifiée par la décision de la Commission européenne du 24 décembre 2004 : 2004/915/CE) et celles encadrant les transferts de responsable de traitement à sous-traitant (issues d'une décision de la Commission européenne du 5 février 2010 : 2010/87/UE). Ainsi, la signature de ces clauses contractuelles types est un moyen d'accroître la sécurité juridique des transferts de données, et donc de s'assurer d'une procédure d'autorisation plus rapide.

[53] Loi modifiée du 2 août, article 19, (2).

[54] CNPD, *Rapport d'activité 2012*, juillet 2013.

58. Il peut également s'agir des règles internes d'entreprise (ou *Binding Corporate Rules* ou BCR) adoptées par des entreprises – responsables de traitement – appartenant à un même groupe en vue de constituer un code de conduite interne contraignant en matière de protection des données. Elles constituent ainsi une alternative aux clauses contractuelles types et permettent d'uniformiser les pratiques au sein d'un groupe, mais aussi d'éviter la conclusion d'autant de contrats qu'il existe de transferts au sein d'un groupe. Mais, partant du constat que les outils existants d'encadrement des transferts hors Union européenne n'étaient pas suffisamment adaptés à toutes les situations et notamment d'*outsourcing* (tel que le *cloud computing*), le groupe de travail « Article 29 » propose désormais – depuis le 1er janvier 2013 – le recours aux BCR « sous-traitants ». Cet outil juridique est destiné aux prestataires de services (sous-traitants) effectuant, pour le compte de leurs clients (responsables de traitement), des opérations dont l'exécution de certaines implique des transferts internationaux de données vers d'autres entités de leur groupe. Ainsi, les BCR « sous-traitants » s'analysent également comme un code de conduite interne définissant la politique d'un groupe en matière de transfert de données à caractère personnel, en vue de constituer une sphère de sécurité pour les transferts effectués par un sous-traitant vers d'autres sous-traitants appartenant au même groupe. Cet outil pourra s'avérer fort utile dans le cas d'un contrat conclu entre un client (responsable de traitement) et un fournisseur de services de *cloud computing* (sous-traitant établi sur le territoire de l'Union européenne), pour l'exécution duquel certaines prestations seront réalisées hors de l'Union européenne par d'autres sociétés du même groupe que le fournisseur. En effet, pour le responsable du traitement, un tel document juridique, d'une part, constituera une garantie que les transferts sont réalisés en conformité avec les principes de la directive 95/46/CE et donc des législations nationales ayant transposé celle-ci (à cet égard, les BCR devront être annexées au contrat de sous-traitance), d'autre part, lui permettra d'éviter de conclure autant de contrats qu'il existe de transferts au sein du groupe du sous-traitant et, enfin, lui garantira d'obtenir, de la part des autorités nationales de protection des données, les autorisations de transfert. Pour le sous-traitant (fournisseurs de services de *cloud computing*), les BCR lui permettront d'uniformiser les pratiques relatives à la protection des données au sein du groupe, mais aussi de communiquer sur la politique d'entreprise en matière de protection des données auprès des clients et de leur assurer un niveau de protection satisfaisant.

Chapitre 2
La maîtrise des données

59. La propriété se décrit comme le droit pour une personne d'exercer une complète maîtrise sur une chose[55]. Ce constat amène, dès lors, à s'interroger sur le concept de propriété des données (section 1). Par ailleurs, cette maîtrise, qui est indispensable dans l'optique d'optimiser la protection desdites données, doit être appréhendée au regard des pratiques et problématiques qui sont inhérentes au phénomène de globalisation : le transfert des données (section 2) et leur traitement en masse avec la question de l'archivage électronique (section 3). Enfin, la problématique de la maîtrise des données par une entreprise appelle celle de la maîtrise de son image, avec la question de la gestion de son e-réputation (section 4).

Section 1
La propriété

60. Aucun texte ne consacre, à proprement parler, l'existence d'un droit privatif sur les données en tant que tel, ce qui laisserait supposer qu'il n'existerait pas de droit de propriété sur les données. Ceci ne signifie pas pour autant qu'une certaine maîtrise des données par leurs titulaires est impossible, car des dispositifs juridiques existent.

Sous-section 1
Existe-t-il un droit de propriété ?

61. La propriété est définie par l'article 544 du Code civil comme « le droit de jouir et de disposer des choses, pourvu qu'on n'en fasse pas un usage prohibé par les lois ou par les règlements ou qu'on ne cause un trouble excédant les inconvénients normaux du voisinage rompant l'équilibre entre des droits équivalents ».

62. D'après De Page[56], tout ce qui existe, sauf l'être humain, est une chose. Ainsi, toute chose devient un bien lorsqu'elle s'avère économiquement utile pour les sujets de droit qui vont s'en emparer. Les biens sont donc des choses appropriables.

---

55 Ph. Malaurie, L. Aynes, *Les biens, droit civil*, 4e éd., Defrénois, 2010, no 400.

56 H. De Page, *Traité élémentaire de droit civil belge*, tome 5, 3e éd., 1972, no 531.

63. La loi distingue plusieurs catégories de biens : les biens meubles et immeubles[57] ; les biens corporels et incorporels. La catégorie des biens meubles incorporels appréhende les biens qui n'ont pas de réalité tangible, c'est-à-dire, ceux qui sont immatériels, à l'instar des œuvres de l'esprit, des signes distinctifs, des inventions, etc., mais aussi des données (qu'elles soient à caractère personnel ou non).

64. La loi a expressément consacré le droit de propriété sur certains de ces biens meubles incorporels. C'est le cas notamment des œuvres de l'esprit (par le droit d'auteur), des signes distinctifs (par le droit des marques) et des inventions (par le droit des brevets), pour lesquels le législateur reconnaît expressément un droit de propriété au profit respectivement de l'auteur, du titulaire du signe et de l'inventeur.

65. Dans la mesure où les données paraissent susceptibles d'une appropriation par l'homme, en ce qu'elles se rapportent très souvent à des informations concernant directement ou indirectement une personne physique ou morale, elles seraient donc également susceptibles de faire l'objet d'un droit de propriété. Toutefois, il est difficile de parler de droit de propriété, alors qu'aucun texte ne prévoit expressément de droit privatif en faveur des personnes, « titulaires » de ces données.

66. D'ailleurs, et à titre d'illustration, si une personne physique est titulaire d'un droit au respect de sa vie privée[58], aucun texte n'a jusqu'à récemment expressément reconnu à cette personne un droit de propriété sur les données relevant de sa sphère privée (à l'exception du droit à l'image et du droit à la voix[59]). La loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement de données à caractère personnel, reconnaît bien des droits au profit de la personne concernée par un traitement – droit d'accès, droit de rectification et droit d'opposition –, mais ne consacre pas pour autant un droit de propriété au profit de celle-ci sur « ses » données. Il en va de même pour le responsable du traitement, qui, bien que débiteur de nombreuses obligations sur les données à caractère personnel qu'il traite, ne se voit pas reconnaître un droit de propriété.

---

57 Code civil, article 516 : « Tous les biens sont meubles ou immeubles ».

58 Loi du 11 août 1982 concernant la protection de la vie privée.

59 « Toute personne a sur son image et l'utilisation qui en est faite un droit exclusif et peut s'opposer à une diffusion non autorisée par elle », *Lux*, référés 20 novembre 1978, *Pas.*, 25, 358.

67. Toutefois, il convient de nuancer cette dernière affirmation. On pourrait très bien considérer que le législateur luxembourgeois, en modifiant l'article 567 du Code de commerce par la loi du 9 juillet 2013, reconnaît désormais l'existence d'un droit de propriété sur les données. En effet, l'article 567, alinéa 2, prévoit désormais que « [L]es biens meubles incorporels non fongibles en possession du failli ou détenus par lui peuvent être revendiqués par celui qui les a confiés au failli ou par leur propriétaire ». Cela signifie donc qu'une donnée, bien meuble incorporel, pourrait avoir un « propriétaire ». Il ne s'agit que d'une hypothèse, dans la mesure où le texte susvisé indique aussi que ce droit de revendication appartient au « propriétaire » du bien meuble incorporel, mais également à celui qui l'a confié au prestataire en faillite. Cette question de la titularité des données, qui ne se posait pas tant que les données ne circulaient pas (ou pas autant), est aujourd'hui d'actualité en raison de l'émergence d'une véritable économie des données. Un commerce lucratif s'est bâti autour du commerce de données à caractère personnel.

68. Quoi qu'il en soit, la maîtrise des données peut être assurée grâce à d'autres moyens de protection juridique.

Sous-section 2

Quels moyens juridiques de protection ?

69. Ces moyens juridiques de protection permettant de conserver une certaine maîtrise sur les données sont, d'une part, des dispositifs légaux et, d'autre part, la mise en place d'un cadre contractuel protecteur.

§ 1. Les dispositifs légaux

70. Tout d'abord, la directive 96/9/CE du Parlement européen et du Conseil du 11 mars 1996 est venue conférer au producteur d'une base de données un droit dit *sui generis,* dont l'objet est de protéger l'investissement réalisé pour la constitution de cette base de données. En effet, compte tenu de l'importance des investissements nécessaires pour la réalisation d'une base de données, mais également du développement des nouvelles technologies permettant l'accès au contenu des bases et leur pillage par des tiers, il a été considéré comme indispensable de reconnaître au producteur de bases de données un « droit » sur leur contenu.

71. Il ne s'agit toutefois pas d'un droit de propriété, à proprement parler, sur le contenu de la base, ni d'un droit sur les données contenues dans cette base, mais d'un droit permettant au producteur de s'opposer à l'extraction substantielle de son contenu par un tiers sans son autorisation. Ainsi, en application de

l'article 67 de la loi du 18 avril 2001[60] : « [L]e producteur d'une base de données[61] peut interdire le transfert, permanent ou temporaire, sur un autre support et toute forme de mise à disposition du public, de tout ou partie substantielle de cette base de données, de manière permanente ou temporaire, par quelque moyen et sous quelque forme que ce soit. » Il peut également « interdire l'utilisation répétée et systématique de partie non substantielle du contenu d'une base de données qui serait contraire à l'exploitation normale de cette base de données ou qui causerait un préjudice injustifié à ses intérêts légitimes ».

72. Ensuite, même en l'absence d'investissement substantiel, il est possible de protéger ses données privées (celles qui sont le produit de l'entreprise ou qui relèvent de la sphère privée des individus) par des actions mises en œuvre sur le fondement de la concurrence déloyale et/ou du parasitisme économique (article 1382 du Code civil et/ou loi du 30 juillet 2002 réglementant certaines pratiques commerciales sanctionnant la concurrence déloyale).

73. Il a été notamment jugé qu'une société, en reprenant « sans bourse délier » les données de son concurrent et en se plaçant ainsi dans le sillage de la renommée de ce dernier, a voulu profiter des retombées d'une telle renommée et a commis, en conséquence, un « acte contraire aux usages honnêtes en matière commerciale » qualifié d'« acte de concurrence déloyale »[62].

74. Par ailleurs, il est utile de rappeler que l'action en contrefaçon peut être également envisagée dans l'optique de protéger des données, sous réserve toutefois de démontrer que l'appropriation faite par le tiers porte sur des données qui constituent une œuvre de l'esprit originale, une marque ou encore une invention.

75. À noter également que la loi prévoit la protection des secrets de fabrique[63] et sanctionne certains actes d'espionnage industriel[64].

---

60 Loi du 18 avril 2001 sur les droits d'auteur, des droits voisins et les bases de données.

61 Le producteur est entendu, en application de l'article 67, § 2, de la loi du 18 avril 2001, sur les droits d'auteur, des droits voisins et les bases de données, comme « la personne physique ou morale qui prend l'initiative et assume à titre principal le risque d'effectuer les investissements nécessaires à la création d'une base de données ». Il convient de souligner que, depuis la loi du 2 août 2002, la notion de « banque de données » n'est plus utilisée (voy. Conseil d'État, avis du 6 décembre 2011 sur le projet de loi 6284 portant sur l'exploitation d'une base de données à caractère personnel relative aux élèves, *Doc. parl.*, 6284-5, p. 3).

62 Cour d'appel de Luxembourg, 14 novembre 2007, nº 32297.

63 Code pénal, article 309.

64 Code pénal, article 108.

76. Le droit fondamental à la protection des données à caractère personnel est consacré par la charte des droits fondamentaux de l'Union européenne[65]. Sur le plan national, la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement de données à caractère personnel vise à « protéger les libertés et les droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement de données à caractère personnel ». À ce titre, toute personne dont les données sont susceptibles de faire l'objet d'un traitement (la « personne concernée ») a le droit de s'opposer à ce traitement[66]. La loi modifiée du 2 août 2002 confère, par ailleurs, au responsable de traitements dans ses relations avec les tiers (à l'exception de la personne concernée), une totale maîtrise de ses données. À ce titre, le sous-traitant, qui accède aux données, ne peut les traiter que sur instructions du responsable du traitement et n'a, en aucun cas, la maîtrise desdites données qui reste entre les mains du responsable du traitement[67]. Le projet de loi 6543 sur l'archivage électronique se situe dans la même lignée : le prestataire de services de dématérialisation n'a pas la maîtrise des données et, par exemple, ne peut consentir de sûretés sur les données archivées.

77. Enfin, la loi du 15 juillet 1993 tendant à renforcer la lutte contre la criminalité économique et la fraude informatique confère un autre moyen légal de protection des données en érigeant comme délit notamment l'accès ou le maintien frauduleux de tout ou partie d'un système de traitement automatisé de données. L'entrave au fonctionnement d'un tel système ainsi que la modification des données qu'il contient sont également des actes pénalement répréhensibles[68].

§ 2. Les dispositifs contractuels

78. Lorsque les relations commerciales avec un partenaire supposent un échange de données entre les différentes parties au contrat, une telle mise à disposition et les conditions de leur exploitation doivent être encadrées contractuellement.

79. Dans ce cadre, il est généralement stipulé par le titulaire des données utilisées dans le cadre de l'exécution du contrat qu'il en est le propriétaire et qu'en conséquence il appartient à l'autre partie de se conformer aux instruc-

---

65 Charte des droits fondamentaux de l'Union européenne (2000/C 364/01), article 8 : « Toute personne a le droit à la protection des données à caractère personnel la concernant. »

66 Loi modifiée du 2 août 2002, article 30.

67 Loi modifiée du 2 août 2002, article 21.

68 Code pénal, articles 509-1 et s.

tions spécifiées dans le contrat, en termes de moyens mis en œuvre pour garantir notamment leur confidentialité et leur restitution à l'issue de la relation contractuelle.

80. Il convient de rappeler que l'article 21 de la loi modifiée du 2 août 2002 met à la charge du responsable de traitement l'obligation pour celui-ci de conserver la maîtrise de ses données à caractère personnel dans ses rapports avec son sous-traitant, ce qui l'oblige, dans le contrat conclu avec ce dernier, à spécifier les conditions notamment techniques et juridiques sous lesquelles le prestataire est autorisé à traiter les données.

81. De même, un encadrement contractuel est prévu par cette loi modifiée du 2 août 2002 en ce qui concerne le transfert des données à caractère personnel vers un État non membre de l'Union européenne qui n'assure pas un niveau de protection adéquat[69].

Section 2
Le transfert des données

82. Le recours à l'*outsourcing*, et notamment au *cloud computing* – qui implique nécessairement un transfert des données – suscite bien souvent des craintes du côté des entreprises qui voient dans ces solutions un risque de perte totale ou partielle de la maîtrise de leurs données. La délocalisation des données et l'incertitude sur leur localisation, mais aussi leur indisponibilité et leur réversibilité incertaine sont autant de risques qu'il convient de prendre en considération dans l'optique d'optimiser la maîtrise de ses données.

Sous-section 1
La localisation

83. Comme indiqué précédemment, la globalisation a entraîné une augmentation très significative des flux transfrontières de données. Ainsi, comme l'indique Jean-Philippe Walter dans son rapport réalisé pour le Conseil de l'Europe, « à l'ère de la globalisation et de l'internalisation des échanges, le traitement des données […] ne connaît plus de frontières et la technologie rend de plus en plus facile la dissémination ou la délocalisation des traitements ».

84. Cette délocalisation s'est d'ailleurs accentuée avec la généralisation par les entreprises de l'utilisation de solutions de type *cloud computing*, lesquelles peuvent être définies, sur le plan technique, comme des solutions « de stoc-

[69] Sur ce régime, voy. P. Santer, T. Hoss, *op. cit.*, pp. 404 et s.

kage d'informations sur une ou plusieurs machines (substituables) qui n'ont pas d'attribution fonctionnelle particulière »[70].

85. Ainsi, le *cloud computing* permet une concentration des données sans considération du support, et ce, tout en permettant leur restitution quelle que soit leur localisation. À cet égard, il convient de souligner que, traditionnellement, ces données sont fragmentées et ces fragments sont dupliqués et distribués sur plusieurs serveurs dans plusieurs centres de données (*datacenters*). Il est donc très difficile pour l'entreprise de savoir avec exactitude où se trouve une catégorie de données en particulier. Il convient de noter, toutefois, que certains prestataires offrent des solutions qui proposent une répartition des données (plus exactement des fragments de données) sur plusieurs serveurs, localisés dans un seul et unique centre de données.

86. Le choix doit donc s'opérer en faveur d'un prestataire proposant des garanties en termes de localisation des données. Toutefois, ce choix peut s'avérer parfois compliqué en pratique. En effet, l'insuffisance manifeste de transparence de la part de ces derniers concernant les conditions d'exécution des prestations (et la localisation des serveurs) rend ce choix très difficile par manque d'informations. Par ailleurs, la majorité des offres de c*loud computing* étant standardisées et faisant l'objet d'un contrat d'adhésion, leur négociation est rarement possible.

87. Il n'en demeure pas moins que la connaissance de la localisation des données est indispensable pour l'entreprise, afin de pouvoir mettre le traitement considéré en conformité avec les exigences légales, dans le cas notamment d'un transfert des données vers un pays situé hors de l'Union européenne.

Sous-section 2
La disponibilité

88. N'est plus maître de ses données l'entreprise qui n'y a pas accès à sa convenance. C'est la question de la disponibilité qui est souvent l'objet de discussions et de craintes dans le cadre d'un projet d'*outsourcing*.

89. Cette question de la disponibilité des données est liée à celle de la disponibilité et de la continuité des services. Même si les « pannes » de services de *cloud computing* sont extrêmement rares, elles peuvent être extrêmement préjudiciables lorsqu'elles se produisent. Selon le Syntec informatique, « la

[70] Cigref, *Fondamentaux du* Cloud computing*: le point de vue des grandes entreprises*, mars 2013.

redondance des applications et des données est consubstantielle à l'architecture *Cloud*, ce qui élimine pratiquement les causes d'origine matérielle ». Les interruptions de services seraient donc dues à des « problèmes logiciels ou réseaux, voire à des virus ou à des actes malveillants »[71]. En tout état de cause, une offre de services adéquate complétée d'un *SLAs* (convention de niveaux de services) garantissant un certain niveau de disponibilité constitue un prérequis. L'application de pénalités en cas de non-respect de ces niveaux de services n'est pas, en revanche, systématiquement prévue dans les contrats.

90. La question de la disponibilité des données appelle aussi une autre question : comment se prémunir contre le risque de la perte de données ? La seule réponse à cette question consiste à prévoir un système de réplique (duplication) de celles-ci sur un ou plusieurs autre(s) site(s) avec un engagement de résultat de restauration des données dans des délais contractuellement convenus.

91. Il convient de noter que, dans le secteur financier, la continuité est un aspect à prendre en considération par l'établissement qui envisage de recourir à la sous-traitance (*outsourcing*). L'établissement doit, en effet, prendre toutes « les précautions qui s'imposent afin d'être à même de transférer de manière adéquate les services sous-traités à un autre fournisseur ou de les reprendre en gestion propre, chaque fois que la continuité ou la qualité de la prestation risque d'être compromise »[72]. D'ailleurs, la CSSF rappelait, dans la circulaire 13/554, que les professionnels du secteur financier « doivent conserver le contrôle complet des ressources dont ils sont responsables et de l'accès à ces ressources, en premier lieu pour des raisons de conformité et de gouvernance et, en deuxième lieu, pour protéger les données confidentielles soumises au secret professionnel »[73].

92. C'est l'une des raisons pour lesquelles les services de gestion/d'opération des systèmes informatiques de ces établissements ne peuvent être sous-traités, dès lors qu'il contiennent des données confidentielles lisibles, qu'au Luxembourg et auprès d'un établissement de crédit ou un professionnel financier disposant d'un agrément de PSF de support, ayant le statut d'opérateur de systèmes informatiques primaires de secteur financier ou le statut d'opérateur de systèmes informatiques secondaires et de réseaux de communication du

---

71 Syntec informatique, *Le livre blanc du* cloud computing*, tout ce que devez savoir sur l'informatique dans le nuage*, 2010.

72 Circulaire CSSF 12/552, telle que modifiée par la circulaire CSSF 13/563 du 19 mars 2013, section 7.4.1. (188).

73 Circulaire CSSF 13/554, 7 janvier 2013.

secteur financier[74]. Le sous-traitant peut également être une entité du groupe auquel l'établissement appartient (y compris à l'étranger), mais, dans ce cas, aucune donnée confidentielle lisible concernant des clients ne peut être transférée, sauf consentement éclairé des clients concernés. Les exigences ainsi posées par la CSSF, en matière de maîtrise et de disponibilité des données, rendent pratiquement impossible aux établissements relevant de sa surveillance le recours à des services de *cloud computing*, et notamment lorsque des données relevant de leur clientèle sont concernées.

Sous-section 3
La réversibilité

93. La réversibilité doit permettre à l'entreprise, au terme du contrat, de retrouver la totale maîtrise « physique » de ses données. Cela passe par une restitution desdites données et l'engagement pris par le prestataire de procéder à leur destruction, après restitution.

94. L'outil juridique utilisé pour encadrer ce processus est appelé « plan de réversibilité ». Il doit notamment prévoir les conditions d'exportation des données ainsi que des garanties sur leur portabilité et interopérabilité avec le système du client, voire avec celui des autres fournisseurs de services de *cloud computing*.

95. Cela suppose une attention toute particulière sur le processus proposé par le fournisseur. En effet, si ce dernier s'appuie sur « une technologie de virtualisation exotique ou peu répandue »[75], il existe un risque sérieux que les données ne soient pas convertibles avec une technologie standard. Il s'ensuit un risque de dépendance technologique vis-à-vis du fournisseur de *cloud computing*, c'est-à-dire l'impossibilité pour l'entreprise de changer de prestataire et de solution, sauf à accepter la perte de ses données… Le Syntec informatique reconnaît aisément que la réversibilité « est l'un des problèmes majeurs du *Cloud Computing*, car les clients ne doivent pas être – ou se sentir – captifs d'un nuage »[76].

---

[74] Circulaire CSSF 12/552, telle que modifiée par la circulaire CSSF 13/563 du 19 mars 2013, section 7.4.1. (193).

[75] Syntec informatique, *Le livre blanc du* cloud computing*, tout ce que devez savoir sur l'informatique dans le nuage*, 2010.

[76] Syntec informatique, *Le livre blanc du* cloud computing*, tout ce que devez savoir sur l'informatique dans le nuage*, 2010.

Section 3
L'archivage électronique[77]

96. Par la loi modifiée du 14 août 2000 sur le commerce électronique, le législateur a précisé les règles de preuve pour les contrats conclus par voie électronique. Ainsi, aux termes de l'article 1322-2 du Code civil, un contrat signé par voie électronique vaut comme un original, « lorsqu'il présente des garanties fiables quant au maintien de son intégrité à compter du moment où il a été créé pour la première fois sous sa forme définitive ». Évidemment, l'exigence prescrite par l'article 1325 du Code civil, selon laquelle un acte sous seing privé contenant une convention synallagmatique n'est valable que s'il a été établi en autant d'originaux qu'il y a de parties ayant un intérêt distinct, ne s'applique pas aux contrats revêtus d'une signature électronique. En outre, l'article 18, paragraphe 2 de cette loi du 14 août 2000 précise que le juge ne peut rejeter une signature électronique « au seul motif qu'il ne s'agit pas d'une signature manuscrite, qu'elle ne repose pas sur un certificat qualifié, qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de certification ou qu'elle n'est pas créée par un dispositif sécurisé de création de signatures ». L'acte sous seing privé électronique se voit ainsi reconnaître une valeur équivalente à celui signé manuscritement.

97. Ce qui était ainsi fait pour l'original ne l'était cependant pas pour la copie numérique. La copie s'était toujours vu accorder un rôle mineur dans le Code civil, eu égard au risque d'erreur[78]. Mais « dès lors que la copie gagnait en fiabilité, il devenait possible de lui accorder un plus grand crédit »[79] ; en revanche, plus la fiabilité est grande, plus la découverte de falsification risque de devenir difficile.

98. La dématérialisation d'un original ou d'un acte sous seing privé signé électroniquement et leur conservation ne peuvent s'envisager que si la copie ainsi dématérialisée se voit reconnaître le même rang que l'original dont elle est issue. Or, d'après les auteurs du projet de loi 6543, le cadre législatif actuel ne serait pas adapté à une telle équivalence. D'un côté, le règlement grand-ducal du 22 décembre 1986 pris en exécution des articles 1348 du Code civil et 11 du Code de commerce ne refléterait plus le dernier état de la technologie en la matière. D'autre part, l'article 1333 du Code civil prévoit que, si l'original subsiste, les copies « ne font foi que de ce qui est contenu au titre ou à l'acte » et le juge peut toujours demander la représentation de l'original en cas de discor-

---

77 État au 30 novembre 2013.

78 D. Veaux, M. Oudin, *Jcl. Civil*, art. 1334-1337, § 2, p. 3.

79 *Eod. loc.*

dance avérée entre un original et une copie, ce qui, d'après la Chambre de commerce, obligerait la conservation de documents créés sous forme papier, de manière physique[80]. L'article 1334 de ce Code envisage la situation lorsque l'original n'existe plus. Dans ce cas, les copies peuvent avoir la même valeur probante que l'original « dont elles sont présumées, sauf preuve contraire, être une copie fidèle lorsqu'elles ont été réalisées dans le cadre d'une méthode de gestion régulièrement suivie et qu'elles répondent aux conditions fixées par règlement grand-ducal », à savoir le règlement grand-ducal précité du 22 décembre 1986.

99. Afin de permettre « aux acteurs économiques de profiter pleinement des technologies de l'information »[81] et ainsi contribuer à l'attractivité de la place luxembourgeoise, le gouvernement a déposé le 13 février 2013 un projet de loi numéro 6543 afin d'adapter le cadre législatif actuel que nous venons d'esquisser.

100. Ce projet de loi traite de l'archivage électronique et de la conservation électronique de tout acte sous seing privé et de tout document visé à l'article 16 du Code de commerce, à savoir les documents comptables, les pièces justificatives, la correspondance commerciale et l'inventaire des commerçants, à l'exclusion du bilan et du compte de profits et pertes. Cette exclusion peut *a priori* sembler surprenante au regard notamment de la procédure de dépôt des comptes annuels par voie électronique par le biais de la plate-forme eCDF prévue par règlement grand-ducal du 14 décembre 2011 déterminant la procédure de dépôt de la liasse comptable auprès du gestionnaire du registre de commerce et des sociétés. Dans son avis du 8 octobre 2013, le Conseil d'État s'est interrogé sur les raisons qui ont amené les auteurs du projet de loi à ne pas inclure les documents administratifs dans le champ d'application de la loi en projet et a plaidé pour y inclure « tous les documents et copies dématérialisés, peu importe que ceux-ci relèvent du secteur financier ou commercial ou qu'ils aient été générés dans un autre contexte ».

101. Pour les originaux tombant dans le champ d'application de la loi à venir, une copie, c'est-à-dire « une reproduction fidèle et durable sous forme numérique d'un original » a, en application de l'article 3 du projet de loi 6543, « la même valeur probante que l'original lorsqu'elle a été réalisée dans le cadre d'une méthode de gestion régulièrement suivie qui réponde aux conditions fixées par règlement grand-ducal ». Cet article 3 précise encore que l'ar-

80 *Doc. parl.*, 6543-1, p. 1.

81 *Doc. parl.*, 6543, exposé des motifs, p. 2.

ticle 1333 du Code civil n'est pas applicable, les autres articles sur la preuve continuant de l'être.

102. Si la dématérialisation a été effectuée par un prestataire de services de dématérialisation et de conservation ou par un prestataire de services de dématérialisation (qui sont des professions expressément créées par le projet de loi, mais qui sont réservées aux seules personnes morales, ce qui a amené le Conseil d'État à formuler une opposition formelle sur base de l'article 10*bis* de la Constitution), l'article 5 du projet de loi érige en présomption que la copie répond aux conditions précitées de l'article 3 et est ainsi conforme à l'original. Si une personne n'a pas recours à un tel prestataire, il faudra donc qu'elle démontre, en cas de contestation, que la copie numérique dont elle dispose a été réalisée dans le cadre d'une méthode de gestion régulièrement suivie répondant aux conditions fixées par règlement grand-ducal.

103. La présomption instaurée par l'article 5 semble être une présomption irréfragable, alors qu'*a contrario* l'article 1334 du Code civil fait clairement référence à une présomption simple, en mentionnant la possibilité d'une preuve contraire. Or, dans la mesure où l'erreur, même d'un professionnel, reste toujours possible, la preuve contraire doit être admise. La différence entre la situation où un professionnel est intervenu dans la dématérialisation d'un document original et celle où il n'est pas ainsi intervenu se situe au niveau de la charge de la preuve. Dans le premier cas, visé à l'article 5, il appartient à celui qui soulève la contestation d'en rapporter la preuve. Dans le second, celui de l'article 3, le détenteur de la copie numérique doit prouver que les conditions de l'article 3 ont été remplies. Le Conseil d'État, qui a estimé que les règles de preuve devraient être reprises au Code civil ainsi qu'au Code de commerce et non dans une loi spéciale, a sévèrement critiqué les articles 3 et 5 du projet de loi 6543 alors que « le projet de loi ne propose pas de réponse évidente au problème de la valeur probante d'une copie numérique effectuée à partir d'un original existant en plusieurs exemplaires dont l'exemplaire utilisé pour la copie numérique sera détruit après la confection de celle-ci, lorsqu'un ou plusieurs des exemplaires subsistants de l'original feraient par la suite l'objet d'une falsification. Un problème analogue peut se poser, dans l'hypothèse où la copie numérique est confectionnée à partir d'un original qui a été illicitement modifié avant sa dématérialisation. De l'avis du Conseil d'État, il faudra, dans ces conditions, éviter toute hiérarchie entre la valeur probante d'un original, qu'il existe sous forme de document papier ou à l'état numérique, et celle des copies numériques, qui en ont été faites selon les règles légales en projet par un prestataire de services certifié ».

104. Il faudra cependant aussi tenir compte qu'en matière commerciale, la preuve est libre. Il appartient au juge d'utiliser son pouvoir souverain pour apprécier les éléments de preuve qui lui sont déférés, y compris en reconnaissant une valeur probante à une copie dont rien ne fait douter de sa fidélité à l'original[82].

105. Un tel prestataire de services de dématérialisation ou un prestataire de services de dématérialisation et de conservation est une personne morale qui doit être accréditée par un certificateur accrédité par l'organisme luxembourgeois d'accréditation et de l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS)[83]. La question, d'ailleurs relevée par le Conseil d'État dans son avis du 8 octobre 2013 et qui n'a pas été traitée dans le projet de loi 6543, est aussi de savoir si des copies dématérialisées ont été effectuées par des prestataires établis dans un autre État membre de l'Union européenne, alors que, selon la Haute Corporation, il serait difficilement justifiable au regard des principes du marché intérieur de faire une différence selon que le prestataire est établi ou non au Luxembourg.

106. Le projet de loi 6543, en ajoutant les nouveaux articles 29-5 et 29-6 à la loi modifiée du 5 avril 1993 relative au secteur financier, crée une nouvelle catégorie de PSF de support. En effet, si le prestataire procède à la dématérialisation ou la conservation de documents pour le compte d'établissements de crédit, de PSF, d'établissements de paiement, d'établissements de monnaie électronique, des OPC, des FIS, des SICAR, des fonds de pension, des organismes de titrisation agréés, des entreprises d'assurance ou de réassurance, de droit étranger ou de droit luxembourgeois, il doit en outre être agréé par le ministre des Finances[84]. D'après le commentaire des articles[85], si le prestataire en question effectue l'activité de dématérialisation et celle de stockage, deux agréments sont nécessaires.

107. Le projet de loi a, de manière incomplète, donc insuffisante, abordé la question du sort des documents dématérialisés en application du règlement grand-ducal du 22 décembre 1986 avant l'entrée en vigueur de la loi qui sera issue du projet de loi 6543. L'article 15 du projet de loi n'aborde cette question que du point de vue du gestionnaire du registre du commerce et des sociétés, mais encore, uniquement à condition qu'une signature électronique au sens de l'article 1322-1 du Code civil intervienne dans un délai d'un an à comp-

---

82 Cour, 29 octobre 2003, *Pas.*, 32, 597.

83 Voy. à propos de la réorganisation de l'ILNAS, le projet de loi 6315.

84 Articles 29-5 et 29-6 nouveaux insérés dans la loi modifiée du 5 avril 1993 relative au secteur financier.

85 *Doc. parl.*, 6543, p. 14.

ter de l'entrée en vigueur de la loi en projet. Cette disposition soulève deux problèmes auxquels le projet de loi n'apporte aucune réponse. En premier lieu, qu'en est-il des documents conservés sous forme numérique par d'autres administrations ou établissements publics ou par les acteurs du secteur privé ? Certes, le gestionnaire du registre du commerce et des sociétés a dû procéder à des dématérialisations ou a reçu des documents déjà sous forme numérique. Mais il n'est pas le seul dans cette situation, ce qui a entraîné une opposition formelle de la part du Conseil d'État. Pourquoi privilégier le gestionnaire de ce registre, alors que d'autres ont bien pu avoir mis en place une infrastructure répondant aux critères du règlement grand-ducal du 22 décembre 1986 ? En second lieu, quel que soit le champ d'application personnel de l'article 15 du projet de loi 6543, quelle conclusion en tirer au regard de la valeur probante des copies ainsi numérisées ? En l'absence de certification par un prestataire de services de dématérialisation et/ou de conservation, est-ce que les copies en question peuvent bénéficier de la présomption de conformité de l'article 5 du projet de loi ? La réponse à cette question reste en l'état ouverte.

108. Les auteurs du projet de loi se devaient de régler la question des conséquences du principe selon lequel le prestataire de services de dématérialisation n'est pas propriétaire des données dont il a fait des copies numériques ou qu'il conserve pour les détenteurs. Ainsi, le prestataire ne peut constituer aucune sûreté ni donner en garantie de quelque manière que ce soit les matériels ou supports sur lesquels les copies sont conservées[86]. Il s'agit là d'une interdiction générale ne souffrant aucune exception.

109. De même, le projet de loi vise à régler le sort des données numérisées lorsque le prestataire de services de dématérialisation cesse ses activités ou fait faillite ou est liquidé[87]. Dans ce dernier cas, le détenteur est en droit de réclamer la restitution de ses copies et originaux ainsi que toute information relative à la dématérialisation à la conservation des copies. Ces données et informations qui appartiennent au détenteur échappent au concours avec les créanciers. Cependant, le curateur, le commissaire à la gestion contrôlée ou le liquidateur gardent un droit de rétention pour les services non encore payés par le détenteur en question.

110. La dématérialisation de documents, donc le fait de les « transformer » en données numérisées, permet certes leur conservation dans de meilleures conditions, mais favorise également leur transfert et leur insertion dans la globalisation alors que, par définition, il est plus aisé de transférer des données

86 Projet de loi 6543, article 11.

87 Projet de loi 6543, article 12.

à un, voire à plusieurs destinataires, que de leur envoyer des documents sur support papier. Ainsi, l'archivage électronique se situe dans le cadre de la globalisation esquissé précédemment.

Section 4
La gestion de l'image sur internet

111. La maîtrise des données concernant une personne physique ou morale permet notamment à celle-ci de maîtriser son image et sa réputation. Internet étant considéré comme « le carrefour central de l'influence »[88], la gestion de la réputation numérique est devenue pour l'entreprise un enjeu majeur, et ce, en vue d'y créer et d'y développer une influence positive maîtrisée.

112. La gestion de l'« e-réputation », en d'autres termes l'image que les internautes peuvent se faire d'une personne ou de ses produits et services à partir des informations trouvées sur internet et notamment sur les médias sociaux[89], s'inscrit principalement à travers les actions suivantes : la construction de l'image sur internet (sous-section 1) et la gestion de l'image négative (sous-section 2).

Sous-section 1
La construction de l'image

§ 1. Une présence positive loyale

113. La construction de l'image sur internet passe principalement par l'accroissement de la présence positive. La mise en ligne d'un site internet, lequel constitue un support d'informations maîtrisé pour l'entreprise, y contribue, à condition toutefois de recourir à des techniques de référencement dans l'optique d'optimiser la visibilité dudit site par l'amélioration de son positionnement.

114. Par ailleurs, et afin de diffuser une image attractive de ses produits et services, l'entreprise peut également être tentée d'intervenir sur les nombreux sites ou forums dédiés aux avis de consommateurs. Si une telle pratique n'est pas répréhensible en soi, le message de l'entreprise ne doit en aucun cas être trompeur et être présenté faussement comme le reflet de l'opinion de consommateurs. En d'autres termes, si l'entreprise peut encourager

88 E. Filias et A. Villeneuve, *Influence et réputation à l'heure d'internet*, Éditions Ellipses.

89 Le terme de média social désigne tous ces outils du Web 2. 0 qui permettent d'entrer en relation et de partager du contenu avec les autres internautes. Les réseaux sociaux virtuels, dont les plus connus sont Facebook, LinkedIn et Viadeo, sont une sous-partie de ce grand ensemble d'outils que sont les médias sociaux.

en interne les messages spontanés, elle doit écarter tous ceux qui seraient de nature trompeuse.

115. D'ailleurs, des études récentes révèlent que les internautes sont de plus en plus méfiants sur la qualité et la sincérité de l'information mise en ligne et se montrent extrêmement réservés sur la question de la fiabilité des prétendus « avis de consommateurs » publiés sur les sites internet des professionnels. Selon le 3e baromètre de Testntrust, trois quarts des internautes pensent que parmi les avis de consommateurs se cachent de faux avis…[90] Cette pratique des faux avis de consommateurs n'est pas nouvelle, mais la prise de conscience des internautes sur les abus auxquels se livrent certains professionnels a eu pour effet d'affaiblir sensiblement la confiance.

116. Parce que la confiance et la qualité de service sont indispensables dans l'optique de créer et de développer une influence positive sur le web, certains acteurs se sont mobilisés pour que soient édictés, dans le cadre d'une norme, des « principes et exigences portant sur les processus de collecte, modération et restitution des avis en ligne de consommateurs ». Il en est résulté la norme française Afnor NF Z 74-501, publiée le 4 juillet 2013.

117. Cette norme a pour objet d'assurer une primauté à la fraîcheur des avis et à la transparence des méthodes, au titre des 3 étapes de traitement :

– la collecte des avis, qui doit reposer notamment sur : l'identification de l'auteur de l'avis ; l'engagement de l'auteur à avoir vécu l'expérience de consommation décrite ; la nécessité de pouvoir contacter l'auteur ; l'interdiction d'acheter des avis ; la nécessité de vérifier l'expérience de consommation ;
– la modération des avis, qui suppose principalement : une réelle transparence des règles de modération dans les conditions générales d'utilisation du site internet ; une impossibilité de modifier les avis en ligne ; l'exigence d'une modération *a priori* des avis (de manière automatique ou humaine) ; l'exigence d'une homogénéité dans le processus de modération ;
– la restitution et la publication des avis, qui impliquent notamment : le respect d'un ordre chronologique, du plus récent au plus ancien ; l'affichage de l'intégralité des avis ; le respect d'un délai maximum de publication à compter de l'émission par le consommateur de son avis.

118. Cette norme contribue, selon l'AFNOR, à « la définition de repères de confiance » pour les internautes.

---

90 http://www.testntrust.fr/

119. Tout professionnel implanté au Luxembourg se voit reconnaître la faculté de demander à obtenir une certification sur la base de cette norme. Il peut également, s'il respecte les principes et exigences susvisés, s'autodéclarer respecter cette norme. En tout état de cause, à l'heure de la globalisation, une norme internationale, dans le cadre de l'organisation internationale de normalisation (ISO) serait évidemment souhaitable.

§ 2. Une présence positive sécurisée

120. Construire une identité numérique, c'est aussi et surtout contrôler son image sur internet pour créer l'influence recherchée. C'est pourquoi, lorsqu'une entreprise décide d'investir dans le développement de son image, elle doit veiller à ce que l'information qu'elle véhicule ne puisse pas être altérée. Pour ce faire, elle doit s'assurer que les accès aux divers comptes de l'entreprise, notamment sur les réseaux sociaux, soient sécurisés, au risque de voir de fausses informations diffusées.

Sous-section 2
La gestion de l'image négative

§ 1. La surveillance

121. La prévention ne permet pas d'éliminer tout risque de publication de contenus négatifs sur internet. C'est pourquoi la mise en place d'une politique de gestion de l'image suppose également des actions de surveillance. En effet, la veille numérique doit permettre à l'entreprise de se renseigner sur l'information qui est véhiculée sur internet. Pour ce faire, l'entreprise dispose de multiples outils logiciels qui permettent de procéder à des recherches exclusivement sur des blogs, qui récupèrent les derniers *tweets* sur le service de *micrologging* Twitter, qui identifient les nouvelles pages indexées pour la ou les requêtes choisies. À l'aide de ces outils, l'entreprise peut détecter de l'information, qui peut être positive pour son image…comme négative. Dans ce cas, l'information n'est pas nécessairement illicite, et une réponse n'est pas toujours adaptée.

§ 2. La qualification juridique du contenu

122. Le principe reste, y compris sur internet, celui de la liberté d'expression[91]. L'entreprise doit donc accepter que des internautes expriment leurs opinions sur ses produits et services, sa politique *marketing* ou encore sa

[91] Loi du 8 août 2004 sur la liberté d'expression dans les médias, article 1er.

gestion des ressources humaines. Des affaires anciennes, qui avaient défrayé la chronique, montrent qu'il peut être parfois très compliqué pour une entreprise de faire cesser certaines pratiques pourtant particulièrement nuisibles. C'est ainsi notamment le cas de la société Danone qui n'était pas parvenue à faire interdire l'usage par une association des noms de domaines « jeboycottedanone.net » et « jeboycottedanone.com », et ce, au motif que cet usage s'inscrivait « dans le cadre d'un strict exercice de [la] liberté d'expression et dans le respect des droits »[92].

123. Il ressort de ce qui précède qu'un contenu, aussi négatif soit-il, n'est pas nécessairement illicite. Sa publication peut donc être parfaitement réalisée dès lors qu'elle s'inscrit dans le prolongement du principe de la liberté d'expression. En revanche, ce principe tombe si l'entreprise victime d'un tel contenu démontre qu'il est illicite parce que sa publication est abusive, réalisée en violation de ses droits ou encore d'un engagement contractuel.

124. Un contenu négatif peut être qualifié d'illicite s'il porte atteinte à la personne ou à ses produits. Il en est ainsi notamment des propos injurieux[93] et diffamatoires[94], qu'ils soient dirigés contre la personne morale – l'entreprise – ou contre des personnes physiques – ses collaborateurs et dirigeants.

125. La publication sur internet d'une information en violation d'une obligation de confidentialité est illicite et engage la responsabilité de son auteur, et ce, quelle que soit la nature de cette information. Un tel manquement aux dispositions d'un contrat de travail –mais aussi en violation de l'obligation de loyauté à laquelle tout salarié est tenu à l'égard de son employeur – constitue une faute pouvant justifier le licenciement du collaborateur indélicat[95].

§ 3. Quelles actions ?

126. L'image de l'entreprise se construit notamment à partir des réponses apportées par celle-ci, à la suite de la publication d'informations la concernant. Mais ses réponses peuvent également avoir un effet négatif et créer un *buzz* autour de cette publication. Il appartient ainsi à l'entreprise de juger de l'opportunité de réagir sur le contenu d'une publication, étant précisé qu'il est

---

92 CA Paris, 4e ch., section A, 30 avril 2003, *Olivier M., Réseau Voltaire c. Compagnie Gervais Danone*. Voy. également, dans le même sens, l'affaire *Greenpeace*: Cass., 1re civ., 8 avril 2008, *Greenpeace France et New Zealand c. SPCEA*.

93 Code pénal, article 448.

94 Code pénal, articles 443 et s.

95 CA Reims, 24 octobre 2012, nº 11/01249; CA Rouen, 15 novembre 2011, nº 11/01827; CPH Boulogne-Billancourt, 19 novembre 2010, nº 10/00853.

parfois préférable de garder le silence et de ne pas entamer le dialogue sur un événement anodin afin de ne pas lui donner une publicité plus importante.

127. En tout état de cause, et en cas de volonté pour l'entreprise de réagir à un contenu publié sur internet dans lequel elle est nommée ou désignée, elle peut exercer son droit de réponse[96], et ce, quel que soit le contenu en cause (licite ou illicite). En effet, en application de l'article 36 de la loi modifiée du 8 juin 2004 sur la liberté d'expression dans les médias : « Sans préjudice des autres voies de droit, toute personne physique ou morale, toute association de fait ou tout corps constitué, cité nominativement ou implicitement désigné dans une publication périodique, a le droit de requérir la diffusion gratuite d'une réponse. » La demande doit être adressée alors par envoi recommandé avec avis de réception à l'éditeur « au plus tard le quatre-vingt-dixième jour qui suit la date de la diffusion ». En cas de refus non justifié de ce dernier, en application de l'article 46 de la même loi, l'entreprise peut demander au président du tribunal d'arrondissement d'« ordonner la diffusion d'une réponse dans la publication concernée, dans un délai et selon les modalités qu'il détermine ».

128. L'entreprise peut aussi utiliser les voies de droit traditionnelles pour obtenir le retrait d'un contenu illicite, et notamment la procédure du référé, prévue à l'article 933 du Nouveau Code de procédure civile, qui prévoit que « [L]e président, ou le juge qui le remplace, peut toujours prescrire en référé les mesures conservatoires ou de remise en état qui s'imposent, soit pour prévenir un dommage imminent, soit pour faire cesser un trouble manifestement illicite […] ».

Chapitre 3
La sécurité et la confidentialité des données

129. Protéger ses données, c'est en garantir la sécurité et la confidentialité. Il s'agit d'un prérequis indispensable pour l'entreprise qui entend protéger son patrimoine « informationnel ». Il s'agit également d'une obligation légale (section 1). En tout état de cause, l'entreprise ne pourra pleinement assurer la sécurité et la confidentialité de ses données que si elle se livre au préalable à une analyse des risques (section 2).

96 Loi du 8 août 2004 sur la liberté d'expression dans les médias, articles 36 et s.

Section 1
Les obligations légales

130. Cette obligation légale trouve sa source principalement dans la loi modifiée du 2 août 2002 applicable en matière de traitements de données à caractère personnel. Pour les établissements du secteur financier, le référentiel légal et réglementaire doit être complété par la loi du 5 avril 1993 et les circulaires CSSF.

Sous-section 1
La loi modifiée du 2 août 2002

131. Malgré l'utilisation, dans le langage courant, des termes génériques de « protection des données » (tout comme *data protection* en anglais et *Datenschutz* en allemand), qui semblent attirer l'attention sur le fait qu'il s'agit de protéger des données à caractère personnel, l'objectif de la loi modifiée du 2 août 2002 est de protéger les personnes dont les données sont traitées contre des traitements abusifs ou illégitimes[97]. Ainsi, cette loi a fixé les conditions dans lesquelles un traitement de données à caractère personnel peut avoir lieu.

132. Tout naturellement, elle a également imposé au responsable du traitement une obligation de sécurité et de confidentialité qu'elle aborde cependant non seulement du point de vue de la protection de la personne concernée, mais aussi sous l'angle de la protection des données elles-mêmes, donc aussi de la protection des intérêts du responsable du traitement. Celui-ci « doit mettre en œuvre toutes les mesures techniques et d'organisation appropriées pour assurer la protection des données qu'il traite contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite »[98]. Les mesures de sécurité techniques et d'organisation relatives aux traitements, dont l'article 23 de la loi énumère un certain nombre de mesures de sécurité particulières[99], s'imposent tant au responsable du traitement qu'aux sous-traitants qui ne peuvent agir que sur instruction du responsable du traitement et qui sont liés au responsable du traitement par « un contrat ou un acte juridique consigné par écrit »[100]. Ces mesures doivent être communiquées à la

---

97 *Doc. parl.*, 4735-13, p. 6.

98 Loi du 2 août 2002, article 22, § 1.

99 Contrôle à l'entrée des installations, contrôle des supports, contrôle de la mémoire, contrôle de l'utilisation, contrôle de l'accès, etc.

100 Loi du 2 août 2002, article 22, § 3.

CNPD dans le cadre d'une procédure de notification ou d'autorisation d'un traitement.

133. La loi modifiée du 2 août 2002 fixe ainsi le cadre général de sécurité et de confidentialité dans lequel les traitements peuvent être mis en œuvre soit par le responsable du traitement, soit par les personnes qui effectuent ces traitements pour son compte (les sous-traitants).

134. Toute donnée à caractère personnel doit être soumise à des mesures de sécurité et de confidentialité, quel que soit le contenu qu'elle renferme. Cependant, ce contenu déterminera le niveau de sécurité et de confidentialité à mettre en place. En effet, l'article 22 de la loi modifiée du 2 août 2002 vise des mesures techniques et une organisation « appropriée ». L'article 23 relatif aux mesures de sécurité particulières fixe les critères dont le responsable du traitement doit tenir compte : il s'agit du risque d'atteinte à la vie privée, de l'état de l'art, mais aussi, et de manière plus surprenante, des coûts liés à la mise en œuvre des mesures de sécurité.

135. S'agissant de protéger la personne concernée, il est évident que les mesures de sécurité et d'organisation soient proportionnelles au risque d'atteinte au droit à la vie privée. Si une donnée est soumise à un secret professionnel en application d'une disposition légale, le plus haut niveau de sécurité doit être mis en place.

136. Bien qu'expressément mentionnés à l'article 23 de la loi modifiée du 2 août 2002, les coûts de mise en œuvre des mesures de sécurité et de confidentialité ne doivent pas être avancés pour justifier réduire le niveau de sécurité et de confidentialité en présence d'un risque d'atteinte à la vie privée. Ils représentent certes un élément protégeant les intérêts du responsable du traitement, mais ils doivent toujours être considérés comme secondaires par rapport à l'atteinte à la vie privée, qui est un droit reconnu par la Constitution et la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Plus ce risque d'atteinte à la vie privée est grand au regard de la nature des données traitées, notamment en présence de données soumises à un secret d'origine légal, plus le critère des coûts de mise en œuvre sera insignifiant.

Sous-section 2

La loi 5 avril 1993 et les circulaires CSSF

137. En ce qui concerne le secteur financier, l'obligation de sécurité et de confidentialité imposée par la loi modifiée du 2 août 2002 a été précisée par la

CSSF dans un certain nombre de circulaires. Le principe sous-jacent est que le PSF – responsable du traitement – doit garder la maîtrise des données qu'il traite[101], et cette maîtrise est l'un des éléments composant l'administration centrale que tout PSF doit avoir au Luxembourg en application de la loi modifiée du 5 avril 1993 relative au secteur financier. Ainsi, la circulaire CSSF 12/552 telle que modifiée par la circulaire CSSF 13/563 sur l'administration centrale, la gouvernance interne et la gestion des risques des établissements de crédit, entreprises d'investissement et professionnels opérant des opérations de prêt indique que « le centre administratif comprend en particulier une bonne organisation administrative, comptable et informatique »[102]. Les établissements de crédit et entreprises d'investissement de droit luxembourgeois ainsi que les succursales luxembourgeoises de tels établissements et entreprises dont l'origine se situe en dehors de l'Espace économique européen sont obligés d'avoir un membre du personnel responsable pour la fonction informatique (dénommé « *IT Officer* ») et un autre pour la sécurité des systèmes d'informations (dénommé « *Information Security Officer* » ou « Responsable de la Sécurité des Systèmes d'Informations (RSSI) »). Pour des établissements de taille réduite, une personne de la direction autorisée peut assumer la responsabilité de « *IT Officer* ») ou de RSSI, voire même des deux ensemble. Cette personne peut alors se faire assister d'une expertise externe[103].

138. Le RSSI « est la personne chargée de l'organisation et du pilotage de la sécurité de l'information, c'est-à-dire la protection de l'information »[104]. La protection de l'information est certes plus large que la seule protection des données à caractère personnel traitées par l'établissement de crédit ou l'entreprise d'investissement, mais celle-ci constitue le cœur de la protection de l'information. Il n'a pas de tâche opérationnelle et pourra, en fonction de la taille de l'établissement et de son positionnement dans la hiérarchie, être dispensé de la mise en œuvre opérationnelle des actions de sécurité. Il s'agit en quelque sorte d'un chargé de la protection des données prévu à l'article 40 de la loi modifiée du 2 août 2002.

139. Le RSSI doit analyser les risques liés à l'information, déterminer les moyens organisationnels, techniques, juridiques et humains en vue d'assurer la protection de l'information, en contrôler non seulement la mise en place, mais aussi leur efficacité et établir des plans d'action pour améliorer cette

---

101 Voy. sur la maîtrise des données, §§ 60 et s. ci-dessus.

102 Circulaire CSSF 12/552, § 7.

103 Circulaire CSSF 12/552, §§ 86 et 87.

104 Circulaire CSSF 12/552, § 86.

protection. Il doit rapporter tout problème « exceptionnel » « au plus haut de la hiérarchie, y compris le conseil d'administration » suivant un « mécanisme d'escalade ».

140. La circulaire modifiée CSSF 12/552 exige aussi que la sécurité et la confidentialité des données soient assurées en permanence en cas de sous-traitance informatique[105], car c'est lorsque des données, que ce soient des données couvertes par le secret bancaire ou des données concernant le personnel ou l'établissement lui-même, quittent le giron de cet établissement, que ce soit physiquement ou virtuellement par l'octroi de codes ou droits d'accès, que le risque d'atteinte à la vie privée, de violation d'un secret légalement protégé (secret bancaire, secret médical, secret d'affaires) et de violation de la loi du 2 août 2002 s'accroît. Comme pour la fonction informatique, le mot d'ordre est la maîtrise de l'information : l'établissement, responsable du traitement, ne doit pas être tributaire du sous-traitant et « la confidentialité des données doit être garantie en permanence, sauf consentement explicite du client ou du propriétaire des données ou de son représentant, donné sur base d'un avis éclairé concernant l'intérêt de cette sous-traitance, la spécificité de la finalité recherchée, du contenu de l'information transmise, du destinataire et de la localisation, ainsi que de la durée dans le temps »[106].

141. La directive 95/46/CE, que la loi modifiée du 2 août 2002 a transposée, visait, dans son intitulé, tant la protection des personnes à l'égard des traitements de leurs données à caractère personnel que la libre circulation de ces mêmes données au sein de l'Union européenne.

142. À l'instar de la sous-traitance, le transfert international de données à caractère personnel pose un risque en termes de confidentialité et de sécurité du fait de la multiplication des intervenants. Le responsable du traitement, du moins le responsable du traitement initial, si l'importateur peut également être considéré comme un responsable du traitement ou un coresponsable du traitement, perd la maîtrise des données.

143. Il arrive fréquemment que les données à caractère personnel traitées par les sociétés d'un même groupe soient regroupées dans une société pour des raisons d'organisation et de coûts. Se basant sur la « maîtrise des données », la circulaire CSSF 13/554 du 7 janvier 2013 rappelle que les PSF doivent conser-

[105] Circulaire CSSF 12/552, §§ 181 et s.

[106] Circulaire CSSF 12/552, § 182.

ver le contrôle des outils permettant de gérer les droits d'accès aux ressources informatiques et d'administrer ces dernières[107].

144. La note technique annexée à cette circulaire énumère les obligations des PSF en la matière. Ainsi si un PSF veut ou doit être impliqué dans un système centralisé des outils de gestion de droits d'accès au sein d'un groupe, une demande détaillée doit être soumise à la CSSF. Le requérant devra démontrer qu'il gardera toujours le contrôle de ces outils, notamment une ségrégation des outils et des règles d'utilisation internes rédigées en termes clairs pour des non-initiés[108]. Tout changement à cette politique doit être autorisé par le PSF avant sa mise en vigueur (contrôle préventif). Un contrôle dit « correctif » par le PSF ne sera pas considéré comme suffisant et ne doit être utilisé qu'en cas de solution d'urgence en cas d'échec du contrôle préventif. Le PSF ou un PSF de support en cas de sous-traitance doit avoir le contrôle des outils d'accès et en assurer la sécurité. La situation doit faire l'objet d'un rapport d'évaluation annuel et les outils d'accès doivent être contrôlés périodiquement. Les règles d'utilisation peuvent être calquées sur celles applicables au sein du groupe en question, mais devront toujours se conformer aux règles techniques annexées à la circulaire CSSF 13/554.

145. La circulaire CSSF 13/554 précise que ce contrôle doit avoir lieu « en premier lieu pour des raisons de conformité et de gouvernance et, en deuxième lieu, pour protéger les données confidentielles soumises au secret professionnel ». Il ne faudrait pas comprendre ce passage comme instituant un ordre hiérarchique, c'est-à-dire que les raisons de conformité et de gouvernance « vaudraient » plus que la protection des données confidentielles, mais plutôt sous l'angle des compétences de la CSSF, dans la mesure où le contrôle de l'administration centrale d'un PSF relève de sa compétence, alors que le respect des règles relatives à la protection des données a été attribué à la CNPD.

146. En liant la confidentialité des données et leur protection à l'organisation interne du PSF, la CSSF pourrait empiéter sur la compétence de la CNPD : le contrôle du respect des obligations de sécurité de la loi modifiée du 2 août 2002 par des PSF relève aussi de la CNPD. Les PSF sont ainsi soumis à des compétences concurrentes de deux établissements publics et, comme dans toute matière où existent des compétences concurrentes, il est à espérer que les politiques poursuivies par ces établissements publics ne divergent pas.

---

[107] Circulaire CSSF 13/554 concernant l'évolution de l'usage et de la maîtrise des outils de gestion des ressources informatiques et de gestion des accès à ces ressources

[108] « [t]ext document written in such a way that people who are not AT specialists – as the FI [pour : Financial Institution] management – are able to understand, discuss and finally approve ».

Remplir les obligations de l'un tout en se faisant sanctionner par l'autre est contre-productif.

Section 2
L'analyse et la gestion des risques

147. L'analyse des risques – comme préalable indispensable dans le choix des mesures de sécurité et de confidentialité que l'entreprise doit mettre en œuvre pour neutraliser un risque – semble s'imposer progressivement. Reste à définir la méthode d'analyse et à mettre en œuvre (ou à faire mettre en œuvre) les mesures identifiées.

Sous-section 1
Une exigence nouvelle ?

148. L'une des principales conclusions tirées de l'avis 05/2012 du groupe de travail « Article 29 » sur le *cloud computing*[109] est que « les entreprises et les administrations qui souhaitent recourir à l'informatique en nuage devraient, dans un premier temps, procéder à une analyse de risques rigoureuse et exhaustive ». Dans sa recommandation de juin 2012 également consacrée au *cloud computing*, la CNIL va dans le même sens, en indiquant que la conduite d'une analyse des risques est essentielle pour être en mesure « de définir les mesures de sécurité appropriée à exiger du prestataire ou à mettre en œuvre au sein de l'entreprise »[110].

149. L'analyse des risques, comme préalable à la mise en œuvre d'un traitement, semble donc s'imposer progressivement. D'ailleurs, la proposition de règlement 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 du 25 janvier 2012 précise qu'« afin de préserver la sécurité et de prévenir tout traitement contraire au présent règlement, il importe que le responsable du traitement ou le sous-traitant évalue les risques inhérents au traitement et prenne des mesures pour les atténuer »[111]. Ces mesures devraient ainsi assurer « un niveau de sécurité approprié compte tenu, d'une part, de l'état de la tech-

[109] Groupe de travail « Article 29 », *Avis 05/2012 sur l'informatique en nuage*, 1er juillet 2012.

[110] CNIL, *Recommandations pour les entreprises qui envisagent de souscrire à des services de* Cloud computing, 25 juin 2012.

[111] Proposition de règlement 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, 25 janvier 2012, considérant (66).

nique et de leur coût de mise en œuvre, et, d'autre part, des risques présentés par les traitements et de la nature des données à protéger ».

150. Cette évaluation des risques est également une action que le responsable du traitement devra accomplir au titre de l'« analyse d'impact relative à la protection des données », telle que visée à l'article 33 de la proposition de règlement susvisée. En effet, dans l'optique de supprimer l'obligation générale de notification – « qui génère une charge administrative et financière, sans pour autant avoir véritablement amélioré la protection des données »[112] –, il est prévu que le responsable du traitement réalise une analyse d'impact relative à la protection des données, préalablement à la mise en œuvre de certains traitements, c'est-à-dire ceux présentant « des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités »[113]. Cette analyse contiendrait ainsi une description générale du traitement envisagé, une évaluation des risques pour les droits et libertés des personnes concernées, les mesures envisagées pour faire face à ces risques, les garanties, les mesures de sécurité et les mécanismes visant à assurer la protection des données.

151. Enfin, il convient de souligner que, dans le secteur financier, l'analyse des risques portant sur les données est également prévue par les textes. En effet, la circulaire CSSF 12/552, telle que modifiée par la circulaire CSSF 13/563, prévoit que le RSSI – responsable de l'organisation et du pilotage de la sécurité de l'information – est notamment chargé de la « gestion de l'analyse des risques liés à l'information ». Dans ce cadre, il lui appartient de définir les moyens organisationnels, techniques, juridiques et humains requis, d'assurer le contrôle de leur mise en place et de leur efficacité ainsi que de concevoir un ou plusieurs plans d'action visant à l'amélioration de la couverture des risques[114]. Reste à déterminer la méthode d'analyse des risques la plus efficace et la plus accessible pour l'entreprise…

---

[112] Proposition de règlement 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, 25 janvier 2012, considérant (70).

[113] Proposition de règlement 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, 25 janvier 2012, article 33.1.

[114] Circulaire CSSF 12/552 telle que modifiée par la circulaire CSSF 13/563 du 19 mars 2013, section 7.4.1. (86).

Sous-section 2
Quelle méthode ?

152. Chaque entreprise est libre de choisir la méthode qu'elle juge la plus appropriée pourvu qu'elle lui permette d'identifier, d'une part, les risques inhérents au traitement qu'elle envisage de mettre en œuvre et, d'autre part, les mesures de sécurité adaptées.

153. La CNIL, de son côté, considère que la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) constitue une méthode « pertinente », à condition toutefois « que les données à caractère personnel soient considérées dans les biens à protéger et que les impacts sur la vie privée des personnes concernées soient pris en compte »[115]. En application de cette méthode, l'entreprise identifie, à partir d'un contexte qu'elle définit, non seulement les risques associés aux traitements, mais aussi la ou les mesure(s) visant à les traiter.

154. L'étude du contexte, qui constitue la première étape, doit permettre à l'entreprise d'obtenir « une vision claire du périmètre en identifiant tous les éléments utiles à la gestion du risque »[116]. Cela consiste, selon la CNIL, à s'interroger sur les éléments qu'il convient de protéger (traitements, supports et données). C'est l'occasion aussi pour le responsable du traitement de recenser les données et de vérifier que chacune d'entre elles est indispensable au traitement. Ainsi, la CNIL recommande de définir, pour chaque traitement, les données concernées en distinguant les données à caractère personnel (dont les données sensibles), les données stratégiques pour l'entreprise et les données utilisées par les applications métiers. Une réflexion doit être également menée sur les bénéfices attendus du traitement et sur les principales règles à respecter (dispositions réglementaires, sectorielles, etc.). Les sources de risques sont aussi à établir parmi les personnes internes à l'entreprise (utilisateurs, administrateurs, etc.), les personnes externes (clients, prestataires, etc.) et les sources non humaines (sinistre, phénomène naturel, etc.).

155. La deuxième étape est consacrée à l'étude des risques, à proprement parler. Elle s'effectue en trois temps à travers, tout d'abord, la définition des événements redoutés (accès illégitime aux données, modification non désirée des données, etc.) au regard de leurs impacts potentiels sur les droits des personnes. Ensuite, elle se traduit par l'établissement d'une liste explicite et

---

[115] CNIL, *Recommandations pour les entreprises qui envisagent de souscrire à des services de* Cloud computing, 25 juin 2012.

[116] CNIL, *Guide: Gérer les risques sur les libertés et la vie privée*, édition 2012.

hiérarchisée de toutes les menaces (vol, détournement d'usage d'un logiciel, etc.) qui permettraient aux événements redoutés de se produire. Enfin, elle se termine par la réalisation d'une cartographie des risques en fonction de la gravité de l'événement redouté et de la vraisemblance de la menace associée, et ce, en vue de la définition d'une priorité de traitement. Il s'agit ainsi de relier à chaque risque identifié une ou plusieurs mesure(s) pour un traitement le plus efficace possible dudit risque. S'agissant des risques résiduels qui ne feront pas l'objet d'une mesure particulière, l'entreprise doit pouvoir expliquer les raisons pour lesquelles ils peuvent être acceptés par l'entreprise, au regard des critères de gravité identifiés et de la vraisemblance de la menace.

156. La CNIL a parfaitement conscience que cette méthode ne peut être utilisée par tous les responsables du traitement, compte tenu des moyens à mettre en œuvre pour mener à bien une telle analyse. C'est pourquoi elle propose, s'agissant par exemple des services de *cloud computing*, de consulter la liste fournie par l'ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information) qui énumère les 35 principaux risques pour la protection des données[117]. Parmi ces risques figurent : la faille dans l'isolation des données, à savoir le risque que les données hébergées soient modifiées ou rendues accessibles à des tiers non autorisés ; la prise de connaissance des données par des autorités étrangères dans le cadre des réquisitions judiciaires ; la destruction non effective ou non sécurisée des données à l'issue de contrat ; ou encore la communication illégitime des données en raison d'une mauvaise gestion des droits d'accès par les personnes autorisées.

Section 3
La gestion contractuelle des risques

157. Eu égard aux résultats de l'analyse des risques réalisée en amont, le choix du prestataire qui va effectuer le traitement pour le compte du responsable du traitement doit s'opérer en faveur de celui qui propose des garanties adéquates en termes de sécurité et de confidentialité des données. Dans de nombreuses hypothèses, ce choix ne pose pas de difficulté particulière. L'entreprise doit juste s'assurer que les mesures de sécurité et de confidentialité qu'elle a identifiées sont prises en charge par le prestataire, au titre des missions qui lui sont confiées (*outsourcing*, *business process outsourcing*, etc.).

158. Comme indiqué précédemment, ce choix peut s'avérer parfois plus compliqué. C'est le cas dans le cadre de la souscription de services de *cloud*

[117] ENISA, *Critical cloud computing*, décembre 2012.

computing, dans la mesure où la majorité des offres – qui sont standardisées – manquent de transparence et font l'objet d'un contrat d'adhésion, rendant leur négociation très difficile. La circonstance selon laquelle les responsables du traitement ne sont pas en mesure d'évaluer le niveau de protection assuré par le prestataire de services de *cloud computing* ni de le négocier et d'imposer leurs exigences a conduit la CNIL à s'interroger sur la qualification juridique dudit prestataire. En effet, s'il est traditionnellement admis que lorsqu'un client fait appel aux services d'un prestataire, le premier est responsable du traitement et le second est sous-traitant, la question mérite d'être posée lorsque « les clients, bien que responsables du choix de leurs prestataires, ne peuvent pas réellement leur donner d'instructions et ne sont pas en mesure de contrôler l'effectivité des garanties de sécurité et de conformité »[118]. Dans de telles situations, le prestataire pourrait être considéré comme coresponsable du traitement et se voir reconnaître plus d'obligations qu'il n'en a, en qualité de sous-traitant.

159. En tout état de cause, il est de la responsabilité du client de choisir un prestataire qui assure un niveau de protection suffisant des données qui lui sont confiées. Dans ces conditions, il se doit d'avoir une attention particulière sur les points suivants : la nature des mesures de sécurité physique déployées sur le site d'hébergement (sécurité des accès, sécurité électrique, etc.), le choix des mesures de sécurité logique (pare-feu, antivirus, gestion des authentifications, etc.), le choix des mesures de confidentialité mises en œuvre (chiffrement des données, liaison sécurisée, etc.) et l'existence ou non d'une certification, par exemple ISO 27001[119].

---

[118] CNIL, *Recommandations pour les entreprises qui envisagent de souscrire à des services de* Cloud computing, 25 juin 2012.

[119] La norme ISO/IEC 27001:2005 « Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences » est destinée à assurer le choix de mesures de sécurité adéquates et proportionnées qui protègent les actifs de l'entreprise et donnent confiance aux parties intéressées.