Mars 2017

Domaine d'intervention :

Droit des Nouvelles Technologies et Propriété Intellectuelle

Sécurité des systèmes d'information d'importance vitale : précisions relatives aux obligations règlementaires de sécurité des opérateurs

Par Claude-Etienne Armingaud, Alexandre Balducci

Quatre nouveaux arrêtés sectoriels relatifs à la sécurité des systèmes d'information des opérateurs d'importance vitale ont été publiés au Journal Officiel du 4 décembre 2016. Ces arrêtés viennent préciser la partie règlementaire du Code de la défense relative aux règles de sécurité et aux modalités de déclaration des systèmes d'information d'importance vitale dits « SIIV ».

La sécurité des systèmes d'information, élément du dispositif de sécurité des activités d'importance vitale

A la suite des attaques terroristes de New York City le 11 septembre 2001 puis des attentats de Madrid en 2004 et de Londres en 2005, la France a initié une réflexion sur ses infrastructures les plus critiques dans le but de renforcer la protection accordée à ces infrastructures.

Un dispositif interministériel de sécurité des activités d'importance vitale dit « SAIV » a ainsi été inscrit dans le Code de la défense en 2005[1]. Les activités d'importance vitale, définies par un décret du 23 février 2006[2], désignent en pratique les activités indispensables au maintien de l'autorité de l'État, de la sécurité de la Nation et plus généralement du fonctionnement normal de la vie de la Nation (télécommunications, information, finance, industrie…).

Piloté par le Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN), le dispositif de vise à protéger les opérateurs d'importance vitale dits « OIV »[3] mentionnés à l'article L.1332-1 du Code de la défense contre les actes de malveillance (terrorisme, etc.) et les risques technologiques, naturels et sanitaires pouvant les impacter.

Aux fins de contrer la menace toujours grandissante des attaques informatiques, la loi de programmation militaire du 18 décembre 2013 est venue imposer aux OIV des mesures relatives à la sécurité de leurs systèmes d'information[4]. Leurs systèmes d'information les plus critiques, dits systèmes d'information d'importance vitale ou « SIIV », sont désignés par les OIV eux-mêmes selon une procédure définie aux articles R.1332-42-1 et suivants du Code de la défense et sont désormais soumis à des obligations de contrôle et surveillance renforcées. Ces obligations de sécurité sont établies par arrêté du Premier

---

[1] Loi n° 2005-1550 du 12 décembre 2005 modifiant diverses dispositions relatives à la défense créant les articles L1332-1 et suivants du Code de la défense

[2] Décret n°2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale

[3] Article L.1332-1 du Code « *Les opérateurs publics ou privés exploitant des établissements ou utilisant des 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, sont tenus de coopérer à leurs frais dans les conditions définies au présent chapitre, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste. Ces établissements, installations ou ouvrages sont désignés par l'autorité administrative* ».

[4] Articles L.1332-6-1 et suivants du Code de la défense

Sécurité des systèmes d'information d'importance vitale : précisions relatives aux obligations règlementaires de sécurité des opérateurs

Ministre sur proposition de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI).

Précisions sur le périmètre des nouveaux arrêtés sectoriels

Les quatre arrêtés sectoriels publiés le 4 décembre 2016 ont un champ d'application particulièrement étendu, puisqu'ils concernent les secteurs et sous-secteurs d'activité d'importance vitale « Industrie », « Finances », « Communications Électroniques et Internet » et « Audiovisuel et Information ».

Ils viennent préciser, pour les OIV opérant sur les secteurs visés (i) la procédure permettant aux OIV d'identifier leurs SIIV auprès des services du SGDSN et de notifier certains incidents de sécurité affectant ces SIIV et (ii) les règles impératives de sécurité organisationnelle et technique qui s'imposent à ces SIIV, en supplément des mesures de sécurité qui s'imposent déjà à tous les systèmes d'information des OIV.

Plus particulièrement, les arrêtés précisent que les OIV sont tenus de mettre en place en leur sein une politique de sécurité des systèmes d'information dite « PSSI » qui décrit la politique de gouvernance de ces OIV en matière de sécurité. Les arrêtés précisent que le PSSI concerne l'ensemble des moyens tant organisationnels que techniques mis en œuvre par l'OIV aux fins d'assurer la sécurité des SIIV, notamment les mesures de contrôle et d'habilitation du personnel, les procédures d'audit, de traitement des incidents de sécurité, de gestion de crise et de continuité d'activité.

Il convient donc pour les opérateurs désignés OIV d'établir et de mettre en œuvre au plus vite une politique de gouvernance forte en matière de sécurité de leurs systèmes d'information.

Rappelons que les OIV sont tenus par le Code de la défense de déferrer sur leurs frais propres aux obligations qui leurs sont imposées par le Code de la défense, en ce compris les nouvelles exigences d'identification et de sécurité instaurées par les arrêtés publiés le 4 décembre 2016.

Les dispositions pénales de l'article L.1332-7 du Code de la défense, qui s'appliquent en cas de non-respect des obligations imposées par ce Code aux OIV, sont à tout le moins dissuasives ; les dirigeants des organismes désignés OIV qui ne respecteraient pas leurs obligations de sécurité de leurs systèmes d'information encourent des peines d'amende de 150.000 euros et les personnes morales déclarées responsables des mêmes infractions au Code de la défense encourent une amende de 750.000 euros.

Prochaines étapes

Les quatre arrêtés sectoriels relatifs à la sécurité des systèmes d'information d'importance vitale sont entrés en vigueur au 1er janvier 2017. Ils ont vocation à s'appliquer à tous les OIV déjà désignés à compter de cette date, ainsi qu'à tous les organismes dont la désignation interviendrait postérieurement, dès cette désignation.

Les prochaines semaines représentent par conséquent une fenêtre d'action limitée pour les acteurs dont la qualité d'OIV a déjà été établie ; ces derniers devront se focaliser sur un effort rapide de détection de leurs SIIV, de mise en œuvre des mesures de sécurité destinés à protéger ces SIIV ainsi que des procédures internes de détection et de notification des incidents affectants ces SIIV.

Les équipes parisiennes de K&L Gates disposent d'une expérience en matière de sécurité des systèmes d'information et de protection des données à caractère personnel.

Sécurité des systèmes d'information d'importance vitale : précisions relatives aux obligations règlementaires de sécurité des opérateurs

Nous pourrons ainsi vous accompagner dans l'identification de vos SIIV ainsi que dans la mise en place de procédures de sécurité conformes aux nouvelles exigences règlementaires posées par le Code de la défense.

Auteurs:

Claude-Etienne Armingaud
claude.armingaud@klgates.com
+33.1.58.44.15.16

Alexandre Balducci
alexandre.balducci@klgates.com
+33.1.58.44.15.20