DOCTRINE

Une nouveauté en matière de protection des données : la réglementation des « Security Breaches » au détour d'une modification de la directive e-privacy

Yves Poullet

À l'occasion de la réforme de la réglementation des communications électroniques, le législateur européen a introduit le concept nouveau de « violation des données à caractère personnel » (« Security Breach »). Le texte impose l'obligation pour les prestataires des services de communications d'informer tant les personnes concernées que les clients de toute violation, et ce indépendamment de tout dommage. Ainsi l'Union européenne développe de nouvelles exigences en matière de protection des données à caractère personnel. L'article décrit les contours de cette obligation, son champ d'application, les débats relatifs à son adoption et s'interroge sur l'approche nouvelle de la protection des données induites par ces dispositions.

• • •

Taking the opportunity of the revision of all EU e-communications directives, the EU legislator has introduced, last year, a new concept : the "Security Breach". By imposing to e-communications service providers an obligation to inform data subjects and customers of any security breach, EU introduces additional data protection requirements. The article describes the scope and the limits of this regulation, the debates they have raised and how these provisions introduce a new Privacy Protection approach.

La multiplication des incidents nés d'atteintes à la sécurité des traitements de données à caractère personnel (vol d'identité, atteinte à la confidentialité, publication de mots de passe,…) explique la volonté du législateur européen d'accroître les obligations de certains prestataires de manière à assurer une meilleure protection des personnes concernées. Sans doute, la volonté exprimée à l'occasion de la révision de la directive 2002/58 dite e-privacy est-elle encore timide en comparaison des avancées déjà opérées aux États-Unis mais il est évident que la directive adoptée le 25 novembre 2009[1] préfigure une nouvelle approche en matière de protection des données.

[1] Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, 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 et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs.

Cette directive s'inscrit dans le cadre de la révision voulue par les autorités européennes de l'ensemble des réglementations relatives aux infrastructures et services de communications électroniques (le *Telecom Package*). Elle contient des dispositions modificatrices tant de la directive sur les droits des utilisateurs que de la directive dite e-privacy[2]. Parmi les dispositions nouvelles introduites en 2009, figure en particulier l'ajout à l'article 4 de la directive 2002/58, article intitulé : « Sécurité des traitements », de paragraphes nouveaux. L'idée essentielle de la révision de l'article 4 est d'imposer à celui qui subit un tel incident d'informer à la fois les personnes qui suite à cet incident, risquent d'être les victimes des conséquences dommageables de l'incident mais également les autorités en charge de la protection des données qui dans ce cadre reçoivent de nouvelles compétences. Cette obligation nouvelle s'ajoute à l'obligation classique de sécurité des données affirmée par l'article 17 de la directive générale de protection des données[3], article transposé en droit belge par l'article 17 de notre loi du 8 décembre 1992[4].

Après s'être inquiété des définitions et du champ d'application encore restreint des dispositions européennes, notre propos analyse le régime mis en place[5] avant de risquer en conclusion quelques réflexions sur l'approche nouvelle de la protection des données, que révèlent les dispositions.

I. DES DÉFINITIONS ET UN CHAMP D'APPLICATION RESTREINT

Pour mesurer l'ampleur des dispositions européennes prises en matière de violation de données à caractère personnel (en anglais « *Security Breach* »), un détour par les législations américaines s'impose. C'est en effet aux États-Unis que l'idée d'imposer certaines obligations aux prestataires de services de la société de l'information a pris corps avant d'inspirer notre législateur européen. Dès 2003, la Californie votait une loi sur le sujet, suivie rapidement par 48 autres États[6]. Au niveau fédéral, le « *Data Accountability and Trust Act* (DATA) »[7] est sur le point d'être adopté par les sénateurs après avoir été approuvé par la Chambre des représentants.

Les lois américaines étendent les obligations de notification en cas de « *Security Breach* » non seulement à l'ensemble des prestataires de services de la société de l'information, au sens de l'article 1er de la directive 98/34/CE[8] ainsi qu'à une compagnie d'assurance ou une

2 Sur l'analyse de la directive e-privacy, voy. A. Dix, Y. Poullet et K. Rosier, in A. Büllesbasch, S. Girath, Y. Poullet, C. Prins (eds.), *Concise European IT Law*, The Hague, Kluwer Law International, 2010, à paraître.

3 Directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.*, L 281, 23 novembre 1995, pp. 31-50.

4 Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993.

5 Pour un commentaire plus complet d'un texte alors en projet, voy. R. Barcelo et P. Traung, « The Emerging European Union Security Breach Legal Framework », in *Data Protection in a profiled world – Proceedings of the 2nd CPDP Conference,* S. Gutwirth, Y. Poullet et P. De Hert (eds.), 2010, XXIII, Springer Verlag, Dordrecht, pp. 77 à 104.

6 Le lecteur trouvera ces 48 législations sur le site : http://www.nclsorg/programs/lis/clp/priv/breachlaws.htm.

7 HR 2221 Data Accountability and trust Act « *to protect consumers by requiring reasonable security policies and procedures to protect data containing personal information, and to provide for nationwide notice in the event of a security breach* », texte adopté par la Chambre des représentants le 9 décembre 2009 et soumis actuellement au Sénat.

8 La définition donnée par la directive 98/34/CE est reprise pour fixer le champ d'application de la directive dite e-commerce, directive n° 2000/31/CE relative à certains aspects du commerce électronique, *J.O.C.E.*, L 178 du 17 juillet 2000 transposée par la loi belge du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information, *M.B.*, 17 mars 2003.

banque en ligne, des prestataires de soins de santé ou d'informations offrant des services en ligne, mais au-delà, du moins dans certaines législations, à tout responsable de traitement. Le projet fédéral américain vise ainsi, en sa section 3 (a), «*Any person engaged in interstate commerce that owns or possesses data in electronic form containing personal information shall, following the discovery of a breach of security of the system maintained by such person that contains such data:*

(1) notify each individual who is a citizen or resident of the United States whose personal information was acquired or accessed as a result of such a breach of security; and

(2) notify the Commission[9]». Ainsi, tombe sous le champ d'application de la loi américaine, toute personne qui traite des données à caractère personnel même si son activité de traitement n'est pas connectée au réseau, ainsi un médecin qui détiendrait des données sur ses patients sans que son ordinateur ne soit relié au réseau tant pour recevoir de l'information que pour en donner. À l'inverse, le texte européen limite les obligations nouvelles aux seuls opérateurs de services de communications électroniques accessibles au public sur les réseaux de communication publics[10]. C'est en effet ainsi que l'article 3 de la directive e-privacy, modifié par le texte de 2009, fixe le champ d'application *ratione personae* de la directive[11] et que, pour éviter toute ambiguïté, l'article 4 (3), paragraphe 1er précise: «En cas de violation de données à caractère personnel, le fournisseur de services de communications électroniques accessibles au public avertit sans retard indu l'autorité nationale compétente de la violation». Cette restriction a été lourdement critiquée par les défenseurs de la vie privée et leurs critiques relayées par le groupe de l'article 29[12] et le contrôleur européen à la protec-

9 La *Federal Trade Commission* (FTC) est une autorité administrative juridictionnelle en charge de la protection des données. On connaît le rôle important que la FTC joue en matière de protection des données, rôle que les autorités européennes ont reconnu très largement dans le cadre de la décision dite «*Safe Harbor*» qui dès 2000 permettait de considérer l'autorégulation des États-Unis en matière de protection des données comme adéquate et ce sous certaines conditions en particulier la supervision par la FTC (décision 2000/520/CE du 26 juillet 2000 de la Commission conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la «sphère de sécurité» et par les questions souvent posées y afférentes, publiés par le ministère du Commerce des États-Unis d'Amérique, *J.O.C.E.*, L 215, 25 août 2000, pp. 7-47).

10 Ainsi incontestablement les opérateurs de réseaux accessibles au public et les fournisseurs d'accès ou les opérateurs de courrier électronique. Par contre, les opérateurs de plateformes web tels les opérateurs de réseaux sociaux (Facebook *et alii*) peuvent difficilement être jugés comme visés par la directive qui insistent sur le fait que le service doit consister entièrement ou du moins principalement dans la transmission de signaux.

11 «La présente directive s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications publics dans la Communauté, y compris les réseaux de communications publics qui prennent en charge les dispositifs de collecte de données et d'identification». La précision couverte par le dernier bout de phrase permet de viser les services de communication accessibles au public utilisant des dispositifs RFID comme par exemple les réseaux de transport public fonctionnant avec des puces RFID, ainsi le système MOBIB de la STIB.

12 Groupe de travail «article 29» sur la protection des données, document de travail WP 150, «Avis 2/2008 sur la révision de la directive 2002/58/CE concernant la protection de la vie privée dans le secteur des communications électroniques (directive "vie privée et communications électroniques")», adopté le 15 mai 2008 et Avis 1/2009 concernant les propositions modifiant la directive 2002/58/CE sur la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques»), p. 4: «Par ailleurs, le groupe observe que les trois propositions (du Parlement, de la Commission et du Conseil) adoptent des approches substantiellement différentes en ce qui concerne les violations de la sécurité et des données à caractère

tion des données (le CEPD)[13] ont trouvé écho dans les travaux parlementaires[14]. La demande du Parlement d'étendre la portée de l'obligation de notification à tous les prestataires de services de la société de l'information a abouti finalement à un compromis repris dans le considérant 59 de la directive de 2009 amendant la directive 2002/58/CE : « L'intérêt des utilisateurs à être informés ne se limite pas, à l'évidence, au secteur des communications électroniques, et il convient dès lors d'introduire de façon prioritaire, au niveau communautaire, des exigences de notification explicites et obligatoires, applicables à tous les secteurs. Dans l'attente d'un examen, mené par la Commission, de toute la législation communautaire applicable dans ce domaine, la Commission, après consultation du contrôleur européen de la protection des données, devrait prendre les mesures appropriées pour promouvoir, sans retard, l'application, dans l'ensemble de la Communauté, des principes inscrits dans les règles relatives à la notification des violations des données contenues dans la directive 2002/58/CE (directive "vie privée et communications électroniques"), quel que soit le secteur ou le type de données concerné. Les autorités nationales compétentes devraient assurer le suivi des mesures prises et diffuser les meilleures pratiques parmi les fournisseurs de services de communications électroniques accessibles au public ». Cet appel clair à une intervention législative consacrant une extension de l'obligation de notification à l'ensemble des services de la société de l'information voire à l'ensemble des traitements de données à caractère personnel sera-t-il suivi ? Dans son opinion relative à l'« avenir de la protection des données » regroupant nombre de suggestions pour une nouvelle réglementation de la protection des données en Europe déjà citée, le Groupe de l'article 29 réaffirme à trois reprises le besoin d'une telle extension[15].

En ce qui concerne le champ d'application « *ratione materiae* », par contre, la comparaison

personnel, notamment lorsqu'elles considèrent la portée de l'obligation (qui s'étend aux services de la société de l'information dans les amendements du Parlement et est limitée aux services de communications électroniques accessibles au public pour le Conseil et la Commission) ; le groupe soutient fermement une extension de l'obligation aux services de la société de l'information ;… ».
Le groupe dit de l'article 29 (parce que mis en place par l'article 29 de la directive 95/46/CE) est un groupe consultatif, indépendant composé de représentants des autorités de protection des données. Les avis du groupe de l'article 29 sont disponibles en ligne sur le site de la Commission européenne http://ec.europa.eu/justice/policies/privacy/workinggroup/.

13 Voy. en particulier la seconde opinion du CEPD du 9 janvier 2009 sur la révision de la directive 2002/58/CE (http://www.edps.europa.eu/EDPSWEB/edps).

14 En première lecture, le Parlement européen s'était opposé au texte préparé par la Commission et approuvé par le Conseil et qui retenait l'application des dispositions en matière de violation de la protection des données pour les seuls services de communication accessibles au public sur les réseaux de communications publics. Nonobstant cette opposition, la Commission répéta son point de vue : « *The inclusion of providers of Information services goes beyond the current scope of the regulatory framework … and is accordingly deleted.* ». Cet argument fondé sur la volonté de ne pas étendre le champ d'application actuel de la directive 2002/58/CE est jugé faible dans la mesure où la directive 2002/58 contient déjà de nombreuses dispositions qui visent d'autres acteurs que les opérateurs des seuls services susmentionnés, ainsi les dispositions en matière de spam, d'intrusion dans l'ordinateur d'autrui et surtout en matière de terminaux.

15 « En outre, la transparence impose une information des personnes concernées en cas de violation de la vie privée susceptible de nuire à leurs données à caractère personnel ainsi qu'à leur vie privée. Elles pourraient de cette manière tenter de limiter le préjudice qu'elles ont subi (dans certains cas, les autorités devraient également être informées,…). La notification générale de violation de la vie privée devrait être introduite dans le nouveau cadre juridique » (L'avenir de la protection de la vie privée, Contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel, Groupe de l'article 29, avis n° 168, 1er décembre 2009). Cette demande d'extension est reprise dans les chapitres 2, 5 et 6 de l'avis.

avec la législation américaine s'avère plus flatteuse pour l'européenne. L'article 2 (h) de la directive 2002/58 telle qu'amendée en 2009 définit comme suit la « violation de données à caractère personnel » : une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture de services de communications électroniques accessibles au public dans la Communauté ». Contrairement au projet américain, la définition européenne couvre toute donnée à caractère personnel et ce au sens le plus large[16] et non uniquement certaines données sensibles[17]. La notion de violation est large : elle couvre non seulement les accès ou communications non autorisés mais également les destructions, pertes de données peu importe qu'elles soient suivies d'accès non autorisés. De même, on note que la définition vise tous les incidents « en relation avec la transmission de données » et pourrait donc couvrir des incidents relatifs à des transactions effectuées par l'opérateur dans le cadre de son réseau interne ou dans le cadre de ses relations avec un sous-traitant. Enfin, la notion de violation s'entend d'une atteinte soit à l'intégrité physique, soit à des intérêts qui peuvent être économiques ou financiers soit enfin également au contraire des États-Unis à des intérêts purement moraux comme l'est une simple atteinte à la réputation : « Une violation devrait être considérée comme affectant les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier lorsqu'elle est susceptible d'entraîner, par exemple, le vol ou l'usurpation d'identité, une atteinte à l'intégrité physique, une humiliation grave ou une réputation entachée en rapport avec la fourniture de services de communications accessibles au public dans la Communauté »[18]. On sait qu'aux États-Unis seules seront retenues les atteintes ayant un impact économique ou physique sur la personne.

II. LE RÉGIME JURIDIQUE MIS EN PLACE PAR LA NOUVELLE DIRECTIVE

Que proposent les dispositions introduites par les modifications de 2009 ? L'article 17 de la directive 1995/46 dite de protection des données consacrait une obligation de sécurité c'est-à-dire « la mise en œuvre des mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel 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. Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger ». À cette obli-

16 Nous n'évoquerons pas ici les difficultés liées à la définition du concept de données à caractère personnel. Ainsi, les adresses IP ou les *cookies* sont-elles des données à caractère personnel ? Sur cette notion, Groupe de travail « article 29 » sur la protection des données, document de travail WP 136, « Avis 4/2007 sur le concept de données à caractère personnel », adopté le 20 juin 2007.

17 La section 5 (7) restreint ainsi la notion de « *personal data* » : « *The term 'personal information' means an individual's first name or initial and last name, or address, or phone number, in combination with any or more of the following data elements for that individual :*
(i) Social Security number.
(ii) Driver's license number, passport number, military identification number, or other similar number issued on a government document used to verify identity.
(iii) Financial account number, or credit or debit card number, and any required security code, access code, or password that is necessary to permit access to an individual's financial account ».

18 *Cfr.* le considérant n° 61 de la directive.

gation, la révision de 2009[19], en introduisant un article 4(3), ajoute le devoir, aujourd'hui, pour les seules personnes visées par la directive 2002/58, demain, peut-être pour tous les responsables de traitement des données, de notifier les incidents de sécurité tant aux personnes concernée qu'aux autorités de protection des données.

L'objectif de cette obligation supplémentaire est triple. Premièrement, les coûts de l'exécution de cette obligation à la fois financiers mais surtout en termes d'affectation de la réputation sont tels que les personnes y soumises auront tout intérêt à veiller de manière plus consciencieuse au respect de l'obligation générale de sécurité visée par l'article 17 de la directive de protection des données. Deuxièmement, l'information des personnes concernées leur permet de prendre des mesures afin de diminuer les dommages qu'elles risquent de subir à la suite de l'incident. Ainsi, être prévenu du vol de son mot de passe permet à son titulaire de modifier ce dernier et de prévenir le dommage. En ce sens, l'obligation d'information peut être rapprochée[20] de l'obligation contractuelle de minimisation des risques (*duty of mitigation*) que la jurisprudence impose aux contractants sur la base de l'obligation de bonne foi. Troisièmement, le devoir d'informer les autorités de protection des données permettront à ces dernières de mieux préciser l'obligation de moyens que constitue l'article 17 de la directive et de préconiser, le cas échéant, des standards de protection techniques et organisationnels afin d'éviter dans le futur des incidents de sécurité.

A. L'obligation de notification – contenu et limites

L'article 4(3) distingue, en fonction de son destinataire, l'étendue du devoir de notification. Vis-à-vis de l'autorité de protection des données, cette obligation existe pour tout incident indépendamment de son importance ou de l'importance de ses conséquences. Elle doit être effectuée « sans retard indu »[21] et n'appelle pas nécessairement du moins de réaction de l'autorité compétente. À l'inverse, lorsqu'il s'agit de prévenir les « abonnés *(subscribers)* ou les particuliers *(individuals)*[22] », le devoir de notification n'existe que « lorsque la violation de données à caractère personnel est de nature à affecter négativement les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier ». Le texte anglais permet de mieux comprendre la signification de l'expression « de nature à affecter » : « *likely to adversely affect* ». Ainsi, il est exclu d'obliger à notification l'opérateur lorsque l'incident n'a que de faibles chances d'aboutir à des conséquences dommageables pour l'abonné ou le particulier, ainsi si un accès illégal n'a visiblement permis

19 La directive 2002/58 avait déjà imposé aux opérateurs de services de communications électroniques accessibles au public sur les réseaux de communication publics une obligation de sécurité élargie, en imposant des obligations de sécurité, d'intégrité et de confidentialité lors de la transmission des messages. Mieux, l'article 4 (2) imposait en cas de risque relatif à la sécurité du réseau une obligation d'information relative à ce risque et aux moyens de le prévenir ou d'éviter totalement ou partiellement les dommages y liés. L'article 4 (3) prolonge donc ces extensions de l'obligation de sécurité déjà introduite par le texte original de la directive 2002/58.

20 … même si le champ d'application de la disposition introduite en 2009 ne suppose pas nécessairement l'existence d'un contrat entre la personne concernée et le débiteur de l'obligation d'information.

21 C'est-à-dire dès que l'incident est connu… sauf si la notification nuit aux besoins d'une enquête judiciaire ou de sureté de l'État : « Par ailleurs, ces règles et procédures devraient tenir compte des intérêts légitimes des autorités chargées de l'application du droit, dans les cas où une divulgation prématurée risquerait d'entraver inutilement l'enquête sur les circonstances d'une violation » (considérant 64).

22 On note que la directive évite de parler des « personnes concernées ». Par ailleurs, on rappelle que la directive 2002/58 protège également les personnes morales.

à l'intrus que de prendre connaissance des clés d'accès qui ont pu être modifiées instantanément. À cette première limite, le texte en ajoute une seconde : « La notification d'une violation des données à caractère personnel à l'abonné ou au particulier concerné n'est pas nécessaire si le fournisseur a prouvé, à la satisfaction de l'autorité compétente, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation. De telles mesures de protection technologique rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès ». Cette exception constitue certes une promotion des mesures technologiques de protection de la vie privée (*Privacy Enhancing Technologies*), en particulier des mesures de cryptographie et suit le vœu déjà formulé par la Commission en 2007[23]. On note les limites de cette seconde exception liée à une démonstration de la mise en œuvre de ces mesures en ce qui concerne les données en question et de leur effectivité à 100 % vis-à-vis des personnes non autorisées. En outre, il faut que l'autorité compétente ait été convaincue par la démonstration[24]. On ajoute que l'alinéa 4 du paragraphe 3 permet à l'autorité compétente de substituer son jugement à celui de l'opérateur concerné et de forcer ce dernier à notifier l'incident.

Le paragraphe 3 ne précise pas le mode de notification. Sans doute, le mode devra-t-il être approprié et garantir que chaque bénéficiaire ait eu la possibilité d'en prendre connaissance. Ainsi, une notification dans les journaux à grand tirage avec renvoi pour plus de détails à un site web sans que des courriers papier ou électroniques ne doivent être envoyés à chacun. Plus discutable serait par contre le recours à une simple information postée sur un site web. En ce qui concerne cette fois le contenu de la notification, la directive distingue le contenu suivant le destinataire de l'information notifiée mais n'est guère plus précise : « La notification faite à l'abonné ou au particulier décrit au minimum la nature de la violation de données à caractère personnel et les points de contact auprès desquels des informations supplémentaires peuvent être obtenues et recommande des mesures à prendre pour atténuer les conséquences négatives possibles de la violation de données à caractère personnel. La notification faite à l'autorité nationale compétente décrit en outre les conséquences de la violation de données à caractère personnel, et les mesures proposées ou prises par le fournisseur pour y remédier ». Pour fixer le contenu, le critère à retenir nous semble devoir être fonctionnel : l'information communiquée doit permettre la réaction de la personne concernée. Il apparaît important que la nature de l'incident doive

[23] La communication de la Commission du 2 mai 2007 (COM (2007) 228 Final, Bruxelles, 2 mai 2007) intitulée « Promouvoir la protection des données par les technologies renforçant la protection de la vie privée » définit des actions précises pour atteindre l'objectif consistant à limiter le traitement des données à caractère personnel et recourir autant que possible à des données anonymes ou à des pseudonymes en soutenant le développement de ces technologies et leur utilisation par les responsables du traitement des données et les personnes »… De manière générale sur les PETs, voy. : J. Borking, « The Status of Privacy Enhancing Technologies », in E. Nardelli, S. Posadziejewsji et M. Talomo, *Certification and Security in E-Services*, Boston 2003, p. 223 ; R. Hes et J. Borking, *Privacy Enhancing Technologies : the path to anonymity (2nd revised edition)*, Report from the Dutch Data Protection Authority AV no. 11 Den Haag, 2000.

[24] … ce qui suggère que les opérateurs le plus souvent pour éviter toute contestation feront un pré-test des mesures envisagées auprès de l'autorité compétente. Deux remarques : 1. il n'est pas évident que les autorités jouissent aujourd'hui du personnel et des moyens de juger de la qualité des mesures technologiques envisagées et 2. lorsqu'un opérateur offre son service de communications électroniques dans divers pays, faudra-t-il qu'il fasse ainsi reconnaître auprès de chaque autorité nationale de protection la qualité de ses mesures ?

être décrite : vol d'identité, perte de données, accès fortuit ou au contraire intentionnel d'un tiers. Des détails comme l'origine de l'attaque peuvent être importants : s'agit-il d'une attaque menée à partir d'un pays étranger ? L'attaque était-elle ciblée par rapport à telles données ou tels clients ? L'information sur les mesures de précaution suggérées est également essentielle. Plus les mesures suggérées sont pertinentes et faciles à mettre en œuvre, plus l'information claire sur ces mesures à prendre par le titulaire ou le particulier permettront à l'opérateur de voir sa responsabilité diminuée au cas où la personne informée n'ayant pas suivi les conseils a subi des dommages ou les a laissés s'aggraver. Le devoir d'atténuation des conséquences dommageables est en effet réciproque et au devoir d'informer de l'opérateur sur les mesures à prendre, répond le devoir de la personne informée de suivre les instructions, objet de la notification. Enfin, il apparaîtra souvent nécessaire que des détails supplémentaires sur l'incident, ses circonstances et les parades possibles soient disponibles auprès d'un point de contact. On ajoutera que l'information doit être concise, claire et sans ambiguïté, en particulier on évitera de mêler l'annonce de l'incident et des messages publicitaires relatifs à de nouveaux services y compris de sécurité.

B. Les compétences additionnelles confiées aux autorités de protection des données

Le paragraphe 4 de l'article 4 confère aux autorités de protection des données des compétences nouvelles qui devront être traduites dans notre pays peu enclin jusqu'à présent à confier à sa Commission de protection des données des compétences réglementaires et de sanction[25] : « Sous réserve des mesures techniques d'application adoptées en vertu du paragraphe 5, les autorités nationales compétentes peuvent adopter des lignes directrices et, le cas échéant, édicter des instructions précisant les circonstances dans lesquelles le fournisseur est tenu de notifier la violation de données à caractère personnel, le format applicable à cette notification et sa procédure de transmission. Elles doivent également être en mesure de contrôler si les fournisseurs ont satisfait aux obligations de notification qui leur incombent en vertu du présent paragraphe et infligent des sanctions appropriées si ces derniers ne s'y sont pas conformés ». Ainsi, les autorités fixeront le cas échéant les hypothèses de notification obligatoire mais également le contenu et le format des notifications, elles conduiront des audits préventifs pour s'assurer du respect effectif par les opérateurs de leurs obligations de sécurité et de notification. L'alinéa 2 du paragraphe impose d'ailleurs la mise à disposition au bénéfice des autorités de protection des données des incidents, mesures prises et conséquences de ces incidents. On ajoute que la directive de 2009 prévoit la sanc-

[25] Certains auteurs (voy. en particulier P. De Hert, *In het licht van de technologie : Pleidooi voor continuiteit en veranderingen in gegevensbescherming, gesprek voor het Privacy bescherming Commissie,* Den Haag, 009, published *in* http://www.vub.ac.be/LSTS/members/dehert/) parle ainsi de seconde génération d'autorités de protection des données. Alors que les premières législations de protection des données n'admettaient qu'un pouvoir consultatif de ces autorités, progressivement nombre de pays ont confié à leurs autorités des compétences de décisions, de réglementations et de sanctions et transformé celles-ci en autorités administratives sujettes au contrôle des juridictions au moins administratives. Notre pays s'est montré plus prudent, ce qui n'est pas sans poser difficultés quant aux recours des responsables de traitement vis-à-vis d'« avis » ou de recommandations de la Commission de la protection de la vie privée. Sur ce point, voy. E. Degrave, « La Commission de la protection de la vie privée : un organisme invincible ? », *R.D.T.I.,* 2006, pp. 237-238.

tion possible par les autorités en cas de non-respect des obligations de notification. On rappelle que par ailleurs, l'autorité de protection des données reçoit notification de tous les incidents de violation de la vie privée. Toutes ces compétences supplémentaires si elles sont louables dans leur principe soulèvent cependant question. Nos autorités ne disposent ni du personnel qualifié ni des ressources nécessaires pour faire face à ces devoirs nouveaux. Or faute de ce personnel et de ces ressources, il est à craindre que le texte reste lettre morte. Le préambule de la directive[26] le rappelle de même que plus énergiquement encore, le groupe de l'article 29 dans l'avis déjà cité relatif à l'avenir de la vie privée[27].

Le paragraphe 5 essaie de répondre à ces défis nouveaux en promouvant la coopération entre autorités de protection des données mais également par la mise sur pied d'un système de réglementation européenne uniforme des procédures de notification. En la matière, la décision reviendrait à la Commission qui s'appuierait tant sur le travail de l'Agence européenne chargée de la sécurité des réseaux et de l'information que du groupe de l'article 29, du contrôleur européen et d'une large consultation des intéressés, c'est-à-dire tant les prestataires visés par l'obligation que les associations de libertés civiles ou de consommateurs, représentant les intérêts des particuliers: « Afin d'assurer une mise en œuvre cohérente des mesures visées aux paragraphes 2, 3 et 4, la Commission peut, après consultation de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), du groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 29 de la directive 95/46/CE et du Contrôleur européen de la protection des données, adopter des mesures techniques d'application concernant les circonstances, le format et les procédures applicables aux exigences en matière d'information et de notification visées au présent article. Lors de l'adoption de ces mesures, la Commission associe toutes les parties prenantes concernées, notamment pour être informée des meilleures solutions techniques et économiques disponibles pour assurer la mise en œuvre du présent article ». On ajoute en outre que cette décision de la Commission suivra la procédure de comitologie, comme rappelé à l'article 14 de la directive 2002/58 telle que révisée. Ce qui permettra au Parlement européen et au Conseil des ministres de s'opposer le cas échéant à des initiatives de la Commission.

CONCLUSIONS

Quelques points nous paraissent transcender le cadre précis de l'intervention législative européenne et révèlent une approche nouvelle de la protection des données[28]. Sans doute, la volonté de plus en plus marquée de l'Union européenne de renforcer l'effectivité des règles de protection des données constitue le point

[26] Considérant 3: « Les États membres veillent à ce que l'autorité nationale compétente et, le cas échéant, d'autres organismes nationaux disposent des pouvoirs d'enquête et des ressources nécessaires, et notamment du pouvoir d'obtenir toute information pertinente dont ils pourraient avoir besoin, afin de surveiller et de contrôler le respect des dispositions nationales adoptées en application de la présente directive ».

[27] « En tout état de cause, un contrôle indépendant implique la mobilisation de ressources et de compétences appropriées ».

[28] Bien d'autres réflexions pourraient être faites à propos de la directive 2002/58 et de la façon dont elle peut apparaître comme anticipatrice d'une troisième génération de législations de protection des données. Sur ce point, nous renvoyons le lecteur à ce que nous avons écrit in Y. Poullet, « Pour une troisième génération de réglementation de protection des données », in *Défis du droit à la protection à la vie privée*, coll. Cahiers du CRID, 31, Bruxelles, Bruylant, 2008, pp. 25-70.

le plus saillant de cette approche nouvelle. Cette volonté se traduit en premier lieu, mais nous l'avons déjà signalé, par un renforcement du rôle des autorités de protection des données conviées à pratiquer des audits, à sanctionner et à mettre en évidence des « *best practices* » en matière de sécurité de systèmes d'information. En deuxième lieu, on note que les modifications de la directive s'appuient sur une responsabilisation accrue des responsables de traitement, pour le moment certains du moins. Cette idée américaine promue sous le slogan d'« *Accountability Principle* »[29] d'approcher la protection des données non par un cadre législatif et administratif externe lourd et peu approprié mais par la création d'obligations à charge des responsables de traitement, obligations de veiller eux-mêmes au respect des principes de protection des données, en l'occurrence celui de sécurité et de veiller à démontrer la conformité de leurs pratiques aux meilleures pratiques en la matière. En troisième lieu, l'effectivité est obtenue par la définition de normes technico-organisationnelles[30] si possible au niveau européen et établies en concertation avec les acteurs intéressés[31].

29 Ce principe (sur ce principe, son historique et sa progressive consécration, voy. : Centre for Information Policy Leadership, *Data Protection Accountability : The essential Elements – A Document for Discussion,* octobre 2009, p. 4) est repris et promu par le Groupe de l'article 29 dans son opinion déjà citée sur l'avenir de la protection des données comme suit : « Pour résoudre ce problème, il conviendrait d'introduire un principe de responsabilité dans le cadre global aux termes duquel les responsables du traitement des données seraient contraints de prendre les mesures nécessaires pour veiller au respect des obligations et principes essentiels de la directive actuelle lors du traitement des données à caractère personnel. Une telle disposition renforcerait la nécessité de mettre en place des politiques et des mécanismes permettant la mise en œuvre effective des principes et obligations essentiels de la directive actuelle. Elle confirmerait la nécessité de prendre des mesures efficaces donnant lieu à une application interne efficace des obligations et principes essentiels actuellement consacrés dans la directive. En outre, le principe de responsabilité exigerait des responsables du traitement des données qu'ils mettent en place les mécanismes internes nécessaires pour démontrer leur conformité aux parties prenantes externes, notamment aux autorités nationales chargées de la protection des données. Au final, la nécessité de prouver que les mesures appropriées ont été prises pour assurer la conformité facilitera considérablement l'exécution des règles applicables ».

30 « *If Technology is viewed as the major challenge for our privacy, it might also be the solution. The role of technology must be reassessed and new research efforts should be devoted in computer science to the design of future "privacy aware systems". With traditional Privacy Enhancing Tools (PETs), technologies are used to enhance "user empowerment", for example by providing means to ensure that the subject can hide his personal data (or encrypt them) or by offering guarantees for the express consent of the user through computer facilities such as software agents. But technologies might also be used in direct or indirect relationships with law either by enforcing or facilitating the compliance of controllers with their legal commitments, by developing a policy for the standardisation of terminal equipments which takes into consideration the privacy requirements, by providing auditing techniques for labelling authorities, by facilitating the attribution of liabilities in case of litigation and, finally, in relationship with social uses, by defining architectures for reinforcing negotiation or for adopting collective privacy statements, notably in the context of Web 2.0 platforms, what we call : P5P (Peer to Peer Platforms for Privacy Preferences)* », Y. Poullet, « About the E-Privacy Directive : Towards a third generation of data protection legislation ? », in *Data Protection in a profiled world – Proceedings of the 2nd CPDP Conference,* S. Gutwirth, Y. Poullet et P. De Hert (eds.), 2010, XXIII, Springer verlag, Dordrecht, pp. 3 à 30.

31 Cette tendance était déjà présente dès 2002 dans la directive e-privacy dans la mesure où l'article 14 permettait à la Commission d'imposer la définition de normes techniques pour la fabrication des terminaux afin d'assurer le respect de la protection. Plus récemment, le 12 mai 2009, la Commission européenne publiait la recommandation 2009/387/CE (*J.O.C.E.*, C 3200) sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence. La recommandation prévoit de plus que la « Commission veillera à définir des orientations au niveau communautaire, sur la base des pratiques existantes et de l'expérience acquise dans les États membres et les pays tiers, sur la gestion de la sécurité de l'information en matière d'applications RFID ». Sur cette recommandation, L. Costa, « RFID, vie privée et protection de données à caractère personnel :

Les conséquences des incidents de sécurité touchent les personnes tant dans leur qualité de consommateurs, soucieux de leurs intérêts économiques que de citoyens soucieux de leurs libertés. Le fait que les dispositions ont été introduites à l'occasion de discussions relatives à un texte qui portait à la fois sur la protection des consommateurs de services de communications électroniques que sur la vie privée dans les réseaux de communication conforte l'idée selon laquelle l'approche « *Consumer Privacy* » représente un atout majeur pour la cause de la vie privée. La protection des consommateurs et celle de la vie privée trouvent une occasion de cause commune que les dispositions légales permettent d'encourager : utilisation des dispositions en matière de pratiques commerciales déloyales ou agressives, possibilité d'actions collectives et au-delà intérêt d'un rapprochement des autorités de protection des données, des associations de libertés civiles et des associations de protection des consommateurs. La réglementation des violations de la vie privée dans les réseaux de communications touche autant aux intérêts des consommateurs qu'à la protection de nos libertés[32].

Nul doute que la réglementation des « *Security Breaches* » fera parler d'elle dans les années futures. Même inachevée, la révision de la directive 2002/58, en consacrant quelques dispositions en matière de sécurité des données, constitue une évolution significative de la protection des données.

commentaires sur la recommandation du 12 mai 2009 de la Commission européenne », article à paraître in *Lamy droit de l'immatériel*, 2010.

[32] Sur ce point, C. Colin et Y. Poullet, « Du consommateur et de sa protection face à de nouvelles applications des technologies de l'information : risques et opportunités », article à paraître in *D.C.C.R.*, 2010, à paraître.