LES OBLIGATIONS DES OPERATEURS D'IMPORTANCE VITALE

Par Emmanuel JOUFFIN
Responsable du département veille réglementaire groupe – La Banque Postale, Direction juridique

1. Des menaces protéiformes

La loi de programmation militaire[1] oblige les opérateurs désignés comme d'importance vitale (OIV) à adopter un certain nombre de mesures destinées à protéger leur intégrité et, notamment, celle de leurs systèmes informatiques. Cette préoccupation puise sa source dans divers événements mettant en évidence l'émergence d'une "*cyber war*". Ces actes de guerre peuvent être issus d'un état. Ainsi, en 2010, la NSA et l'armée israélienne ont créé un ver informatique baptisé *Stuxnet* destiné à s'attaquer aux centrifugeuses iraniennes d'enrichissement d'uranium. Les attaques peuvent aussi être le fruit d'organisations terroristes. Le 8 avril 2015, la chaîne TV 5 monde était la cible d'une attaque entrainant l'indisponibilité de nos onze chaînes de télévision, ainsi qu'à une perte de contrôle des réseaux sociaux de TV 5 et de ses sites Internet. Le 15 août 2012, Saudi Aramco est victime d'un malware dont le but est d'extraire des informations vitales. Environ 30.000 postes et 3.000 serveurs sont contaminés. Il faudra plus de trois semaines pour rétablir la sécurité des systèmes d'information. L'attaque fut revendiquée par un groupe Cutting Sword of Justice avec la complicité d'un administrateur système de l'entreprise victime. Ce ne sont que quelques exemples, parmi tant d'autres des menaces face auxquelles la loi de programmation militaire entend faire face

2. Les obligations pesant les sur les OIV

Le statut d'OIV repose sur deux conditions cumulatives. Toute d'abord, l'opérateur exerce son activité en tout ou en partie dans un des 12 secteurs d'activités d'importance vitale[2] et, par ailleurs, il doit gérer ou utiliser au titre de cette activité un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, "*d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation*"[3]. S'agissant de ces points d'importance vitale, des plans particulier de protection (PPP) doivent être mis en œuvre.

La liste, classée "*confidentiel défense*" des OIV identifiée par l'Agence Nationale de la Sécurité des Systèmes d'Information, comporterait 218 entreprises[4]. On devrait y trouver les entreprises du CAC 40, de même que les grands acteurs des transports, des communications, de la santé, de la banque....

Les opérateurs désignés comme d'importance vitale doivent réaliser, à leurs propres frais[5], un plan de sécurité opérateur devant conduire, notamment, à la mise en place de dispositifs en matière de

[1] - Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale. Cf. l'Instruction Générale Interministérielle relative à la sécurité des activités d'importance vitale n°6600/SGDSN/PSE/PSN du 7 janvier 2014.
[2] - Arrêté du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs tel que modifié par un arrêté du 3 juillet 2008.
[3] - Article R1332-1 du Code de la défense.
[4] - Liste établie le 21 janvier 2014. http://www.portail-ie.fr/article/1154/La-protection-des-systemes-d-information-des-OIV
[5] - Article L 1332-1 du Code de la Défense.

sécurité informatique selon des règles fixées par le Premier ministre et portant notamment sur l'installation de dispositifs "*qualifiés*"[6] de détection et de protection contre de futures attaques[7].
Les mesures sécuritaires à adopter par les OIV reposent sur des directives nationales de sécurité (DNS) définissant les objectifs et les politiques de sécurité du secteur ou d'une partie du secteur. A ce titre, sont précisées les mesures planifiées et graduées de vigilance, de prévention, de protection et de réaction contre diverses menaces, notamment d'origine terroriste. Dans le cadre de ces directives, le Premier ministre fixe par arrêtés[8], les méthode d'analyse et de gestion du risque, les procédures à suivre pour déterminer, par secteur d'activités d'importance vitale, les scénarios de menace et leur hiérarchisation selon le type ou le niveau de menace envisagé et, enfin, le plan type des plans de sécurité d'opérateurs d'importance vitale[9], des plans particuliers de protection[10] et des plans de protection externe[11]. Chaque OIV doit se doter d'un délégué pour la défense et la sécurité de l'opérateur (DDSO)[12] représentant l'OIV auprès de l'autorité administrative pour toutes les questions relatives à la sécurité des installations et aux plans de sécurité. Le DDSO est habilité confidentiel défense.

On notera qu'un important décret du 27 mars 2015[13] vient *"mettre en musique"* les dispositions des articles L. 1332-6-1 à L. 1332-6-4 du Code de la défense. L'ANSSI sera notamment chargée de contrôler, à la demande du Premier ministre, le respect des obligations pesant sur les OIV en matière de systèmes d'information. L'objet de ces dispositions n'est pas de protéger les utilisateurs, mais de protéger les entreprises exerçant une activité dans un secteur jugé vital pour la nation. On soulignera spécialement l'obligation faite aux OIV par l'article L. 1332-6-3 du Code de la défense de soumettre « *leurs systèmes d'information à des contrôles destinés à vérifier le niveau de sécurité et le respect des règles de sécurité* ». Au travers de ces contrôles, les opérateurs devront accepter l'implantation, directement dans leur SI, de systèmes de détection, ces « sondes » étant destinées à la recherche et l'analyse des événements susceptibles d'affecter la sécurité des systèmes d'information[14].

Outre l'obligation de déploiement de systèmes agréés, on soulignera l'obligation faite aux OIV d'"*informer sans délai le Premier ministre des incidents affectant le fonctionnement ou la sécurité des systèmes d'information*"[15].

S'agissant des prestataires auxquels les OIV ont recours, l'Instruction Générale Interministérielle relative à la sécurité des activités d'importance vitale énonce "*Dans le cadre de son activité normale,*

---

[6] - Au sens du décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale.
[7] - Article L. 1332-6-1 du Code de la défense.
[8] - Article R. 1332-18 du Code de la défense.
[9] - Les Plans Sécurité Opérateurs (PSO) définissent la politique générale de protection de l'ensemble des activités de l'opérateur, notamment celles organisées en réseau, comportant des mesures permanentes de protection et des mesures temporaires et graduées. Il n'est requis que si l'opérateur gère plusieurs points d'importance vitale.
[10] - Les Plans Particulier de Protection (PPP) sont établis pour chaque point d'importance vitale à partir du PSO vitale, qui lui est annexé. Ces plans comportent les mesures permanentes de protection et des mesures temporaires et graduées.
[11] - Les Plans de protection externe (PPE) sont établis pour chaque point d'importance vitale par le préfet de département en relations avec le délégué de l'opérateur pour la défense et la sécurité de ce point. Ces plans récapitulent les mesures planifiées de vigilance, de prévention, de protection et de réaction prévues par les pouvoirs publics.
[12] - Articles R. 1332-5 et R. 1332-6 du Code de la défense.
[13] - Décret n° 2015-351relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et pris pour l'application de la section 2 du chapitre II du titre III du livre III de la première partie de la partie législative du code de la défense.
[14] - Article R.1332-41-6 al. 1er du Code de la défense : « *Afin de rechercher et d'analyser des événements susceptibles d'affecter la sécurité des systèmes d'information d'importance vitale, l'Agence nationale de la sécurité des systèmes d'information peut demander aux services de l'Etat et aux prestataires de service chargés d'exploiter les systèmes de détection d'utiliser dans ces systèmes des données techniques qu'elle leur fournit* ».
[15] - Article L. 1332-6-2 du Code de la défense.

un OIV peut avoir sous-traité ou externalisé une ou plusieurs fonctions concourant à la réalisation de l'activité d'importance vitale. Dans ce cas, il appartient à l'OIV de prendre les dispositions nécessaires vis-à-vis de son sous-traitant ou de son fournisseur, notamment dans les spécifications du contrat les liant, pour que celui-ci concoure à la réalisation des objectifs de sécurité de l'opérateur"[16]. L'article R. 1332-41-19 du Code de la défense précise que les OIV doivent prendre les mesures nécessaires, notamment par voie contractuelle, pour garantir l'application des règles de sécurité. Cette disposition nécessitera de revoir le contenu des conventions liant les établissements avec leurs PSEE.

3. Les responsabilités encourues par les OIV

Responsabilités pénale et disciplinaires

Les obligations auxquelles sont astreints les OIV au titre de la loi de programmation militaire 2014-2019 sont assorties de sanctions pénales aux termes de l'article L.1332-7 alinéa 3 du Code de la défense. Ce texte prévoit une amende de 150.000 € en cas de manquement par un dirigeant d'un OIV à l'une des dispositions prévues aux articles L. 1332-6-1 à L. 1332-6-4 relatifs aux dispositions spécifiques à la sécurité des systèmes d'information.

Le dernier alinéa de l'article L. 1332-7 précise que les personnes morales peuvent être déclarées responsables ce qui implique, notamment, un quintuplement de l'amende. Cette responsabilité pénale des personnes morales, au sens de l'article L. 121-2 du Code pénal, a été introduite par l'article 22 de la loi de programmation militaire 2014-2019.

Outres les conséquences en termes de responsabilité pénale, on peut également redouter une responsabilité disciplinaire et civile. Au titre de la responsabilité disciplinaire, l'ACPR[17] est en effet chargée par la loi[18] de "*veiller […] à la protection des clients […] des personnes soumises à son contrôle*" ainsi qu'au respect par ces personnes "*des règles destinées à assurer la protection de leur clientèle*", ce qui comprend sans nulle doute la protection des données à caractère personnelle de ces clients, il en va de même pour l'AMF[19].

Responsabilité civile

Outre, les sanctions ci-dessus rappelées, un jugement du TGI Paris du 21 février 2013[20] suscite l'attention. La société *Sarenza*, victime du piratage de son fichier clients contenant 4.7 millions d'adresses mails a été considérée comme responsable, à hauteur de 30 % en raison du manque de rigueur dans la gestion des identifiants d'accès à sa base de données.

Une telle carence pourrait bien donner lieu à une action de groupe. En effet, l'article L. 423-1 du Code de la consommation, l'action de groupe a pour objet de permettre "*la réparation des préjudices individuels subis par des consommateurs placés dans une situation similaire ou identique, et ayant pour cause commune un manquement d'un ou des mêmes professionnels à leurs obligations légales ou contractuelles à l'occasion de la vente de biens ou de la fourniture de service".*

Le manquement à une obligation légale est ici constitué par le fait que le responsable de traitement était censé "*mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les*

---

[16] - Cf. Instruction Générale Interministérielle relative à la sécurité des activités d'importance vitale n°6600/SGDSN/PSE/PSN du 7 janvier 2014, spéc. p. 16.

[17] - Laquelle peut infliger une sanction pécuniaire de 100 millions d'euros - article 612-39 du Code monétaire et financier.

[18] - Art. L. 612-1, CMF.

[19] - Art. L. 621-I, CMF. L'AMF peut également infliger une sanction pécuniaire de 100 millions d'euros (art. L. 621-15-III a du CMF).

[20] - Sarenza c/ Jonathan et autres.

données contre (...) la diffusion et l'accès non autorisé" conformément à l'article 34 de la loi du 6 janvier 1978. On notera en outre que la CNIL, dans sa délibération n° 2008-155[21] a mis en demeure une société de restreindre aux seules personnes habilitées l'accès aux données.

Ces divers textes constituent à n'en pas douter une incitation particulièrement forte des OIV, indépendamment de leur secteur d'activité, à appliquer de manière scrupuleuse les normes relatives à ce sujet dont notamment à la norme internationale ISO 22301 relatives aux systèmes de management de la continuité d'activité (SMCA) publiée en juin 2012[22]. Les dispositions de la loi de programmation militaire, et son cortège de dispositions relatives à la sécurité des systèmes d'information ne font que renforcer la potentialité d'un risque liée à une action, au plan civile, portée par les clients. Il nous faut maintenant nous préparer à la suite. En effet, le dispositif issu de la loi de programmation militaire s'inscrit dans un cadre européen déterminée par la directive 2008/114/CE prévoit un mécanisme d'identification et de désignation des infrastructures critiques européennes (ICE) "*dont l'arrêt ou la destruction aurait un impact considérable sur deux Etats membres au moins*".

[21] - CNIL, délib. n° 2008-155, 29 mai 2008 mettant en demeure la société Jean-Marc Philippe, notifiée le 1er août 2008 : www.cnil.fr

[22] - Elle constitue une sorte de norme pilote dans laquelle s'insèrent diverses normes dont notamment : ISO 22300 qui spécifie le vocabulaire de la continuité d'activité, ISO 22313 relatif au guide de mise en œuvre d'un SMCA, ISO 27031, linges directrices de mise en œuvre de la préparation des technologies de l'information et de communication à la continuité d'activité, ISO 31000, lignes directrices pour le management des risques.