# La protection des réseaux numériques en tant qu'infrastructures vitales

Bertrand Warusfel - *Professeur à l'Université de Lille 2, Avocat au barreau de Paris (cabinet FWPA)*

Les activités numériques sont considérées de longue date comme recelant de grandes vulnérabilités. Si Bertrand Warusfel évoque cette ancienne prise de conscience, il constate que la démultiplication des supports numériques, la généralisation du numérique chez les particuliers et l'interconnexion de ces réseaux dans un contexte mondialisé rendent ce secteur d'activité d'importance vitale plus exposé que jamais. L'auteur évoque par la suite un paradoxe inhérent à la sécurité des réseaux numériques : ceux-ci étant détenus et exploités par les seuls opérateurs privés, des dispositions juridiques interdisent que certaines informations relatives à leurs réseaux physiques soient communiquées aux autorités publiques. Une privatisation de la sécurité qui ne doit pas occulter l'arsenal de plus en plus développé dont disposent ces mêmes autorités pour lutter contre la cybercriminalité.

Parmi les installations d'importance vitale dont la protection est organisée par l'article 1332-1 du Code de la défense et ses textes d'application, on peut classer certains réseaux de communication électronique. L'arrêté du 2 juin 2006 désigne, en effet, parmi les secteurs d'activité d'importance vitale, un secteur dénommé largement : «Communications électroniques, audiovisuel et information». Cette classification – et toutes les conséquences juridiques et opérationnelles qui en découlent – est logique au regard des risques importants que peut faire courir aux intérêts collectifs une éventuelle insécurité des réseaux numériques. Mais la nature particulière de ces réseaux, et notamment leur dimension ouverte et planétaire, rend plus difficile leur prévention efficace contre d'éventuelles menaces organisées. On ne doit donc pas surestimer l'état actuel de la sécurité des systèmes en France et en Europe. Au contraire, un renforcement des politiques de sécurité et de prévention, l'adaptation continuelle de nos moyens de riposte juridiques ainsi qu'une sensibilisation accrue des opérateurs et des entreprises, sont très nécessaires.

## Les enjeux sécuritaires des réseaux numériques

La prise en compte des risques inhérents à la numérisation des activités économiques et sociales n'est pas récente. Le rapport de la commission SARK, établie par le ministère suédois de la défense entre 1977 et 1979, sur la vulnérabilité de la société informatisée, est souvent considéré comme un travail précurseur en la matière[1]. En effet, ce rapport ne se contentait pas d'identifier la vulnérabilité intrinsèque des systèmes d'information (lesquels – comme tout système – peuvent dysfonctionner et cesser de remplir les fonctions qui sont les leurs) mais prenait en compte les conséquences que ces défaillances pourraient avoir sur le fonctionnement plus général des activités sociales qui en

dépendent. De plus, il concluait que des atteintes majeures aux systèmes informatiques susceptibles d'affecter la sécurité de la collectivité pouvaient survenir non seulement en situation de crise ou de guerre, mais aussi en période de paix. Si les analyses détaillées de ce rapport (mettant en avant les risques propres aux architectures informatiques très centralisées de l'époque) datent et ne sont plus directement appropriées aujourd'hui, la typologie générale des facteurs pouvant affecter la sécurité d'une société numérisée (comme la nôtre l'est encore plus qu'il y a trente ans) demeure très pertinente. Elle distinguait les seize «facteurs de risque» suivants :

- actes délictueux à l'encontre des systèmes d'information ;
- utilisation politique de certaines formes de restrictions ou de sanctions commerciales sur la fourniture d'éléments techniques sensibles ;
- actes de guerre affectant les infrastructures numériques ;
- catastrophes naturelles ou accidents ;
- existence de fichiers contenant des informations confidentielles susceptibles d'une utilisation déloyale ou illicite ;
- sensibilité particulière de certains systèmes utilisés dans des activités économiques, financières ou logistiques majeures ;
- concentration géographique et fonctionnelle des systèmes d'information, dans certaines zones vulnérables à des attaques ou des accidents ;
- intégration et interdépendance entre les systèmes, susceptibles d'entraîner une propagation des défaillances ;
- accumulation d'importants volumes de données dont la compilation et le croisement peuvent donner lieu à des exploitations en termes de renseignement ;
- formation déficiente et inadéquate des utilisateurs et des entreprises en ce qui concerne les risques et les pratiques de sécurité ;
- insuffisante qualité des matériels et des logiciels, capables d'entraîner des incidents techniques ayant des conséquences à long terme ;
- écart trop grand entre les utilisateurs et les informaticiens, lesquels peuvent devenir eux-mêmes des cibles pour des attaques contre les systèmes qu'ils gèrent ;
- insuffisante documentation ;
- insuffisance des plans d'urgence et des dispositifs de reprise d'activité en cas d'accidents ou de situations d'urgence ;
- dépendance technologique vis-à-vis de sources étrangères ;
- flux internationaux de données rendant difficile la maîtrise locale des données et de leur traitement.

**Les nouvelles architectures sont beaucoup plus décentralisées que ce qui se faisait à la fin des années soixante-dix.**

La relecture de cette liste, avec le recul, nous montre que certaines tendances lourdes liées à la numérisation massive de nos activités sont toujours là. Certes, les nouvelles architectures sont beaucoup plus décentralisées que ce qui se faisait à la fin des années soixante-dix et des mesures nationales et européennes ont été prises dès cette époque pour prévenir d'éventuelles utilisations abusives des données personnelles[2] et plus tard pour réprimer la criminalité numérique (en France à partir de la loi Godfrain du 5 janvier 1988). Mais sans entrer ici dans un débat complexe, il semble possible d'affirmer que les gains en termes de sécurité et de prévention induits par ces évolutions techniques et juridiques sont largement contrebalancés par les effets considérables de l'accélération de la numérisation des activités et de leur globalisation sous l'effet Internet.
Les risques déjà décelés qui découlent de la complexité des systèmes, de la dépendance technologique sur leurs composants essentiels

[1] *The Vulnerability of the Computerised Society: Considerations and Proposals, Report of the SARK Committee, 1979.*
[2] *Citons la directive communautaire 95/46/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 de ces données (et ses nombreuses déclinaisons spécialisées, notamment en ce qui concerne les communications électroniques) et, pour la France, la loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi du 6 août 2004.*

(non seulement certains composants électroniques physiques, mais avant tout aujourd'hui les composants logiciels), du manque de pratique de la sécurité par les utilisateurs ou encore de l'explosion des échanges mondiaux de données sont donc de plus en plus présents. Par ailleurs, la démocratisation des systèmes d'information (équipements domotiques, terminaux mobiles...) induit un accroissement (et un déplacement) de ces vulnérabilités, puisqu'elle touche des utilisateurs personnels encore moins bien sensibilisés ou formés et des équipements dont les fonctionnalités de sécurité et la protection sont limitées pour des raisons économiques et physiques. Enfin, l'intuition majeure du rapport de 1979 demeure d'une brûlante actualité : l'insécurité des systèmes d'information n'entraîne pas seulement des effets au niveau de ces systèmes eux-mêmes. Elle est susceptible d'avoir des effets directs et indirects immenses puisque l'ensemble des activités économiques, sociales (et progressivement domestiques) reposent sur ces systèmes. Dès lors, si l'on ajoute le facteur de démultiplication (déjà perçue par le rapport SARK) qu'induit l'interconnexion des réseaux et leur mondialisation, on comprend qu'il soit pertinent d'un point de vue théorique de considérer que les réseaux numériques les plus importants doivent être considérées comme des infrastructures vitales pour la collectivité.

## L'apport de la réglementation sur les secteurs d'importance vitale

La logique de la protection des installations d'importance vitale pour la nation est ancienne et s'est concrétisée par l'ordonnance du 29 décembre 1958[3]. Elle concerne les établissements, installations et ouvrages «dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation». La relance à partir de 2006 du grand chantier sur la protection des secteurs d'importance vitale n'en a pas changé les finalités essentielles. Tout au plus, le nouvel article L1332-1 CD concerne-t-il plus explicitement les «*opérateurs publics ou privés*» (et non plus seulement les entreprises) et – plus important – il ne s'agit plus seulement que les exploitants assurent la protection des installations contre les risques de «*sabotage*» (comme dans le texte initial de 1958) mais contre «*toute menace, notamment à caractère terroriste*».

**Il ne s'agit plus seulement que les exploitants assurent la protection des installations contre les risques de «sabotage» (comme dans le texte initial de 1958) mais contre «toute menace, notamment à caractère terroriste».**

C'est cependant de la déclinaison règlementaire de ce dispositif qu'est venue l'innovation consistant à identifier non plus simplement des établissements et des installations, mais à cibler plus globalement des «secteurs d'activité» d'importance vitale et de désigner au sein de ces différents secteurs les «opérateurs d'importance vitale», dont ceux visés par l'article L1332-1 précité. En retenant le secteur «Communications électroniques, audiovisuel et information» parmi la liste des douze secteurs d'activités d'importance vitale, l'arrêté du 2 juin 2006[4] a considéré que le domaine des réseaux numériques remplissait les conditions posées par le nouvel article R.1332-2 du code de la défense[5] : ils sont donc considérés comme ayant trait à la production et la distribution de «biens ou de services indispensables» à la réalisation de l'un ou plusieurs des cinq objectifs suivants :

- la satisfaction des besoins essentiels pour la vie des populations ;
- l'exercice de l'autorité de l'Etat ;
- le fonctionnement de l'économie ;
- le maintien du potentiel de défense ;
- la sécurité de la Nation.

Si la généralité du dernier objectif ne permet

[3] *Ordonnance n°58-1371 du 29 décembre 1958 tendant à renforcer la protection des installations d'importance vitale, JORF du 31 décembre 1958, p. 12064 (aujourd'hui codifiée aux articles L.1332-1 et suivants du code de la défense).*

[4] *Arrêté du Premier ministre du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs, modifié par l'arrêté du 3 juillet 2008.*

[5] *Issu de l'article 2 du décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale.*

pas d'en faire une application discriminante dans le cas présent, on peut penser que les réseaux numériques font bien partie de ces infrastructures indispensables à la satisfaction des besoins des populations et au fonctionnement de l'économie. De même, il n'est pas difficile de comprendre que les moyens de fonctionnement de l'Etat ainsi que la mise en œuvre éventuelle de mesures de défense ne peuvent plus s'envisager aujourd'hui sans le recours à un tel type d'infrastructures[6].

Par ailleurs, le même article prescrit que les activités d'importance vitale doivent – logiquement - être «*difficilement substituables ou remplaçables*». Si cela n'est certainement pas le cas de tous les réseaux numériques (qui sont souvent, au contraire, partiellement ou totalement substituables les uns aux autres), on peut convenir que dans son ensemble le secteur n'est pas substituable (car il n'existe pas aujourd'hui – à grande échelle – une alternative aux communications numériques) et que pris séparément, certains réseaux numériques d'infrastructures (comme ceux des principaux opérateurs nationaux de télécommunications et de fourniture d'accès à Internet) ne pourraient pas cesser de fonctionner sans engendrer de graves dysfonctionnements pour le contexte social, économique et administratif. Il en va évidemment de même si l'on prend comme élément de référence la définition d'une «infrastructure critique» donnée par la directive communautaire du 8 décembre 2008 comme ce qui est «*indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'arrêt ou la destruction aurait un impact significatif dans un État membre du fait de la défaillance de ces fonctions*»[7]. Dès son Livre vert de 2005, la Commission européenne a d'ailleurs considéré que le secteur de l'information et des technologies de communication comptait sept des trente-sept types d'infrastructure critique[8].

**Dès son Livre vert de 2005, la Commission européenne a d'ailleurs considéré que le secteur de l'information et des technologies de communication comptait sept des trente-sept types d'infrastructure critique.**

**On ne s'étonnera donc pas non plus de compter parmi les dix personnalités nommés membre du Comité national des secteurs d'activités d'importance vitale, les dirigeants de deux entreprises de premier plan en matière de communications numériques : France Telecom et Télédiffusion de France.**

On ne s'étonnera donc pas non plus de compter parmi les dix personnalités nommées membres du Comité national des secteurs d'activités d'importance vitale, les dirigeants de deux entreprises de premier plan en matière de communications numériques : France Telecom et Télédiffusion de France[9]. Cette sélection ne fait que reconnaître l'importance majeure de ce secteur parmi l'ensemble des secteurs d'importance vitale en France[10]. Il est ainsi parfaitement cohérent que les réseaux numériques et les activités de communication et de traitement d'information qu'ils permettent soient identifiés comme un secteur d'impor-

[6] *Sur l'importance des questions de sécurité de l'information pour les Etats et leurs politiques de défense et de sécurité, v. (pour un point de vue ancien, et donc nécessairement à replacer dans le contexte de l'époque) notre article : B. Warusfel, "Sécurité informatique et secret de défense", Revue Défense nationale, 1986/2 ; et pour un point de vue récent : Alain Esterlé, "La sécurité de l'information et des Etats est – elle une affaire d'Etat(s) ?", Annuaire Français de Relations Internationales, Volume X, 2009.*

[7] *Article 2 de la directive 2008/114 du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.*

[8] *A savoir : protection des systèmes d'information et des réseaux ; automatisation des instruments et des systèmes de contrôle ; Internet ; fourniture de télécommunications fixes ; fourniture de télécommunications mobiles ; communication radio et radionavigation ; communication par satellite ; radiodiffusion (Commission européenne, Livre vert relatif au programme européen de protection des infrastructures critiques, 17 novembre 2005).*

[9] *Arrêté du 8 décembre 2009, JORF n°0286 du 10 décembre 2009.*

[10] *Même si l'on aurait pu s'attendre à ce qu'il ne soit pas fait uniquement le choix de dirigeants d'entreprise issues du secteur public, pour mieux manifester l'implication du secteur privé concurrentiel dans cette logique de sécurité globale.*

tance vitale au sens du Code de la défense. Mais c'est aussi la nature de ce marché qui rend utile une telle logique de prévention et de défense. En effet, la réglementation sur les secteurs d'importance vitale a pour vocation d'associer les opérateurs privés à la mise en place de mesures de prévention définies par l'autorité publique, au nom des impératifs de défense et de sécurité nationale[11]. Elle a donc la double caractéristique d'une approche partenariale public-privé et d'une obligation légale, ce que l'on pourrait résumer autour de la notion de «partenariat contraint».

**Dès l'origine, en effet, les licences délivrées par l'autorité de régulation (aujourd'hui, l'Autorité de régulation des communications électroniques et de la poste, ARCEP) comportaient des obligations notamment en ce qui concerne la défense nationale et la sécurité publique.**

Cette logique est adaptée à la nature contemporaine du marché des communications électroniques et des réseaux numériques, puisque celui-ci est aujourd'hui entre les mains d'opérateurs privés (même si le premier d'entre eux – France Telecom - demeure une entreprise issue du secteur public et où l'Etat conserve un peu plus de 25% du capital) mais qui se voient soumis, en fonction de leurs activités, à certaines obligations de service public (notamment lorsqu'ils gèrent en propre un réseau physique de communication). Dès l'origine, en effet, les licences délivrées par l'autorité de régulation (aujourd'hui, l'Autorité de régulation des communications électroniques et de la poste, ARCEP) comportaient des obligations notamment en ce qui concerne la défense nationale et la sécurité publique[12]. Mais la prise en compte de leurs obligations spécifiques en matière de sécurité s'est accrue dans ces dernières années. Prenant ses fonctions de Président de l'ARCEP, M. Jean-Claude Mallet, ancien SGDN, déclarait ainsi en janvier 2009 : *«En travaillant sur les conséquences de la mondialisation en matière de défense et de sécurité, il m'est apparu de façon évidente que les questions liées à la révolution numérique et aux réseaux étaient fondamentales pour la sécurité du pays et de l'Europe. (...) La sécurité n'a jusqu'à présent pas fait l'objet d'une intense mobilisation, ni au ministère, ni à l'Arcep. La loi de 2004 oblige pourtant à traiter la question de l'intégrité et de la fiabilité des réseaux d'une part, du rôle de ces réseaux en matière de sécurité publique et de défense d'autre part. De leur côté, les opérateurs ne se préoccupent que de leur propre protection. Or le déni d'accès à Internet et aux réseaux de télécommunications serait une catastrophe. Il est donc indispensable, en amont, de développer une capacité de résistance ou de résilience des réseaux ; cela doit, à mon sens, être inscrit dans l'agenda du président de l'Arcep»*[13].

Cette nécessité d'associer, plus encore qu'ailleurs, les entreprises privées aux impératifs publics de sécurité n'est pas nouvelle. Déjà en 1983, des auteurs américains pouvaient écrire que *«l'essentiel de la responsabilité concernant la résilience de l'information aux USA repose sur le secteur privé. Les organisations d'usagers, tout comme les fournisseurs de systèmes d'information ou de services, doivent déterminer les mesures de précaution qu'il est raisonnable de prendre et accepter de payer pour cela»*[14]. On ne peut donc pas admettre sans réserve que *«la sécurité des réseaux et de l'information reste clairement une affaire d'Etat, dans la mesure où l'Etat y est impliqué en premier chef et y exerce une responsabilité directe»*[15]. Certes des exemples comme l'attaque DDoS contre l'Internet

[11] *Sur la nouvelle architecture juridique française qui distingue les notions de défense nationale et de sécurité nationale, v. notre article : B. Warusfel, "Le cadre juridique des relations entre défense et sécurité nationale", Cahiers de la sécurité, INHESJ, n° 14, (à paraître : novembre 2010).*

[12] *L'article L.32-1 II 6° du Code des Postes et des communications électroniques dispose ainsi que le ministre en charge ainsi que l'ARCEP doivent veiller "au respect, par les exploitants de réseau et les fournisseurs de services de communications électroniques de l'ordre public et des obligations de défense et de sécurité publique".*

[13] *Assemblée nationale, Commission des affaires économiques, de l'environnement et du territoire, audition de M. Jean-Claude Mallet, mercredi 17 décembre 2008, séance de 10 heures 30, compte rendu n° 24. M. Mallet a démissionné en avril 2009 pour raisons de santé.*

[14] *Rein Turn & Eric J. Novotny, Resiliency of the Computerized Society, National Computer Conference, 1983, p. 349.*

estonien en 2007 ou le cas très récent de l'infection par le virus Stuxnet montrent que des Etats pourraient être la cible ou l'auteur d'attaques cybernétiques. Mais si cette responsabilité étatique reste donc nécessaire et éminente (et justifie la mise en place de la réglementation des secteurs d'importance vitale) elle ne peut fonctionner désormais – et particulièrement dans ce secteur – que selon un mode partenarial, tant vis-à-vis des entreprises privées que des autres Etats ou institutions européennes et internationales[16].

**L'opérateur a dû déterminer les points névralgiques de son système et les proposer à l'administration pour classement en tant que points d'importance vitale.**

En application de cette reconnaissance règlementaire comme secteur d'importance vitale, les principaux opérateurs du domaine sont donc désormais assujettis au respect de la directive nationale de sécurité (DNS) propre à la protection du secteur des infrastructures numériques et à chacun de ses sous-secteurs. Bien qu'elle soit classifiée, on sait que sur cette base, chaque opérateur d'importance vitale doit élaborer un plan de sécurité dont l'objet est de définir sa politique générale de protection pour ses établissements, installations et ouvrages, notamment pour ceux organisés en réseaux. Le plan comporte des mesures permanentes (le socle de protection, ou posture permanente de sécurité) et des mesures graduées activées en cas d'alerte transmise par l'autorité publique. L'opérateur a dû déterminer les points névralgiques de son système et les proposer à l'administration pour classement en tant que points d'importance vitale. Pour chacun de ces points, il a dû établir un plan de protection interne, découlant de son plan d'opérateur comportant des mesures permanentes de protection et des mesures graduées d'application temporaire[17]. Mais par delà cette mise en œuvre des mesures découlant de la directive nationale de sécurité sectorielle, le domaine des réseaux numériques peut également s'appuyer sur d'autres moyens juridiques contribuant à sa sécurité.

## La sécurité des réseaux numériques doit être complétée, notamment sur le plan juridique

Le propre des infrastructures et des services de communication numérique est que leur sécurité ne peut se limiter à la mise en œuvre par certains opérateurs spécifiquement désignés des mesures imposées par leur directive nationale de sécurité sectorielle. En effet, dans un monde complexe et interconnecté dans lequel chaque opérateur ou réseau est en communication avec les autres, tout opérateur de réseaux ou de services numériques doit respecter un niveau suffisant de sécurité pour ne pas contribuer à l'affaiblissement de celle des autres.

**En effet, dans un monde complexe et interconnecté dans lequel chaque opérateur ou réseau est en communication avec les autres, tout opérateur de réseaux ou de services numériques doit respecter un niveau suffisant de sécurité pour ne pas contribuer à l'affaiblissement de celle des autres.**

Certaines dispositions concernent donc l'ensemble des opérateurs et non seulement ceux en charge des infrastructures critiques du secteur. Un bon exemple peut en être donné par deux textes récents qui – selon une

[15] *A. Esterlé, op. cit., 2009.*

[16] *A. Esterlé lui-même reconnaît d'ailleurs immédiatement que "néanmoins, les modalités de cette implication et l'exercice de cette responsabilité ont sensiblement évolué avec l'émergence d'acteurs, qu'ils soient non étatiques (opérateurs de systèmes de communication électronique, autorité de régulation) ou qu'ils relèvent de nouvelles coopérations interétatiques".*

[17] *Sur les conditions d'application des Directives nationales de sécurité, v. l'Instruction générale interministérielle relative à la sécurité des activités d'importance vitale n° 6600/SGDN/PSE/PPS du 26 septembre 2008.*

approche assez innovante – ont précisé la nature et les limites des informations que les opérateurs d'infrastructures et de réseaux numériques doivent communiquer aux autorités publiques. Le premier décret du 12 février 2009 précise les données confidentielles dont les pouvoirs publics nationaux ou locaux ont besoin pour assurer leurs missions et pour avoir une réelle connaissance détaillée des réseaux qui sont établis sur leur territoire (notamment en vue de pouvoir intervenir si nécessaire dans le cas où des mesures urgentes de sécurité le justifieraient)[18]. Mais bien que ce premier texte oblige les opérateurs et les autorités concernées à prendre toutes les mesures nécessaires pour assurer la confidentialité de ces données, un second texte paru en 2010 complète le précédent en venant établir la liste des informations relatives à ces mêmes réseaux qu'il est interdit aux opérateurs de communiquer aux autorités publiques lorsqu'il s'agit de certaines infrastructures vitales ou de certaines installations sensibles (au sens du code de la défense) ou lorsque la précision topographique de la situation de certains nœuds de réseaux ou de points de desserte serait trop importante[19].

**S'institue ainsi ici une forme de secret industriel et technologique détenu par l'opérateur pour des motifs de sécurité nationale, et ce même et y compris à l'encontre des autorités publiques.**

Voici donc – pour des raisons de sécurité nationale – que des mesures règlementaires viennent (pour la première fois, à notre sens) limiter la diffusion à l'autorité publique (et notamment aux collectivités locales, qui n'ont pas toutes la possibilité d'assurer une sécurité optimale de l'information) de certaines informations sensibles, afin d'éviter que cette communication puisse donner lieu à une diffusion mal contrôlée ou à des fuites qui seraient dommageables. Cela exprime bien à nouveau nous semble-t-il le paradoxe de la sécurité des réseaux numériques : ceux-ci étant détenus et exploités par les seuls opérateurs privés, leur sécurité peut parfois conduire à recommander que seuls ceux-ci soient détenteurs des données topographiques détaillées qui permettraient à des tiers malveillants de porter atteinte à l'intégrité de ces réseaux. S'institue ainsi ici une forme de secret industriel et technologique détenu par l'opérateur pour des motifs de sécurité nationale, et ce même et y compris à l'encontre des autorités publiques.

De plus, à la sécurisation physique des nœuds de réseau (à laquelle concourt directement l'application des dispositions relatives aux secteurs d'importance vitale), doit s'ajouter une protection logique des réseaux. Dans cette perspective, l'autre support règlementaire qui peut, au moins indirectement, inspirer les efforts de sécurisation des opérateurs de réseaux numériques est le nouveau Référentiel général de sécurité (RGS) récemment établi par l'Etat (en l'occurrence, via sa nouvelle agence nationale de la sécurité des systèmes d'information, l'ANSSI) en vue de servir de base aux mesures de sécurité que doivent respecter les personnes publiques à l'occasion de la mise en œuvre de leurs services numériques[20]. Certes il ne s'agit là que d'un document de référence pour les services numériques du secteur public et rien n'impose aux opérateurs privés de s'y référer, mais on peut penser que certaines de ses recommandations vont acquérir le statut de bonnes pratiques reconnues comme constituant l'état de l'art (ce qui limiterait les risques de mise en cause de la responsabilité des opérateurs qui choisiraient volontairement de s'y conformer). Plus généralement, l'ensemble des disposi-

[18] *Décret no 2009-167 du 12 février 2009 relatif à la communication d'informations à l'Etat et aux collectivités territoriales sur les infrastructures et réseaux établis sur leur territoire, JORF du 14 février 2009.*

[19] *Décret no 2010-57 du 15 janvier 2010 relatif à la sécurité de la communication d'informations à l'Etat et aux collectivités territoriales sur les infrastructures et réseaux établis sur leur territoire, JORF du 17 janvier 2010.*

[20] *V. l'arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques, JORF du 18 mai 2010.*

tions répressives qui assurent la sanction des atteintes aux systèmes d'information constitue un pan important du dispositif public national de prévention contre les risques d'insécurité des réseaux numériques. On ne refera pas ici l'analyse détaillée de ces dispositions contenues essentiellement dans le code pénal[21] et qui sont conformes à l'harmonisation des dispositions pénales prescrites par la Convention sur la cybercriminalité du Conseil de l'Europe[22]. Que l'on se contente de dire que l'existence de ces infractions correctionnelles donne à la justice et aux services d'enquête les moyens juridiques de mener des investigations approfondies lorsque des pénétrations de réseau ou des attaques informatiques sont détectées et qu'elles permettent aussi de mettre en œuvre la coopération interétatique qui existe désormais entre tous les Etats signataires de cette Convention (Europe mais aussi Etats-Unis et Canada notamment) pour mener à distance et très rapidement les opérations de perquisition et de saisie des systèmes d'information suspects ou encore de récupération des données de trafics ou des interceptions de communication susceptibles d'aider à identifier leurs auteurs[23]. Et l'on peut y ajouter (même si leurs objectifs sont plus spécifiques et sont, par ailleurs, plus controversés), les différentes dispositions pénales et administratives créées par les lois successives de 2006 et de 2009 pour lutter contre la contrefaçon des œuvres numériques en ligne et leur téléchargement[24].

**Les instruments juridiques utilisables pour protéger les infrastructures vitales en matière de communication électronique ne sont donc pas inexistants.**

Les instruments juridiques utilisables pour protéger les infrastructures vitales en matière de communication électronique ne sont donc pas inexistants. Bien au contraire, ils constituent désormais un ensemble significatif au point qu'il faut maintenant réfléchir à leur cohérence et aux répercussions qu'ils peuvent avoir sur d'autres objectifs légitimes de l'action publique en matière de liberté de communication et de promotion des technologies numériques.

Le récent débat sur la neutralité de l'Internet[25] a mis, par exemple en valeur le fait que certaines contraintes qui peuvent être imposées aux opérateurs de communication au titre de la sécurité de leurs réseaux ou du filtrage de certains de leurs contenus pouvaient aller à l'encontre de cet objectif général de «neutralité du réseau» (lequel est lui-même pourtant l'une des conditions pour conserver une communication numérique sûre). C'est ce que relevait Nicolas Curien – membre de l'ARCEP - lors du colloque préalable organisé à cette occasion : *«en matière de neutralité des réseaux, les contraintes sont nombreuses. Il y a celles, déjà évoquées, qui sont liées à la gestion du trafic et à l'investissement dans les nouveaux réseaux d'accès. Il y a celles qui sont liées à la protection de la vie privée. Il y a aussi celles qui sont liées à la protection de la propriété intellectuelle, celles liées à la lutte contre le cyber-crime, celles liées à la sécurité et à la résilience des réseaux... Tout un ensemble d'impératifs vient ainsi «tempérer», en quelque sorte, le résultat qui peut raisonnablement être obtenu en matière de neutralité des réseaux»*[26].

Un autre exemple du difficile (mais nécessaire) compromis entre les impératifs de sécurité numérique et d'autres exigences est celui de la signature électronique. On connait les avantages indiscutables que la technologie de signature à clé publique procure en ce qui concerne l'authentification des interlocuteurs

[21] *Essentiellement les articles 323-1 à 323-7 (issus de la loi Godfrain du 5 janvier 1988) et l'article 226-15 (issu de la loi du 10 juillet 1991).*
[22] *Convention signée à Budapest le 23 novembre 2001.*
[23] *V. notamment, Eric Caprioli, "Les moyens juridiques de lutte contre la cybercriminalité", Revue Risques n°51, Les cahiers de l'assurance, juillet-sept 2002, p. 50-55 ; également, notre article : B. Warusfel, Procédure pénale et technologies de l'information : de la Convention sur la cybercriminalité à la Loi sur la sécurité quotidienne", Droit & défense, 2002/1, pp. 17-22.*
[24] *Loi DADVSI du 1er août 2006, loi Création et Internet (dite "HADOPI 1") du 12 juin 2009 et "HADOPI 2" du 21 septembre 2009.*
[25] *Débat qui a abouti au rapport du gouvernement au parlement sur le sujet en date du 16 juillet 2010.*
[26] *Au point de préférer utiliser le terme de "quasi-neutralité" (Nicolas Curien, intervention au colloque Neutralité des réseaux, ARCEP, 13 avril 2010, p. 24).*

d'un échange électronique et la garantie de l'intégrité des données échangées. Cela peut tout à la fois renforcer grandement la sécurité technique des communications numériques mais aussi la sécurité juridique des contrats conclus en ligne, ou encore être utilement utilisé pour garantir le respect des droits de propriété intellectuelle en ligne[27]. C'est pourquoi chacun a salué la mise en place en Europe d'une réglementation ambitieuse et précoce en la matière[28] ainsi que sa rapide transposition en droit français (par la loi du 13 mars 2000, les décrets du 30 mars 2001 et 18 avril 2002 et l'arrêté du 31 mai 2002). Mais pourtant, comme cela a été remarqué dès les premières années de mise en application de ces textes, ce dispositif juridique a été très peu mis en œuvre, sans doute en raison du niveau d'exigences imposées par la réglementation concernant la qualification des logiciels nécessaires ainsi que des organismes chargés de délivrer les certificats électroniques[29]. La Commission européenne a été obligée de le reconnaître en 2006 dans son rapport sur la mise en œuvre de la directive de 1999[30]. En l'occurrence, le souci d'assurer une sécurité juridique très poussée s'agissant de la reconnaissance probatoire des documents électroniques signés a eu jusqu'ici pour conséquence paradoxale de dissuader les opérateurs de services numériques de déployer ces systèmes qui pourtant renforceraient considérablement la sécurité technique de leurs réseaux.

**Il existe une telle variété d'intervenants et de services utilisant ces infrastructures numériques et leur interconnexion est devenue à ce point transnationale que leur sécurisation ne peut résulter que d'une combinaison complexe et imparfaite de mesures de natures et de niveaux très différents.**

Ces quelques exemples de la possible contrariété entre certains aspects de la sécurité des réseaux et d'autres objectifs publics de régulation expriment bien, parmi d'autres[31], la complexité intrinsèque de ce domaine. Il existe une telle variété d'intervenants et de services utilisant ces infrastructures numériques et leur interconnexion est devenue à ce point transnationale que leur sécurisation ne peut résulter que d'une combinaison complexe et imparfaite de mesures de natures et de niveaux très différents. Cela impose donc qu'existe en permanence (même de manière informelle) une forme de négociation entre les acteurs techniques, économiques et sociaux concernés et les Etats. Aux réseaux des infrastructures doit correspondre la constitution d'un réseau virtuel des acteurs de leur sécurité. ■

Bertrand Warusfel,
*Professeur à l'Université de Lille 2,*
*Avocat au barreau de Paris (cabinet FWPA)*

[27] *Sur ces différents aspects, v. notamment B. Warusfel, "Aspects juridiques de la dématérialisation des échanges dans le commerce électronique", Les Petites Affiches, janvier 2004, n° 27, p. 17 et suiv.*
[28] *Par la directive n° 1999/93 du 13 décembre 1999 relative au cadre communautaire des signatures électroniques.*
[29] *V. notamment H. Morin "Pourquoi la signature électronique reste lettre morte", Le Monde, 23 Mai 2003.*
[30] *Rapport de la Commission du 15 mars 2006 sur la mise en œuvre de la directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques (qui reconnaît notamment que "Les signatures électroniques qualifiées sont beaucoup moins utilisées qu'on ne l'escomptait, et le marché est actuellement assez étroit").*
[31] *On pourrait aussi s'interroger sur la contradiction qu'il pourrait exister entre les impératifs de concurrence et d'ouverture de l'accès aux réseaux et ceux de leur sécurité.*