Obligation de notification des failles de sécurité : quand l'Union Européenne voit double…

Par
François COUPEZ, Avocat à la Cour, Chargé d'enseignement à l'université Paris II Panthéon-Assas,
Membre de Cyberlex
Cabinet Caprioli & Associés
www.caprioli-avocats.com
email : contactparis@caprioli-avocats.com

Introduction

Publié ! Le « *Paquet Télécom* », adopté entre le 19 et le 24 novembre après de longues discussions et de nombreux mois de reports (tenant pour l'essentiel au mécanisme de « riposte graduée » qu'a adopté la France à l'occasion des lois « Hadopi » 1 & 2 et que d'autres pays nous copient maintenant[1]), a été publié au Journal Officiel de l'Union Européenne le 18 décembre dernier[2].
Il est donc temps de déballer le « *Paquet* » livré juste avant Noël et d'en découvrir le contenu : rappelons que ce « *Paquet Télécom* » est en réalité le nom donné à l'origine au cadre juridique communautaire des communications électroniques, adopté en 2002, formé notamment de cinq directives différentes et qui fait l'objet d'un vaste processus de révision engagé depuis le 13 novembre 2007.

Aujourd'hui, ces cinq directives sont mises à jour, modifiées par le biais de deux directives différentes :

- la directive 2009/136/CE du 25 novembre 2009 qui modifie les directives 2002/22/CE (« *service universel* »), 2002/58/CE *(« vie privée et 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* » ;

- et la directive 2009/140/CE du 25 novembre 2009 qui modifie les directives 2002/21/CE (« *cadre* »), 2002/19/CE (« *accès* ») et 2002/20/CE *(« autorisation* »).

Ces deux directives, dont la transposition doit intervenir avant le 25 mai 2011, prévoient une série de nouvelles obligations allant de la portabilité du numéro en téléphonie fixe ou portable, avec délai réduit, à l'adoption du principe de l'*opt-in* pour l'utilisation de témoins de connexion (« *cookies* »). Mais pour l'heure, nous nous concentrerons simplement sur une obligation emblématique destinée à améliorer la sécurité des réseaux : l'obligation faite à certains opérateurs techniques de notifier les violations de sécurité de leurs systèmes d'information. Ou plutôt devrait-on dire **les** obligations. Car en effet, le principe est non seulement posé par la directive « *cadre* » modifiée mais également par la directive « *vie privée et communications électroniques* ». Ces obligations se révèlent pourtant, à l'étude, n'être que des « fausses jumelles », sœurs certes, mais loin d'être identiques.

I. Notifier les incidents de sécurité, dans quel but ?

Historiquement né en Californie via une loi de février 2002[3] puis adopté dans d'autres Etats, tant au niveau fédéral que dans d'autres pays, ce type d'obligation avait pour but, originellement, de contribuer activement à la lutte contre l'usurpation d'identité. En effet, les bases de données et réseaux d'un grand nombre d'opérateurs économiques (fournisseurs d'accès à internet, site de e-commerce, banques, etc.) regorgent d'informations à caractère personnel de clients permettant, si celles-ci sont volées, de frauduleusement contrefaire l'identité du client (numéro de sécurité sociale,

[1] Le projet de loi dit « *Digital Economy Bill* » est conçu pour l'heure comme étant l'équivalent de notre Hadopi au Royaume-Uni et prévoit à ce titre un mécanisme proche de notre riposte gradué, prévoyant la coupure d'accès au réseau (http://www.commonsleader.gov.uk/output/page2920.asp).
[2] Journal Officiel de l'Union Européenne (JOUE) L.337 du 18/12/2009 p. 1 à 69.
[3] « *Senate Bill 1386* » du 12 févier 2002, entrée en vigueur le 1er juillet 2003 et ajoutant des dispositions imposant la révélation des incidents de sécurité au Code civil californien. Cette loi a trouvé son origine dans un incident rencontré par l'administration ayant entrainé la dissémination des données de salaires de 200 000 fonctionnaires.

numéros de cartes bancaires, informations fiscales voire patrimoniales, etc.). Or, par le biais d'une notification obligatoire de leurs failles de sécurité, les acteurs économiques n'ayant pas suffisamment sécurisé les données à caractère personnels de leurs clients se voient obligés de prévenir ceux-ci de leurs carences. Dans un pays où l'action de groupe (ou « *class action* ») non seulement existe, mais conduit fréquemment à des condamnations de plusieurs millions de dollars, on comprend aisément que cette incitation indirecte à la sécurisation des systèmes devienne très efficace.
Pourtant, si le « *Data loss barometer 2009* »[4] de KPMG montre que le secteur des services financiers a pris des mesures efficaces (baisse de 2/3 des vols de données), il n'en reste pas moins que, dans l'ensemble, plus de 110 millions de personnes dans le monde ont été affectés par le vol de données au premier semestre 2009, soit une progression inquiétante de plus de 50 % en un an ! La réponse de l'Union Européenne, s'opérant d'abord *via* le « *Paquet Télécom* », est double et prévoit un renforcement notable de la sécurisation des réseaux et des services d'accès, par le biais de mesures *a priori* (obligation d'évaluation de la sécurité des systèmes, etc.) mais également *a posteriori* (obligations de notification, soit l'objet de notre présente étude).

Ainsi, le considérant 44 de la directive 2009/140/CE rappelle spécifiquement que « *la complexité des systèmes, les défaillances techniques ou les erreurs humaines, les accidents ou les attentats peuvent tous avoir des conséquences sur le fonctionnement et la disponibilité des infrastructures physiques qui fournissent des services importants aux citoyens de l'Union européenne, y compris les services d'administration en ligne* », ce qui explique les nouvelles règles, passant par la création dans la directive « *cadre* » d'un nouveau chapitre III bis « *sécurité et intégrité des réseaux et services* », formé de deux articles (13 bis et 13 ter).

Quant à la directive 2009/136/CE, elle prévoit cette obligation au regard de la nécessaire protection des données à caractère personnel transitant via les réseaux de communications électroniques, eu égard non seulement au vol d'identité, mais également aux atteintes « *à l'intégrité physique* », aux « *humiliations graves* » ou à la « *réputation* » « *en rapport avec la fourniture de services de communications accessibles au public dans la Communauté* »[5].

Mais l'Union Européenne prévient clairement dans les considérants de la directive 2009/136/CE que, si ces nouvelles exigences de notification sont limitées aux violations de sécurité intervenant dans le secteur des communications électroniques, **ce n'est que le commencement** et qu'à terme, ces exigences seront étendues à tous les secteurs mais également à tout type de données[6].

Ainsi, l'obligation de notification pourrait s'étendre à court terme aux services de la société de l'information (activités en ligne, etc.) mais également aux activités plus traditionnelles (commerçants de tous types, banque, industrie, etc.). D'ailleurs, dans le cadre du processus législatif d'adoption de la directive 2009/136/CE, cette extension avait été prévue notamment pour les banques puis finalement supprimée pour être vraisemblablement intégrée dans le projet de modification de la directive 1995/46/CE « protection des données »[7]. Le sujet est également à l'ordre du jour en France, M. Détraigne et Mme Escoffier, sénateurs, étant à l'origine de la proposition de loi du 6 novembre 2009 « *visant à mieux garantir le droit à la vie privée à l'heure du numérique* » et proposant également une obligation de notification des « *atteintes aux traitements de données* »[8]. Une telle obligation existe d'ailleurs depuis quelques mois en Allemagne[9].

---

[4] Etude « *Data loss Barometer : Issue 2 – 2009* », publiée le 29 septembre 2009 et disponible sur <http://www.datalossbarometer.com/>.
[5] Considérant 61 de la directive 2009/136/CE.
[6] V. en particulier le considérant 59 de la directive 2009/136/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* ».
[7] Directive 1995/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données ; J.O. L 281 du 23 novembre 1995, p. 31 s.
[8] Art. 7 de la proposition de loi visant à modifier l'article 34 de la loi n° 78-17 du 6 janvier 1978 modifiée qui prévoit actuellement une obligation de sécurité des données, pénalement sanctionnée.
[9] La « *Bundesdatenschutzgesetz* » (loi fédérale allemande de protection des données à caractère personnel du 20 décembre 1990) prévoit ainsi depuis le 1er septembre 2009 en son § 42a que la notification concernera uniquement les atteintes aux données sensibles ou protégées par le secret professionnel qui causent un préjudice significatif aux personnes dont les données ont été compromises.

Par ailleurs, l'obligation de notification prévue dans la directive 2009/136/CE pourrait *a priori* également s'appliquer à des données qui ne seraient pas des données à caractère personnel[10], opérant alors une fusion avec l'obligation de notification de la directive *« cadre »*, applicable elle aussi à tout type de données mais circonscrite spécifiquement au domaine des réseaux et services d'accès aux réseaux.

Reste que cette obligation, telle qu'elle est prévue pour l'heure dans les directives 2002/21/CE modifiée (« *cadre* ») et 2002/58/CE modifiée (« *vie privée et communications électronique* »), apparaît double, sans lien apparent entre chacune de ses composantes, aucune des deux directives ne mentionnant l'autre au sujet de cette obligation pourtant d'apparence gémellaire et destinée à se généraliser.

II. Notifier les incidents de sécurité… doublement ?

En effet, une analyse attentive permet de déterminer que si la problématique apparaît commune, les modalités d'application, voire les autorités à saisir lors de cette notification semblent parfaitement dissemblables.

A. Conditions d'application de l'obligation de notification

Comme l'on pouvait s'en douter, l'origine des directives dans lesquelles sont insérées les deux obligations de notification explique quelques différences :

1. La directive « *cadre* », qui s'applique aux fournisseurs des réseaux de communications publics ou des services de communications électroniques accessibles au public tels que les fournisseurs d'accès à l'internet, ne conditionne pas ainsi la notification au caractère intrinsèque des données accédées *via* la faille de sécurité mais du fait même de l'existence d'une faille. Il faut, d'après le texte, qu'il y ait une atteinte portée à la sécurité ou une perte d'intégrité « *ayant eu un* ***impact significatif*** *sur le fonctionnement des réseaux ou des services* »[11]. La notification consiste en une information de « *l'autorité réglementaire concernée* » (v. B. *infra*) qui informe, le cas échéant, les autorités concernées des autres Etats membres et l'ENISA (l'Agence européenne chargée de la sécurité des réseaux et de l'information) dont on verra qu'elle joue, en matière de notification des incidents de sécurité, un rôle central.

Le public n'est informé par l'autorité nationale ou, au choix de l'autorité, par le fournisseur victime de la faille, qu'à deux conditions : en cas d'impact significatif sur le fonctionnement, comme on l'a vu, mais également, critère supplémentaire, s'il est « *d'utilité publique* » de divulguer les faits. Notons que nulle part il n'est question d'exonération, alors qu'une telle possibilité aurait pu être imaginée, par exemple, en fonction du niveau de protection dont bénéficiait l'information dont la sécurité a été violée.

Le fait que l'autorité nationale remette chaque année à la Commission et à l'ENISA un rapport succinct sur les notifications et les suites données finit de convaincre le lecteur de ces dispositions : **nous nous trouvons dans ce cas dans une notification des atteintes de sécurité opérée dans un souci de visibilité et d'établissement de statistiques fiables afin de permettre une action concertée et efficace des règles de sécurité qu'il convient d'appliquer et qui serviront d'étalon de mesure**. C'est ce qui explique notamment qu'il n'existe pas de critères d'exonération à cette obligation de notification (chiffrement des données, etc.). L'on comprend mieux également les dispositions des §. 1 et 2 du même article 13bis qui imposent notamment aux Etats membres de veiller à ce que ces fournisseurs prennent des mesures « *techniques et organisationnelles adéquates* [… qui] *garantissent un niveau de sécurité adapté au risque existant* », ainsi et surtout que les dispositions de l'article 13 ter. Avec ce dernier article en effet, les autorités nationales compétentes

[10] V. notamment le considérant 59 de la directive 2009/136/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 […]* ».

[11] Art. 13 bis §. 3 de la directive 2002/21/CE modifiée.

disposent du pouvoir d'obtenir des informations d'évaluation de la sécurité ou de l'intégrité des services ou réseaux fournis, d'obliger à la mise en place d'audits de sécurité dont ils ont communication des résultats et enfin d'enquêter sur les cas de non-conformité et leurs effets.

En ce qui concerne ces mesures techniques et la forme que doivent emprunter les notifications, étant donné que ce sont des mesures d'application visant à modifier des éléments non essentiels de la directive « *cadre* » en la complétant, ces mesures pourront être arrêtées par la suite en conformité avec la procédure européenne de « *réglementation avec contrôle* ». Rappelons que cette procédure un peu particulière permet une prise de décision plus adaptée à la pratique grâce à la consultation de comités composés d'experts des États membres (elle s'inscrit en cela dans le cadre de la « comitologie ») tout en conférant un droit de veto au Parlement et au Conseil[12]. Ce mécanisme de réglementation sera allié au fait que la Commission est appelée non seulement à consulter l'ENISA en tenant « *le plus grand compte* » de son avis, mais également de s'appuyer, « *dans toute la mesure du possible* » sur d'éventuelles normes européennes et internationales existantes. Cette architecture démontre - s'il le fallait - l'importance pour l'Union Européenne de prévoir en la matière des solutions à la fois pragmatiques et les plus proches possibles de l'état de l'Art en matière de sécurité, que celui-ci soit européen ou international.

2. La directive « *vie privée et communications électroniques* » agit de manière radicalement opposée. Cette opposition ne réside pas dans la définition extrêmement large de la notion de « *violation de données à caractère personnel* », considérée comme « *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* », ni dans le fait que le §. 3 de l'article 4 de cette directive prévoit une obligation de notification « à géométrie variable ». Tout comme dans la directive « *cadre* », en effet, **toute hypothèse de violation de données personnelles, indépendamment du nombre de victimes de cette violation, entraîne dans tous les cas l'obligation d'en avertir l'autorité nationale compétente** (sur la détermination de cette autorité, v. *infra*). Cet avertissement doit préciser au minimum la nature de la violation, les points de contact mis en place, les recommandations faites aux victimes, les conséquences et les autres mesures prises, et doit se faire, dans le cadre de cette directive, « *sans retard indu* ». Notons que le texte prévoit l'ensemble de ces informations mais qu'en pratique, ce n'est que si la violation est « *de nature à affecter négativement les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier* » que le fournisseur est tenu d'en informer, sans retard indu, *« l'abonné ou le particulier concerné* », et donc de lui faire part de la nature de la violation, mais surtout des points de contact mis en place et des recommandations pour en atténuer les conséquences. On s'étonnera d'ailleurs de constater que la notification à l'autorité compétente, de par les informations demandées et notamment *« les points de contact auprès desquels des informations supplémentaires peuvent être obtenues* » (numéro vert ?), suppose nécessairement que de tels moyens aient déjà été mis en œuvre et donc que soit présumé l'effet négatif de cette violation de sécurité. On le comprend aisément concernant une violation de sécurité dont on s'aperçoit immédiatement des effets, moins pour une alerte de sécurité notifiée ayant des effets finalement plus graves après enquête…

Autre point d'attache entre les deux directives, les autorités nationales compétentes peuvent émettre des recommandations sur les meilleures pratiques que les fournisseurs doivent mettre en œuvre en matière de sécurité.

Par contre, à la différence de la directive « *cadre* », ces obligations de notification et de sécurisation ne s'appliquent qu'aux seuls fournisseurs de services de communications électroniques accessibles au public tels que les fournisseurs d'accès à l'internet, alors même que la directive « cadre » s'appliquait également aux fournisseurs des réseaux de communications publics. Et, autre différence, l'information de l'abonné ou du particulier concerné n'est obligatoire que si les informations à caractère personnel « *violées* » n'ont pas été rendues techniquement « *incompréhensibles* ». On pense ici aux données chiffrées auxquelles une tierce personne aurait accédé indûment, leur chiffrement efficace rendant inutile l'alerte des personnes concernées. Il s'agit de la reprise d'un principe issu des législations américaines, qui avaient déjà prévu cette condition d'exonération : les

[12] Procédure créée par la Décision du Conseil du 17 juillet 2006 (2006/512/CE) « *modifiant la décision 1999/468/CE fixant les modalités de l'exercice des compétences d'exécution conférées à la Commission* » (cette dernière Décision ayant institué la comitologie).

bons élèves de la sécurité qui n'avaient pas attendu pour protéger les données dans leurs systèmes sont ainsi récompensés, même en cas d'intrusion ou d'accès indu. Il leur restera toutefois à prouver effectivement l'efficacité de leur dispositif, « *à la satisfaction de l'autorité compétente* », qui gagne là une arme de plus pour imposer sa vision du niveau de sécurité exigible, au détriment de l'appréciation du fournisseur, sans doute considéré comme subjectif.

La directive prévoit également deux niveaux de contrôle de cette notification faite aux particuliers et clients, au cas où le fournisseur n'aurait pas jugé utile de les prévenir : l'autorité, notifiée au premier chef, a le pouvoir de forcer le fournisseur à effectuer cette information et de le sanctionner. Et le fournisseur a l'obligation de tenir un inventaire à jour des violations et de leurs suites (contexte, effets, mesures prises).

Dans tous les cas de notification, la directive « *vie privée et communications électroniques* » prévoit « *des sanctions appropriées* » en cas d'inobservation de ses prescriptions.

Pour conclure sur ce point, notons que, dans cette directive également, la procédure européenne de « *réglementation avec contrôle* » précitée est également recherchée pour préciser les mesures d'application telle que les circonstances entraînant obligatoirement pour les fournisseurs l'obligation de notifier, ou encore le format et la procédure de notification. Une approche absolument identique à celle de la directive « *cadre* » est donc suivie sur ce point, de même que la consultation nécessaire de l'ENISA. Seule différence : il n'est plus fait référence à un appui « *dans la mesure du possible, sur des normes européennes et internationales* » existantes en la matière, mais il est plutôt fait appel, de façon logique, à la consultation 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* » (dit « *groupe de l'article 29* ») et du « *contrôleur européen de la protection des données* » (ou CEPD). Sous réserve des mesures adoptées ainsi, les autorités nationales compétentes peuvent édicter des lignes directrices voire des instructions sur les mêmes domaines.

B. « Les » autorités réglementaires nationales concernées ?

Toute la question est de savoir en effet qui sont, au juste, les « *autorités réglementaires nationales »* mentionnées tout au long de ces dispositions nouvelles. Le lecteur abordant une des deux directives précitées aura une tendance naturelle à le déterminer en fonction de sa « grille de lecture » habituelle :

- Le spécialiste de droit des communications électroniques, abordant la directive « *cadre* » en premier, considérera sans aucun doute qu'il s'agit pour la France de l'ARCEP (Autorité de Régulation des Communications Electroniques et des Postes), compte tenu du rôle, des pouvoirs et de la compétence de cette autorité[13]. Ne lui en déplaise, il nous semble pour notre part que ce choix serait pourtant le moins logique, compte tenu des autres organismes en lice.

- En effet, le féru de protection des données à caractère personnel pourra, lui, envisager, sans se poser d'autres questions, que « *l'autorité nationale compétente en la matière* » dont il est question dans la directive 2002/58/CE modifiée est, comme il se doit, la CNIL (Commission Nationale de l'Informatique et des Libertés). En effet, cette autorité, dont le rôle central sur ces problématiques est

[13] L'ARCEP a été créée par la loi n° 2005-516 du 20 mai 2005 en tant qu'autorité administrative indépendante, venant alors remplacer l'ART (Autorité de Régulation des Télécommunications), créée elle-même par loi n° 96-659 du 26 juillet 1996, qui avait alors pour mission de réguler la concurrence et permettre l'ouverture du secteur des télécommunications. L'ARCEP a aujourd'hui pour principales missions d'encourager la concurrence au bénéfice des utilisateurs et notamment leur accès aux infrastructures, de veiller à la fourniture du service public des télécommunications, au développement de l'innovation et de la compétitivité dans le secteur des communications électroniques. Ces missions ont été précisées depuis la transposition en France du Paquet Télécom de 2002 par la loi n°2004-669 relative aux communications électroniques et aux services de communication audiovisuelle (dite de transposition du « *Paquet Télécom* » - 1er du nom) adoptée le 9 juillet 2004**,** la loi n° 2004-575 pour la confiance dans l'économie numérique (« *LCEN* ») adoptée le 21 juin 2004, et la loi n° 2003-1365 relative aux obligations de service public des télécommunications et à France Telecom adoptée le 31 décembre 2003). En pratique, l'ARCEP procède plus particulièrement à l'analyse des marchés et fixe les obligations qui s'y attachent, elle reçoit les déclarations des opérateurs, elle attribue et gère les ressources rares (fréquences, ressources en numérotation, etc.), fixe les règles relatives au service universel, aux tarifs applicables, règle les litiges entre opérateurs et dispose d'un pouvoir de sanction auprès des opérateurs ne respectant pas leurs obligations.

indiscutable, est déjà en charge des autres problématiques traitées dans cette directive (courriers électroniques non sollicitées, etc.) et reste l'interlocuteur habituel dans le cadre de la directive plus communément appelée, rappelons-le, « *vie privée et communications électroniques* ». D'autant plus que le §. 5 de l'article 4 de cette directive modifiée mentionne spécifiquement à la fois le « groupe de l'article 29 » et le CEPD comme devant absolument être consultés avant que la Commission adopte les mesures d'application sur les circonstances, le format et la procédure de notification. Pour ce lecteur, l'affaire paraîtrait entendue sans autre forme de procès.

- Enfin, un spécialiste de la sécurité des systèmes d'information, n'ayant aucun *a priori* sur ces textes et les découvrant dans leur ensemble, aura sans doute une tendance bien naturelle à considérer que ces notification de failles de sécurité doivent être coordonnées au niveau français par la nouvelle Agence Nationale de la Sécurité des Systèmes d'Information créée par le décret n° 2009-834 du 7 juillet 2009[14] (ANSSI, ex-DCSSI[15]). Qui d'autre en effet que celle qui est rattachée au Secrétaire général de la défense nationale et surtout qui a « *mission d'autorité nationale en matière de sécurité des systèmes d'information* » pourrait s'occuper valablement de ces questions ? Qui d'autre que cet organisme pourrait être le point de contact français le plus logique de l'ENISA, entité que les deux directives mentionnent et qui apparaît comme le seul point commun de ces deux réglementations sœurs ?

On le voit, il n'est donc pas simple d'anticiper qui sera institué par la France comme étant l'interlocuteur (voire plus probablement **les** interlocuteurs ?) d'un fournisseur d'accès souffrant d'une violation de sécurité ayant « *un impact significatif sur son fonctionnement* » et dans le même temps « *affectant négativement les données à caractère personnel* » de plusieurs clients.
Etant entendu que l'on n'ose guère imaginer un système où les interlocuteurs – et donc les modalités de notification et les mesures correctrices – seraient différents selon que la violation de sécurité n'aurait pas d'impact significatif sur le fonctionnement mais affecterait « *négativement les donnés à caractère personnel* » de plusieurs clients, ou au contraire, n'ayant pas d'impact négatif sur celle-ci aurait plutôt un impact significatif sur le fonctionnement du réseau du fournisseur d'accès. On n'ose guère l'imaginer et pourtant…

Sachant que ce nouveau « *Paquet Télécom* » fera l'objet d'une transposition en droit national sur une période de dix-huit mois ayant débuté le 18 décembre (publication au JOUE), le départ est maintenant officiellement donné pour l'attribution et surtout la coordination des compétences de chacun… pour le bien des clients mais également pour la lisibilité des règles par les fournisseurs de réseaux et de services qui seront en première ligne !

[14] Journal Officiel de la République Française (JORF) du 8 juillet 2009.
[15] Direction Centrale de la Sécurité des Systèmes d'Information. L'ANSSI, dont la création a été décidée par le Président de la République suite aux travaux du Livre blanc sur la défense et la sécurité nationale présenté le 17 juin 2008, se substitue à cette Direction tout en en renforçant ses compétences, ses effectifs et ses moyens.