Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
INHESJ
INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

INSTITUT NATIONAL DES HAUTES ÉTUDES
DE LA SÉCURITÉ ET DE LA JUSTICE

en partenariat avec le cigref Réseau de Grandes Entreprises

Collection Sécurité économique

SEPTEMBRE 2014

Ingérence et politique de sécurité des systèmes d'information

Travaux de la 4e promotion (2013-2014)

du Cycle
« Sécurité des usages numériques »

L'Institut national des hautes études de la sécurité et de la justice publie chaque année des rapports et études sur les champs de la sécurité et à la justice.

Dans le cadre du cycle de spécialisation « *Sécurité des usages numériques* », les auditeurs stagiaires réalisent un travail collectif tutoré par le département sécurité économique de l'INHESJ. Ces travaux sont effectués en toute liberté grâce à l'indépendance dont les auteurs bénéficient au sein de l'Institut.

L'étude ci-dessous publiée est un document à vocation scientifique. Il ne saurait être interprété comme une position officielle ou officieuse de l'Institut ou des services de l'État. Les opinions et recommandations qui y sont exprimées sont celles de leurs auteurs. Le document est publié sous la responsabilité éditoriale du directeur de l'Institut.

Les études ou recherches de l'INHESJ sont accessibles sur le site de l'INHESJ.

Directeur de la publication M. Cyrille SCHOTT, directeur de l'INHESJ

AVANT-PROPOS

L'information est désormais au cœur des actifs immatériels des organisations et constitue un élément clé de leur performance. L'entrée dans le monde numérique a par ailleurs conféré aux systèmes d'information une dimension incontournable dans le développement de l'économie. La « sécurité des usages numériques » représente donc un enjeu majeur pour la pérennité et la compétitivité des entreprises et des administrations. C'est pourquoi, dès 2010, l'Institut national de hautes études de la sécurité et de la justice (INHESJ) et le CIGREF (Réseau de Grandes Entreprises) ont convenu de mettre en place, à destination des cadres d'entreprises des secteurs privé et public, un cycle de formation sur les problématiques et les enjeux liés à la sécurité numérique.

Ce cycle de spécialisation en « Sécurité des usages numériques » concerne tous ceux qui veulent mieux comprendre les enjeux de la sécurité numérique au sein des entreprises. Il a pour objectif de délivrer les savoir-faire visant l'identification, l'évaluation et la maîtrise de l'ensemble des risques et des malveillances.

L'Institut est heureux de présenter dans sa collection *Études et Documents* les travaux des auditeurs de ce cycle, réalisés sous la supervision du département Sécurité économique de l'INHESJ. ■

Cyrille SCHOTT

Directeur de l'Institut national des hautes études de la sécurité et de la justice

Pascal BUFFARD

Président du CIGREF

Remerciements

Le groupe de travail tient à remercier les membres de l'**INHESJ** sans lesquels ce cycle de spécialisation ne saurait être :

- **Nicolas Arpagian** pour l'identification des thèmes à chaque session et le choix des intervenants, la pertinence des sujets abordés,
- **Dominique Henrion**, pour son sens de l'organisation,
- **Elsa Gaussin** et **Anouk Médan** pour leur accueil et leur écoute.

Nous remercions les intervenants au sein de ce cycle pour avoir pris le temps de venir nous exposer leurs points de vue, de partager des moments d'échange particulièrement enrichissants.

Enfin, nous remercions le CIGREF pour sa contribution à l'organisation de ce cycle de spécialisation.

Les **AUTEURS**

Les auteurs de ce travail intitulé : « **Effets de l'ingérence des législations étrangères sur les politiques de sécurité des SI des entreprises**. Quelles sont les options d'une entreprise pour mettre en place une politique de sécurité au niveau international ? » sont :

Katarzyna Bouquet-Lenczner

Emmanuelle Fouques

Frédéric Guillermin

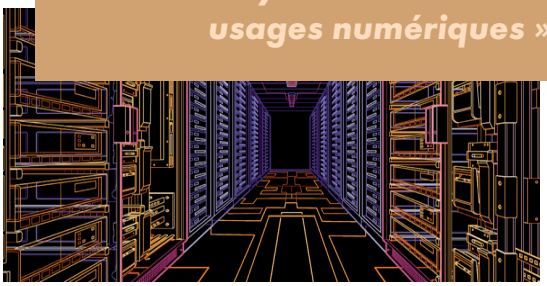
Pierre Guislin

Arnaud Mansey

Sous la direction de **Nicolas Arpagian**, *directeur scientifique du cycle « Sécurité des usages numériques »*.

INGÉRENCE ET POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

Travaux de la 4e promotion (2013-2014) du Cycle « Sécurité des usages numériques »



Sommaire

PRÉAMBULE **7**

INGÉRENCE ET POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

INTRODUCTION 8

- Politique de Sécurité des Systèmes d'Information 8
- Système de Management de la Sécurité de l'Information (SMSI) 9
- Cadre législatif français 10
- Distinction entre les notions de sécurité et de sûreté 11
- L'ingérence 12

PARTIE 1 – L'INGÉRENCE DES LÉGISLATIONS ÉTRANGÈRES SUR LA POLITIQUE DE SÉCURITÉ

- L'existence et les impacts de l'ingérence des législations étrangères sur la politique de sécurité 13
- Les contre-mesures législatives, organisationnelles et techniques existantes et l'ingérence des législations étrangères dans la politique de sécurité 18

PARTIE 2 – OPTIONS D'UNE ENTREPRISE RETENUES PAR LES AUTEURS POUR METTRE EN PLACE UNE POLITIQUE DE SÉCURITÉ AU NIVEAU INTERNATIONAL

- Politique de sécurité et organisation au sein d'une entreprise 25
- Cas d'usage et solutions techniques 29

CONCLUSION **35**

PRÉAMBULE

Miser sur la diversité des compétences pour répondre à des menaces protéiformes.

La sécurité numérique doit se concevoir sur le modèle des multiples formes d'agressions rendues possibles par les technologies de l'information et de la communication qui irriguent désormais les organisations économiques, administratives ou militaires. C'est la raison pour laquelle la réflexion et la stratégie en matière de cybersécurité doivent se concevoir en mettant à contribution une grande variété de compétences et d'expertises : dans les domaines industriels, techniques, informatiques, juridiques, judiciaires, militaires, policiers et même politiques.

De ce croisement de savoir-faire émergeront les stratégies utiles à mettre en place pour concevoir une sécurité numérique plus performante. C'est dans cet esprit que chaque année les auditeurs du cycle « Sécurité Numérique » de l'Institut National des Hautes Études de la Sécurité et de la Justice (INHESJ) travaillent à analyser et éclairer une problématique qui se trouve au cœur des intérêts stratégiques des entreprises, et donc des États. Ils ont pour mission d'expliquer les enjeux de la thématique qui leur a été confiée, d'en présenter les mécanismes et de formuler des réponses réalistes et concrètes pour réduire ou faire cesser l'exposition au risque qu'elle représente. Soit une démarche résolument tournée vers une amélioration continue de la notion de sécurité, au bénéfice du plus grand nombre.

Vous trouverez dans ce document le fruit de leurs réflexions après une année d'étude passée au sein de l'INHESJ à échanger entre pairs et à rencontrer les experts et les praticiens les plus expérimentés dans le domaine de la sécurité numérique. Ils aboutissent à chaque fois à des recommandations opérationnelles directement transposables dans la réalité des entreprises et des administrations.

Ce sont donc des contributions utiles à une meilleure sécurité numérique.

Éric DELBECQUE

Chef du Département
« Sécurité économique »

Nicolas ARPAGIAN

Directeur scientifique du cycle
« Sécurité des usages numériques »

INTRODUCTION

Afin de traiter de la problématique liée aux effets de l'ingérence des législations étrangères sur les politiques de sécurité des entreprises, et pour proposer à une entreprise des options pour mettre en place une politique de sécurité au niveau international, il est indispensable de constituer un socle commun de références concernant les éléments de vocabulaire utilisés dans le présent document.

Dans un contexte interne, la notion de Politique de sécurité des systèmes d'information (PSSI) et de Système de management de la sécurité de l'information (SMSI) est claire.

En revanche, dans un contexte international, il conviendra d'étudier les différentes approches et définitions apportées par des organismes reconnus en la matière. Le panorama brossé n'est pas exhaustif, il s'agit plutôt d'établir la définition la plus adéquate à la suite du développement de ce rapport.

Politique de Sécurité des Systèmes d'Information

Afin de mieux cerner la notion de Politique de sécurité des systèmes d'information dans le contexte français, nous prendrons en compte comme définition celle donnée par l'ANSSI [1] qui définit la Politique de sécurité des systèmes d'information, (PSSI), comme un ensemble formalisé dans un document applicable des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du (des) système(s) d'information de l'organisme[2].

La PSSI constitue ainsi le socle de la sécurité des systèmes d'informations (SSI). C'est le référentiel qui « fait foi », théoriquement à tout moment, au sein du périmètre dans lequel il s'applique. Toute réflexion relative à la SSI dans le cadre de ce périmètre devra être conforme à cette politique.

Les normes ISO 27001 et 27002 donnent une définition de ce qui est attendu dans un document de politique de sécurité de l'information :

- Une définition de la sécurité de l'information, les objectifs généraux recherchés, le domaine d'application retenu, ainsi que l'importance de la sécurité en tant que mécanisme nécessaire au partage de l'information.
- Une déclaration des intentions de la Direction soutenant les objectifs et les principes de sécurité de l'information, en conformité avec la stratégie et les objectifs de l'organisme.
- Une démarche de définition des objectifs de sécurité et des mesures intégrant l'appréciation et le management du risque.

(1) Agence Nationale de la Sécurité des Systèmes d'Information. L'ANSSI a été créée par le décret n°2009-834 du 7 juillet 2009, sous la forme d'un service à compétence nationale. Elle est rattachée au Secrétaire général de la défense et de la sécurité nationale (SGDSN), autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. La création de l'ANSSI est l'une des suites données à la publication, le 17 juin 2008, du Livre blanc sur la défense et la sécurité nationale.

(2) Organisme est le terme générique permettant d'adresser l'ensemble des structures hébergeant un système d'information au profit d'une activité humaine tel que : une entreprises publique ou privée, un service public, une institution internationale, une administration centrale et territoriale (régions et villes), un centre d'études et de recherches, une université, une école, une chambre de commerce et d'industrie...

- Une explication des politiques, principes, normes et exigences en matière de conformité, qui présentent une importance particulière pour l'organisme.
- Une définition des responsabilités générales et spécifiques dans le domaine de la gestion de la sécurité de l'information, traitant en particulier de la remontée des incidents de sécurité.

Le groupe de travail considèrera dans la suite du développement que l'approche de la PSSI développée dans les normes ISO 27xxx constitue une référence internationale. Il est à noter que peu d'écrits sont suffisamment synthétiques par ailleurs pour prétendre constituer une définition.

Les auteurs reprendront plus en détail les éléments constitutifs d'un système de management de la sécurité de l'information (SMSI), et d'une PSSI dans la première partie du document et s'attacheront à décrire en quoi la mise en œuvre d'une gouvernance orientée Sécurité de l'information constitue un éventail de mesures pour contrer l'ingérence, problématique traitée dans ce document.

Système de Management de la Sécurité de l'Information (SMSI)

Selon le CLUSIF[3], la notion de SMSI fait référence à un ensemble d'éléments interactifs permettant à un organisme d'établir une politique et des objectifs en matière de sécurité de l'information, d'appliquer la politique, d'atteindre ces objectifs et de contrôler l'atteinte des objectifs.

Il s'agit de désigner une approche systémique par laquelle une organisation veille à la sécurité des informations sensibles. Construit selon un processus de management du risque, un SMSI englobe les personnes, les processus et les systèmes de traitement de l'information.

Au niveau international, plusieurs normes et standards ont été développés afin de s'assurer que les informations sensibles ou non, stockées et manipulées sur des ordinateurs très souvent connectés le soient de manière sécurisée.

Parmi celles-ci, la norme ISO 27001[4] publiée en 2005 et révisée en 2013 succède à la BS 7799[5] elle-même datant dans sa première version de 1995. Elle décrit les étapes de la mise en œuvre d'un SMSI et propose des exigences sur les mesures de sécurité propres à chaque organisme afin qu'elles soient adéquates et proportionnées aux risques adressés.

D'autres organismes ont vocation à développer des bonnes pratiques et aider la démarche de sécurité des entreprises. L'ISF (*Information Security Forum*), créé en 1989 a pour vocation d'enquêter, clarifier et résoudre des questions importantes dans le domaine de la sécurité de l'information et de la gestion des risques en développant notamment le *Standard of good Practice*.

(3) Club de la Sécurité de l'Information Français. Le CLUSIF est un club professionnel, constitué en association indépendante, ouvert à toute entreprise ou collectivité. Il accueille des utilisateurs et des offreurs issus de tous les secteurs d'activité de l'économie.
La finalité du CLUSIF est d'agir pour la sécurité de l'information, facteur de pérennité des entreprises et des collectivités publiques.
Il entend ainsi sensibiliser tous les acteurs en intégrant une dimension transversale dans ses groupes de réflexion : management des risques, droit, intelligence économique...

(4) La famille de normes ISO 27000 aide les organisations à assurer la sécurité de leurs informations. ISO 27001, qui expose les exigences relatives aux systèmes de management de la sécurité des informations (SMSI), est la norme la plus célèbre de cette famille.

(5) BS7799 : *British Standard*.

Publié depuis 1990 et revu régulièrement – la dernière version date de 2013 - le *Standard of Good Practice* donne un ensemble très complet des bonnes pratiques en matière de sécurité de l'information.

Il indique notamment qu'une politique de sécurité doit être documentée, approuvée par les décideurs et qu'elle s'applique à l'ensemble de l'organisation. Il est également évoqué le fait que la politique doit être régulièrement mise à jour.

Le NIST (*National Institute of Standards and Technologie*)[6] qui a pris la succession en 1988 du *National Bureau of Standards* a pour but de promouvoir l'économie par le développement de technologies et de standards en lien avec l'industrie. Il publie de nombreux guides. Parmi ceux-ci le NIST SP800-100 *Information Security Handbook: A guide for manager*. Ce guide évoque la politique de sécurité.

Les approches et définitions décrites par les différents organismes reconnus énoncés précédemment ne font apparaître aucune lacune ou disparité qui pourrait être de nature à complexifier la mise en œuvre d'un SMSI dans une entreprise d'envergure internationale.

Ainsi, à l'issue de ces différents énoncés sur les référentiels en vigueur, le groupe de travail considérera dans la suite du développement que la norme ISO 27001 est la plus à même d'être une référence internationale et la retiendra comme référentiel pour la définition et la mise en œuvre d'un SMSI.

La mise en œuvre d'un SMSI est un processus dont le moteur principal est la politique de sécurité de l'entreprise.

Cadre législatif français

Le droit français sanctionne pénalement des atteintes de toute nature aux Systèmes automatisés de traitement des données (STAD). Le code pénal français prévoit plusieurs peines principales[7].

Ainsi sont sanctionnées par des peines d'emprisonnement allant de 2 à 5 ans et des peines d'amende qui s'échelonnent de 30 000 à 75 000 euros à l'encontre de personnes physiques et/ou morales pour les infractions d'accès ou de maintien frauduleux dans un STAD, pour la suppression, modification de données, altération du fonctionnement d'un STAD. Il est à noter que pour les personnes morales les peines d'amende sont multipliées par cinq.

Il en est de même pour les entraves, ou toute opération qui fausserait le fonctionnement du système.

Le même type de sanctions est prévu en cas de mise à disposition d'un outil permettant l'atteinte aux STAD, comme cela avait été jugé par la Cour d'appel de Paris dans l'affaire Nintendo.

(6) Le *National Institute of Standards and Technologie* est une agence du Département du Commerce des États-Unis. Son but est de promouvoir l'économie en développant des technologies, de la métrologie et des standards en partenariat avec l'industrie.

(7) ***Article 323***: Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à cinq ans d'emprisonnement et à 75 000 euros d'amende.

Article 323-2: Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à sept ans d'emprisonnement et à 100 000 euros d'amende.

Article 323-3: Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de 5 ans d'emprisonnement et de 75 000 euros d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à sept ans d'emprisonnement et à 100 000 euros d'amende.

Article 323-3-1: Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-4: La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

De plus les dispositions de l'article 121-3 alinéa 3 du Code pénal énoncent le principe d'infraction indirecte [8], c'est-à-dire un comportement qui faciliterait la commission d'un crime ou d'un délit lorsque l'on dispose de moyens de l'empêcher du fait de connaissances ou de moyens dont on dispose tombera sous le coup de mêmes sanctions.

Il est important de préciser que les sanctions peuvent impacter solidairement des personnes physiques et morales [9].

Les tribunaux peuvent également prononcer des sanctions complémentaires telles que l'interdiction de droits civiques et familiaux, l'interdiction d'exercer une activité professionnelle concernée, confiscation de la chose qui a servi à commettre l'infraction, fermeture des établissements ayant servi à commettre l'infraction, exclusion des marchés publics, interdiction d'émettre des chèques, affichage ou diffusion de la décision prononcée [10].

Les atteintes aux STAD s'appréhendent classiquement selon les axes suivants :

- **Disponibilité** : propriété d'un STAD à être accessible et utilisable selon la demande d'une entité autorisée *(source ISO 27001)*.
- **Intégrité** : propriété d'un STAD à protéger l'exactitude et l'exhaustivité des actifs qu'il contient *(source ISO 27001)*.
- **Confidentialité** : propriété d'un STAD à ne rendre accessible une information qu'aux personnes, entités ou processus autorisés *(source ISO 27001)*.
- P**reuve ou Traçabilité ou Auditabilité** : propriété d'un STAD à justifier de la délivrance des informations ; cette caractéristique n'est pas portée par la norme ISO 27001.

Distinction entre les notions de sécurité et de sûreté

Afin d'éviter toute confusion dans la suite du développement, les auteurs ont souhaité préciser ici la différence entre les missions de sécurité et de sûreté.

La politique de sûreté fixe les principes afférents à la protection des personnels, des installations, du patrimoine informationnel et de l'image de l'entreprise.

La mission de la sûreté s'inscrit dans le respect des droits de l'homme, en particulier des recommandations des Principes volontaires sur la sécurité et les droits de l'Homme (VPSHR).

Une PSSI est donc dédié aux systèmes d'information et représente donc une composante de la politique de sûreté d'une entreprise.

La politique de sûreté est plus à même d'adresser les problématiques liées à la mise en œuvre des règles et dispositifs visant à garantir l'intégrité physique et logique de l'image et de toutes les ressources de l'organisation y compris ses collaborateurs. Dès lors on peut se positionner en exemple sur la donnée de

(8) ***Article 121-3*** du Code Pénal. Il n'y a point de crime ou de délit sans intention de le commettre.

Toutefois, lorsque la loi le prévoit, il y a délit en cas de mise en danger délibérée de la personne d'autrui.

Il y a également délit, lorsque la loi le prévoit, en cas de faute d'imprudence, de négligence ou de manquement à une obligation de prudence ou de sécurité prévue par la loi ou le règlement, s'il est établi que l'auteur des faits n'a pas accompli les diligences normales compte tenu, le cas échéant, de la nature de ses missions ou de ses fonctions, de ses compétences ainsi que du pouvoir et des moyens dont il disposait.

Dans le cas prévu par l'alinéa qui précède, les personnes physiques qui n'ont pas causé directement le dommage, mais qui ont créé ou contribué à créer la situation qui a permis la réalisation du dommage ou qui n'ont pas pris les mesures permettant de l'éviter, sont responsables pénalement s'il est établi qu'elles ont, soit violé de façon manifestement délibérée une obligation particulière de prudence ou de sécurité prévue par la loi ou le règlement, soit commis une faute caractérisée et qui exposait autrui à un risque d'une particulière gravité qu'elles ne pouvaient ignorer. Il n'y a point de contravention en cas de force majeure.

(9) Cour d'appel de Paris Pole 5, Ch.12, 26 septembre 2011- arrêt dit « Nintendo ».

(10) ***Article 323-5*** : Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;

2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;

3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;

4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;

6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;

7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35.

Article 323-6 : Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

Article 323-7 : La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.

l'organisation, patrimoine immatériel par excellence dont l'intégrité en tant que donnée est garantie par la PSSI mais dont l'intégrité logique (*i.e.* des disques, serveurs, stations, datacenters, bâtiments qui l'hébergent) est couverte par la politique de sûreté de l'entreprise.

L'ingérence

La notion juridique de l'ingérence signifie une intervention non désirée et illicite d'un État dans les affaires d'un autre sans son consentement et au détriment du concept de souveraineté.

L'ingérence peut s'effectuer au niveau individuel, organisationnel ou international. L'ingérence prend diverses formes : politique, juridique, économique, sociale, culturelle, religieuse, humanitaire.

L'ingérence peut aussi être implicite lorsque la souveraineté de l'autre est remise en cause de manière camouflée ou par le biais d'intermédiaires.

Seul le concept d'ingérence humanitaire est considéré comme légitime par le droit international général, toutefois cet aspect ne fera pas partie de notre analyse.

En revanche, les auteurs du présent développement seront amenés à aborder dans la première partie de cette analyse les problématiques liées aux effets de l'ingérence des législations étrangères sur la politique de sécurité (*première partie*), puis nous verrons de quelles options dispose une entreprise pour mettre en place une politique de sécurité adaptée à un contexte international (*deuxième partie*).

L'INGÉRENCE DES LÉGISLATIONS ÉTRANGÈRES SUR LA POLITIQUE DE SÉCURITÉ

Partie 1

L'analyse de la problématique de l'ingérence des législations étrangères sur la politique de sécurité implique en premier lieu l'examen de l'existence et des impacts de l'ingérence, puis nous proposerons des contres mesures pour y pallier.

L'existence et les impacts de l'ingérence des législations étrangères sur la politique de sécurité

De prime abord, du point de vue juridique, la rédaction de l'énoncé peut s'avérer choquante.

Depuis les temps bibliques, pris au sens littéral, une législation n'est censée produire d'effets qu'au sein des États qui les ont édictés, sauf accord contraire passé entre nations intéressées.

Le concept de souveraineté nationale est issu de la Bible, qui est le premier ouvrage dogmatique qui envisage la Société Internationale sous l'angle de l'unité du genre humain, mais s'exprimant par la pluralité de nations, toutes égales entre elles.

Ces nations reconnaissent toutes des règles morales et juridiques d'essence supérieure applicables à l'humanité et auxquelles elles ne sauraient déroger.

Il s'agit là, d'un droit naturel, d'un droit supérieur, commun et s'imposant à tous.

Ces concepts bibliques sont à tel point ancrés dans la « conscience transnationale », qu'ils ont été repris par le Préambule et au Chapitre 1 de la Charte de l'ONU et officialisés par la notion de *jus cogens* [11], dans le texte de la Convention de Vienne de 1969 sur le droit des traités.

Les auteurs du présent développement écarteront sciemment toute description de l'évolution historique du droit international dit public [12], toutefois si nous sommes remontés au temps jadis, c'est pour mieux expliquer les concepts actuels, applicables au principe de la territorialité de la règle de droit.

En effet, il convient d'expliquer deux notions clés du présent développement, à savoir, celles de l'ordre interne et de l'ordre international tout deux spécifiques et distincts entre eux.

(11) Le *Jus cogens* est une norme du droit international général, reconnue par la communauté internationale dans son ensemble en tant que la norme à laquelle aucune dérogation n'est permise et qui ne peut être modifiée que par une nouvelle norme du droit international général ayant le même caractère, art. 53 de la Convention de Vienne sur le droit des traités, du 23 mai 1969.

(12) Un ensemble de règles juridiques régissant les relations entre les États et les autres sujets de la société internationale.

L'ordre juridique interne constitue un système juridique parfait et complet.

La plénitude de l'ordre juridique interne se traduit par la capacité d'édiction et d'exécution de la règle de droit par un État, c'est d'ailleurs un des éléments constitutifs de la notion de souveraineté nationale [13].

La notion de capacité d'édiction se traduit par l'existence de ce que l'on pourrait appeler un « législateur » local, qui dispose du monopole de l'édiction des règles juridiques à portée générale et obligatoire.

Autrement dit, afin d'obtenir une législation uniforme, le processus d'édiction de normes juridiques obligatoires est centralisé.

La notion de la capacité d'exécution se traduit quant à elle, par l'existence d'une « administration » locale dont le rôle est d'assurer l'exécution de normes obligatoires édictées par le législateur. L'État peut à l'égard de ses propres citoyens recourir à la contrainte physique, dont il a également le monopole, pour contraindre ses sujets récalcitrants à respecter la règle de droit.

Bien qu'à des degrés divers tout État contemporain est doté d'un système juridique à compétence obligatoire pour régler définitivement les litiges concernant l'interprétation ou l'exécution de normes locales, une personne privée pourra recourir à la force publique de l'État pour assurer le respect de ses droits à l'encontre d'une autre personne privée qui les violerait.

Il apparaît donc clairement que du point de vue théorique l'ordre juridique interne est non seulement « complet » mais également « parfait », dans la mesure où toute idée de « lacune de droit » est exclue [14].

La situation est diamétralement opposée lorsqu'il est question de l'ordre international.

Comme nous l'avions expliqué en amont de cette analyse, les États sont considérés au regard du droit international dit public, comme des personnes morales [15], toutes égales entre elles.

L'expression de « *législation internationale* », lorsqu'il est question des décisions, avis, recommandations ou résolutions, rendues par les organisations internationales, est trompeuse et inexacte.

En effet, le droit international est un système décentralisé au sein duquel les auteurs des normes sont le plus souvent les seuls destinataires de celles-ci, bien souvent les règles de droit qui régissent le droit international général sont non écrites, basées sur la coutume [16] et leur valeur contraignante dépend de la bonne volonté des États auxquels ladite norme s'applique.

Il en ressort que, sur le plan de l'exécution de normes, le droit international est imparfait, car il n'existe aucun système juridictionnel à compétence générale et obligatoire, pour contraindre à l'exécution de la règle de droit.

Le recours à un juge ou à un arbitre est purement volontaire en raison de l'égalité existante entre les États.

D'ailleurs c'est pour les mêmes raisons que le droit international ignore les sanctions, telles qu'elles sont prévues par le droit interne.

Comme les auteurs du présent développement ont eu l'occasion de le démontrer plus en amont, en raison de l'égalité entre les personnes morales que sont les États, la capacité d'édiction et d'exécution des règles du droit dont ils

(13) Souveraineté dont le titulaire est la nation, une entité collective indivisible et distincte des individus qui la composent.

(14) L'article 4 du Code civil sanctionne le déni de justice, sous prétexte d'obscurité ou d'insuffisance de la règle de droit.

(15) Groupement doté de la personnalité juridique, donc titulaire lui-même de droits et d'obligations abstraction faite de la personne de membres qui le composent : société, syndicat, États, collectivités territoriales, organisations internationales, etc.

(16) Coutume internationale, est une « *pratique juridique acceptée comme étant le droit* », art. 38-§2 du Statut de la Cour Pénale Internationale de justice ; ce qui implique un élément matériel, c'est-à-dire une répétition de précédents constituant un usage continu et général, et un élément psychologique, l'*opinio juris*, à savoir, la conviction des États qu'en suivant cet usage ils obéissent à la règle de droit.

sont auteurs devrait sur le plan juridique être strictement limitée à l'application dans leurs ordres internes respectifs.

Vu sous cet angle, des « exportations forcées » de règles de droit internes apparaissent comme illicites au regard du droit international public et pourraient être analysées comme une ingérence dans l'ordre interne des autres États.

Toutefois, une telle analyse serait superficielle et inexacte, car le droit international général reconnaît aux États une compétence extraterritoriale en matière de l'édiction et de l'exécution de la règle de droit, si la finalité de telles mesures a pour but la protection des intérêts propres de l'État ou bien la protection des intérêts des États tiers.

On parle alors, d'un principe de protection.

La mise en œuvre du tempérament que constitue le principe de protection, est une source de conflits de compétences étatiques d'une part, et d'incertitudes quant à la portée de son champ d'application, d'autre part.

Le droit international général reconnait aux États, un « titre à agir » pour protéger les intérêts des États tiers en même temps que les siens. Le titre à agir dont sont dotés les États se décline sous deux avatars ; il peut s'agir dans certains cas d'une véritable obligation de protection des intérêts légitimes des États tiers, à savoir leur honneur, leur système politique, administratif ou économique.

Ainsi l'ordonnance du 6 mai 1944 a créé un délit d'offense publique commis à l'encontre des chefs d'États étrangers et de leurs représentants. Les articles 133, 134 du Code pénal, sanctionnent la contrefaçon ou l'altération de monnaie étrangère et de billets de banque. De même que les articles 444-1 à 444-9 du Code pénal, sanctionnent la falsification de documents officiels des États étrangers [17].

Le deuxième pendant du principe de protection est le droit à la protection de ses propres intérêts légitimes.

Ainsi au regard du droit international public, un État à la compétence pour réprimer dans son ordre juridique certains actes effectués en pays étranger. L'État se voit ainsi arroger non seulement une compétence d'édiction de la règle de droit à portée transnationale, mais aussi la compétence d'exécution de celle-ci, lorsque les intérêts nationaux vitaux dudit État sont menacés sur le territoire d'un autre pays. Il pourra prétendre à poursuivre les infractions commises à l'étranger par les étrangers sur le fondement de sa législation interne, comme le montre l'article 113-10 du Code pénal [18].

L'exercice du principe de protection par un État constitue une source de conflits, plus particulièrement dans le domaine économique, lorsqu'un État prétend appréhender des actes qui se sont déroulés à l'étranger parce qu'ils produisent des effets nocifs sur son territoire.

En effet, l'application extraterritoriale des lois nationales dans le cadre de l'exercice du principe de protection rentre en conflit avec la compétence territoriale [19] d'un autre État, sa compétence personnelle [20].

L'affaire « *Snowden/Prism* » constitue un exemple parmi tant d'autres de problématiques liées aux conflits de compétences, l'existence de ce type de problématiques n'a rien de nouveau en soi.

(17) Si en temps de paix un État falsifie des documents officiels d'un autre État, il viole son obligation de protéger le système administratif d'un autre État. C'est pour cette raison, que la France a dû présenter ses excuses à la Suisse, lorsque ses agents arrêtés en Nouvelle Zélande en 1985, dans le cadre de l'affaire *Rainbow Warior* étaient porteurs de passeports helvétiques.

(18) La loi pénale française s'applique aux crimes et délits qualifiés d'atteintes aux intérêts fondamentaux de la nation et réprimés par le titre I^er^ du livre IV, à la falsification et à la contrefaçon du sceau de l'État, de pièces de monnaie, de billets de banque ou d'effets publics réprimées par les articles 442-1, 442-2, 442-5, 442-15, 443-1 et 444-1 et à tout crime ou délit contre les agents ou les locaux diplomatiques ou consulaires français, commis hors du territoire de la République.

(19) *Ratione loci*, aptitude d'une juridiction pénale à connaître d'une infraction en fonction d'une circonstance de lieu.

(20) *Ratione personae*, aptitude d'une juridiction pénale à connaître de certaines infractions en fonction de la qualité personnelle du délinquant.

C'est ainsi qu'en matière de droit de la concurrence les États-Unis prétendent faire respecter leurs propres lois nationales par des sociétés mêmes étrangères et opérant en dehors du territoire des États-Unis, pour peu que les activités de ces entreprises, considérées comme répréhensibles, produisent des effets indésirables sur le commerce intérieur américain.

Il s'agit d'une interprétation abusive du principe de protection qui entraînera d'importantes tensions entre les USA et le Royaume-Uni, ainsi que la Suisse, dans les affaires « *U.S. v. Imperial Chemical Industries* » et « *The watchmakers of Switzerland information center* ».

Nous pouvons citer d'autres exemples de conflits basés sur l'application du principe de protection à visées d'ordre stratégique.

Il s'agit de la problématique générée par des embargos de toute nature auxquels les États-Unis prétendent donner une portée territoriale en s'appuyant cette fois-ci sur la compétence personnelle.

La logique appliquée par les Américains est la même que celle qu'ils tentent d'appliquer en matière de droit de la concurrence, la loi américaine adoptant une définition large de ce qu'il faut entendre par « personnes soumises à la juridiction des États-Unis » de façon à soumettre les étrangers au régime juridique édicté.

C'est ainsi que sont traditionnellement définies comme telles les filiales des sociétés américaines à l'étranger, le critère de contrôle étant retenu par l'administration et les juridictions américaines pour décider de l'application extraterritoriale de leurs lois.

Le problème est que ces filiales possèdent juridiquement la nationalité des États dans lesquels elles ont leur siège social ou leur lieu d'incorporation, et de ce fait ces États peuvent également se prévaloir de *ratione personae* à leur égard.

Concrètement cela conduit à des situations juridiquement inextricables pour les filiales et leurs dirigeants, lorsque la législation française considère les dispositions du droit américain contraires à son ordre public, ce qui rend le respect concomitant de ces deux législations impossible. Tel a d'ailleurs été le cas dans la célèbre affaire « Raoul Massardy et autres, société Fruehauf c. Me Solvet et S.A. des Automobiles Berliet » au début des années 1960.

Dans cette affaire la société Fruehauf France, filiale contrôlée majoritairement par la société américaine sous même dénomination, mais juridiquement une société française, car son siège social était situé en France a passé un contrat de fournitures de pièces à la société Berliet. Les pièces commandées devaient être installées dans les camions qui devaient être exportés en République populaire de Chine.

La société mère Fruehauf USA a reçu de la part des autorités fédérales américaines une notification, l'informant de l'illicéité de la transaction réalisée par sa filiale française, car violant un « embargo stratégique » de vente de camions en Chine.

Pour se conformer à sa législation interne la société mère donna pour instruction à sa filiale de dénoncer le contrat qui la liait à la société Berliet.

Se produisait ainsi un conflit de souveraineté entre la compétence territoriale de la France et la compétence personnelle des États-Unis, car ces derniers entendaient leur compétence de manière abusive. Pour le résoudre, un administrateur provisoire avait été nommé par les tribunaux afin de procéder à l'exécution du contrat et la France a pu avoir raison sur la base de sa compétence territoriale, en l'espèce elle disposait à la fois de la compétence d'édiction et de la compétence d'exécution.

Même cas de figure s'était produit en 1982 dans l'affaire dite du « *gazoduc eurosibérien* » où le gouvernement des États-Unis prétendait imposer son embargo stratégique sur certaines exportations en direction de feu l'URSS.

Si les rédacteurs du présent développement ont fait appel à des exemples aussi anciens, cela est fait pour démontrer que « *l'impérialisme juridique* » notamment déployé par les États-Unis d'Amérique n'est pas une nouveauté et, bien qu'il soit perfectible, les États ont élaboré un arsenal juridique permettant de résister tant bien que mal à ce type d'ingérences.

L'exemple le plus frappant, le plus médiatique et le plus récent de l'ingérence des États-Unis est constitué par le programme de surveillance de masse du nom de « PRISM ». Il s'agit en effet d'un programme de surveillance électronique utilisant internet et des sociétés américaines dites de confiance en vue de collecter et traiter un volume jamais égalé de données informatiques.

Cette affaire a été dévoilée par Edward Snowden en Juin 2013.

C'est le *Protect America Act* de 2007, adopté sous la présidence de George W. Bush, et le *FISA Amendments Act* de 2008 qui servent de fondement juridique à ce programme.

Au nom de la lutte antiterroriste le gouvernement américain a autorisé la *National Security Agency* (NSA) à mettre en place un ciblage de personnes vivant hors des États-Unis.

Le *FISA Amendments Act* a été renouvelé en décembre 2012 sous l'administration Obama pour une période de cinq ans en autorisant explicitement les agences de renseignements à surveiller, pour une durée maximale d'une semaine, les appels téléphoniques, les courriels et d'autres communications de citoyens américains sans mandat d'un tribunal à partir du moment où un citoyen américain n'était pas présent sur le sol des États-Unis.

Cette affaire confirme davantage encore l'interprétation excessive et abusive du principe de protection ainsi que celui de compétence personnelle, qui utilise la règle de droit pour légitimer et couvrir des actions liées à l'intelligence économique et la surveillance de masse.

Citons également APT1, dénoncé dans le rapport *Mandiant*, programme lié à une unité militaire chinoise et donc à l'État, conçu en vue de collecter des données d'entreprises dans des pays anglophones correspondant à des secteurs d'activités identifiés comme stratégiques dans le plan quinquennal chinois.

Il existe à l'échelle mondiale sans doute d'autres programmes visant – *via* cette forme d'intelligence économique – à obtenir des informations permettant de se constituer un avantage concurrentiel, économique ou politique.

La démonstration est donc faite que l'ingérence des législations étrangères existe, et que l'arsenal juridique énoncé précédemment ne permet pas de protéger les entreprises en toutes circonstances. Si de nombreux exemples

peuvent laisser entendre que cette ingérence serait majoritairement issue des États-Unis, il ne faut pas se méprendre car si certaines nations sont ou semblent plus avancés que d'autres (États-Unis, Chine, Israël, Royaume-Uni) les autres ne sont pas en reste dans la mise en œuvre de programmes favorisant l'ingérence. On ne pourra que regretter l'hétérogénéité des initiatives à l'échelle européenne.

La politique de sécurité des entreprises peut alors être mise à mal et s'avérer insuffisante, voire inefficace pour protéger les informations sensibles et parfois vitales des entreprises dans un contexte économique et technologique en évolution permanente. Sa définition doit donc prendre en compte cette perpétuelle mutation des contextes législatifs tant comme des catalyseurs que des freins à l'objectif de sécurité qu'elle porte en son sein et imposent sa régulière révision.

Les contre-mesures législatives, organisationnelles et techniques existantes et l'ingérence des législations étrangères dans la politique de sécurité

Comme les auteurs du présent développement l'ont déjà mentionné en amont, l'impérialisme juridique n'est pas une chose nouvelle et plusieurs mesures permettant de le contrer ont été mises en place.

L'Australie, La France, le Royaume-Uni et l'Italie ont mis en place à partir des années 1980, les lois dites de blocage qui permettent de sauvegarder le plein exercice de leurs compétences territoriales en luttant contre les prétentions abusives des pays tiers souhaitant étendre l'application de leur législation hors de leurs frontières en se fondant sur la compétence personnelle ou bien sur le principe de protection.

Le 16 juillet 1980 le législateur français a voté une loi interdisant, sous peine de sanctions pénales, « *la communication de documents, et de renseignements d'ordre économique, commercial ou technique à des personnes physiques ou morales étrangères* » à partir du moment où cette communication pouvait « *porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques de la France ou à son ordre public* »[21].

L'arsenal législatif existe donc et il est de nature à permettre à des Organismes d'Importance Vitale (OIV), de se défendre efficacement notamment dans le cadre des procédures de *discovery*[22] lancées par des tribunaux américains.

(21) J.O. du 17 juillet 1980.

(22) La procédure judiciaire de *discovery* est un de moyen d'obtention de preuves dans le cadre d'une procédure judiciaire aux États-Unis. Un magistrat peut contraindre les parties au contentieux à divulguer toute information susceptible de faciliter l'établissement de preuves.

D'ailleurs il est intéressant de constater que dans les années 1990, le Canada et le Mexique ont adopté également les lois de blocage. Enfin le 22 novembre 1996, la Communauté européenne mettait en place le Règlement CCE n° 2271/96, répondant à une législation américaine particulièrement intrusive consécutive à l'adoption de lois Helms-Burton et d'Amato et en limitant l'impact.

Le Conseil de l'Union européenne a pris le 22 novembre 1996 une position juridique à l'appui de son action commune [23] en indiquant que : « *Considérant qu'un pays tiers a promulgué certaines lois, certains règlements et certains autres instruments législatifs visant à réglementer les activités des personnes physiques ou morales relevant de la juridiction des États membres* » et « *considérant que par leur application extraterritoriale ces lois, règlements et autres instruments législatifs violent le droit international* », sur la base dudit Règlement, il est possible de refuser de reconnaître sur le territoire communautaire des effets de jugements étrangers rendus en application de la législation extraterritoriale contestée (*article 4*).

(23) JOCE du 29 novembre 1996, n°L 309/7

L'article 5 interdit aux ressortissants communautaires de se soumettre à une telle législation extraterritoriale, enfin les États membres sont dans l'obligation de prévoir au bénéfice des entreprises européennes les sommes qui leurs sont réclamées en application d'une législation extraterritoriale devant des tribunaux européens via les saisies des biens des entreprises américaines ou de leurs filiales contrôlées et situées au sein de l'Union européenne (*article 9 du Règlement*).

Toutefois, force est de constater que les solutions normatives mises en place ne sont que très rarement mises en œuvre. Cette situation est souvent liée au déséquilibre économique lors de négociations.

Comme nous l'avions évoqué plus haut, les États-Unis invoquent régulièrement leur compétence personnelle à l'égard des filiales de sociétés américaines situées en dehors de leur territoire. Nous avons vu qu'en application soit de lois de blocage soit en application de la compétence territoriale, les magistrats français disposent de moyens pour limiter l'application exorbitante du droit américain, toutefois, les intérêts et pressions économiques mises en jeu rendent inefficaces l'application de la règle de droit.

Pour gérer ce type de situations, il est possible et plus particulièrement pour les OIV de recourir à des montages corporate qui, en s'appuyant sur les structures de holding, permettent de mettre en place un jeu d'écrans de personnalités morales rendant difficile, voire impossible l'application de la compétence personnelle ou de principes de protection invoqués par les États tiers.

Il s'agit d'opérations bien souvent complexes et coûteuses à mettre en place, leur intérêt doit donc être évalué en tenant compte de la valeur intrinsèque des informations ou du patrimoine que l'on souhaite ainsi protéger.

Un autre moyen de protection tient à la négociation âpre, minutieuse et rigoureuse des engagements contractuels. Rappelons qu'un contrat est un acte juridique qui institutionnalise la rencontre de volonté entre les parties qui le signent. Tout contrat, y compris un contrat d'adhésion est potentiellement négociable et doit être négocié.

Au sein des entreprises, les contre-mesures possibles à mettre en œuvre sont potentiellement connues et décrites dans les textes normatifs concernant la définition d'une politique de sécurité et du système de management qui doit contribuer à la déployer et la faire vivre, tel ISO 27xxx. Il convient cependant de prêter attention à certains aspects du dispositif et de ne pas considérer l'approche « Sécurité des SI » comme une recherche de conformité à un instant « *t* » de la vie de l'entreprise.

Il est fondamental que la PSSI soit formulée par la direction de l'entreprise, et qu'elle permettre – avec des moyens alloués suffisants - de déployer un SMSI en phase avec les objectifs énoncés, en toute cohérence avec d'autres systèmes de management existants, notamment avec le système de management de la qualité, de la sécurité des conditions de travail et de l'environnement.

Il convient également de veiller à ce que la PSSI soit cohérente avec les objectifs de chaque « métier » de l'entreprise et avec les besoins de ses clients et partenaires.

La norme ISO 27001 prévoit de réaliser régulièrement des contrôles et des étapes de capitalisation afin de garantir au mieux la pertinence du SMSI, de l'ajuster en permanence en fonction des évolutions du contexte. Sans entrer dans le détail de la structuration et du contenu de la politique de sécurité, ces étapes s'inscrivent dans une logique d'amélioration continue (r*oue de Deming*).

Pour répondre à la dimension internationale, la politique de sécurité d'un système d'information, comme le souligne l'OCDE [24] doit mettre en place une notion de culture sécurité et une continuité de la gestion des risques du Système d'information. Cette continuité doit contribuer à instaurer une gestion par le risque au sein de cette culture sécurité.

(24) Organisation de Coopération et de Développement Economiques. L'OCDE est une organisation internationale d'études économiques, dont les pays membres ont en commun un système de gouvernement démocratique et une économie de marché.

Selon le référentiel ISO Guide 73, *Management du risque – Vocabulaire* fournissant les principes et lignes directrices, la nouvelle définition (*depuis janvier 2010*) couple le risque aux objectifs de l'organisation : « *le risque est l'effet de l'incertitude sur l'atteinte des objectifs* ».

Cette définition complète une approche initialement mathématique qui permet toutefois de construire le processus d'analyse : « *le risque est la combinaison de probabilité d'évènement et de sa conséquence* ».

Cette analyse consiste principalement à évaluer le risque en fonction de deux facteurs, sa probabilité d'occurrence et l'importance de son impact s'il venait à se concrétiser.

La combinaison des deux facteurs permet de déterminer un niveau de risque. Ainsi, à une probabilité élevée de causer un dommage important et/ou un impact fort en cas d'occurrence du risque correspond un niveau de risque maximum, à l'inverse une probabilité faible de causer peu de dégât entraine un risque minimum.

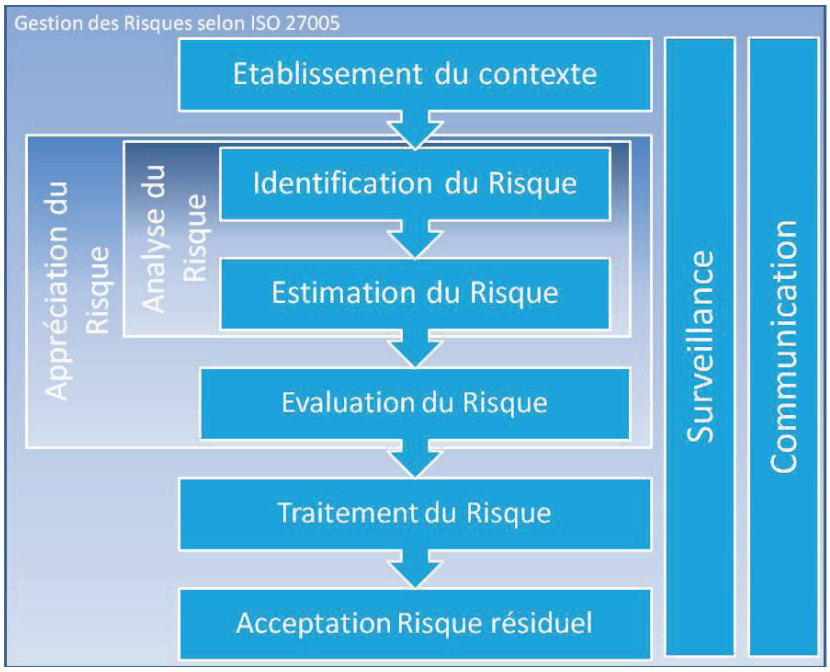
Dans le domaine de la SSI, les menaces sont de plus en plus nombreuses et variées : citons principalement la malveillance, l'erreur et l'accident. Les ressources informatiques impactées peuvent être nombreuses (serveurs, bases de données, réseaux, bâtiments, sites,...), et *in fine*, ce sont les informations sensibles de l'entreprise qui sont touchées.

La gestion des risques doit être bâtie par une équipe pluridisciplinaire représentative des acteurs clés de l'entreprise. Elle s'appuie sur une des nombreuses méthodologies existantes et reconnues.

L'ANSSI dans ses outils méthodologiques propose EBIOS 2010 (Expression des besoins et identification des objectifs de sécurité). On peut également citer MEHARI (Méthode harmonisée d'analyse des risques).

Nous ne détaillerons pas plus chacune d'entre elles, sachant néanmoins qu'elles s'appuient sur le référentiel ISO 27005 et visent à la construction d'un référentiel de la sécurité des systèmes d'information.

Selon ISO 27005, le processus de gestion des risques s'organise en plusieurs sous-processus:



Toute analyse de risque commence donc par l'établissement de son contexte en prenant en compte le contexte externe et en intégrant les attentes des parties prenantes tels que les États, les organismes régulateurs, les actionnaires, les clients... Le contexte interne est également pris en compte et s'inscrit dans l'organisation des fonctions de contrôle définies au sein de la Direction des Système d'Information (DSI, RSSI, contrôle IT,...) ou dans l'organisation d'autres fonctions concernées (risk manager, audit, contrôle); les enjeux métier de l'entreprise sont obligatoirement des éléments structurants du contexte interne.

À cette étape déjà, il est important d'évaluer la nécessité de prendre en compte la dimension internationale de l'entreprise; en effet, lorsque ce processus n'est pas mature, il est d'usage de le mettre en œuvre progressivement en commençant par un périmètre réduit et relativement « facile » à traiter si tant est que cela soit possible.

Or, il faut garder en mémoire que le fait qu'une entreprise soit de dimension internationale constitue déjà un risque en soi et que l'ingérence est à considérer comme une menace.

L'étape d'identification du risque consiste à analyser les évènements redoutés et les scenarii de menaces. Durant cette étape il est nécessaire de procéder à l'identification et à la classification des ressources du SI [25] ciblées par l'analyse de risque afin de délivrer une liste des scenarii de risque majeurs pesant sur elles.

(25) Ressources du SI : on entend par ressources du SI les applications, les données, les moyens techniques nécessaires au fonctionnement des applications et au traitement des données, les environnements d'exploitation ainsi que les compétences requises pour leur conception, leur fonctionnement, leur maintenance et leur utilisation.

L'étape d'estimation du risque consiste à analyser les besoins de sécurité, la gravité des évènements et la vraisemblance des menaces et ce pour chaque scenario. L'estimation du risque permet de quantifier les grandeurs caractéristiques de chaque scénario en termes de probabilité, de niveaux d'impact et de niveaux de vulnérabilité. Les types d'impacts généralement retenus dans le cadre de l'évaluation de la gravité sont de nature financière, réputationnelle (portant atteinte à l'image), juridique ou relative aux personnes et à l'environnement. L'étape d'évaluation du risque consiste à estimer les risques identifiés, c'est-à-dire leur attribuer un niveau de gravité et à les ordonner les uns par rapport aux autres. Il en résulte une cartographie des risques qui permet de trouver un équilibre entre « coût du risque » et « coût de la sécurité ».

L'étape de traitement du risque détermine les mesures de sécurité à mettre en œuvre en regard de chaque risque jugé inacceptable. À l'issue de cette étape, il subsiste alors ce qu'il est convenu d'appeler des risques résiduels [26], donc acceptables ou dans certains cas partagés avec un tiers (recours à une assurance par exemple).

(26) Risques résiduels : risques subsistant après le traitement des risques. Un risque résiduel peut inclure un risque non identifié ou bien un risque accepté.

Le processus d'acceptation du risque doit impliquer le métier (ou sa maîtrise d'ouvrage par délégation), la fonction de responsable de sécurité du SI et tenir compte des acteurs touchés par d'éventuels impacts collatéraux.

La surveillance est la dernière étape et peut notamment être effectuée *via* un reporting sur différents indicateurs. Devront être suivis et mesurés :

- l'efficacité des mesures de sécurité, en évaluant les risques résiduels acceptés, surveillant l'évolution de ces risques dans le temps ;
- les changements structurels ou fonctionnels de l'entreprise ;
- l'apparition de nouvelles menaces ;
- l'efficacité du processus global (principe de l'amélioration continue).

Indissociablement, une analyse de risque s'accompagne d'un plan de communication autour des risques étudiés afin d'assurer une meilleure compréhension des enjeux et des contraintes et de permettre à chaque acteur, qu'il soit en interne (services juridique, achats) ou dépendant des différentes structures de l'entreprise hors du territoire, de prendre conscience de la problématique et d'assumer ses responsabilités.

Parmi les contre-mesures, il est également possible de mettre en place un *Security Operation Center* (SOC) qui permet de s'assurer du respect de la PSSI en assurant une fonction de veille, de surveillance, de contrôle et de *reporting*.

En effet, un SOC est un centre de contrôle où sont remontés et centralisés les logs, traces, piste d'audit, alertes, etc., générés par les systèmes et les applications sensibles, dispositifs de sécurité et mécanismes de surveillance de l'entreprise. Des experts en sécurité analysent ces données, aidés par des outils de corrélation (SIEM). Un pré-requis à la mise en place d'un SOC et

l'implémentation d›un dispositif de journalisation qui permet de disposer des traces des opérations réalisées au moyen du SI de l'entreprise ou sur les ressources qui le composent. Le contenu des traces doit répondre au minimum au « principe QQQ » (Qui ? Quand ? Quoi ?).

Par ailleurs, l'exigence de datation des traces implique la mise en place d'un dispositif d'horodatage fiable et précis, reposant sur une base de temps normalisée et homogène pour l'ensemble des traces enregistrées.

Il est recommandé que, dans le contexte d'ingérence internationale, le SOC soit implanté sur le sol national afin de dépendre de la juridiction française intégrant une analyse permanente de l'environnement international afin d'être à même d'appréhender les attaques et incidents répertoriés en interne et en externe, le contexte réglementaire ainsi que les normes et méthodes reconnues, les vulnérabilités techniques découvertes et les contre-mesures associées, les grandes tendances technologiques et les bonnes pratiques tous secteurs confondus.

Parmi les recommandations de mise en œuvre d'une politique de sécurité, les textes normatifs insistent sur l'importance de la communication et de la sensibilisation des acteurs de la sécurité, il s'avère que cela est l'affaire de tous si l'on veut œuvrer pour une culture sécurité.

Pour répondre aux exigences d'un contexte international, la PSSI doit être comprise et fédérer l'ensemble des parties prenantes de l'entreprise. Pour cela des campagnes de sensibilisation à destination de l'ensemble des acteurs est nécessaire. La population concernée par cette sensibilisation est très large car elle concerne les utilisateurs finaux, mais aussi les personnes en position de prise de décisions (responsable métiers, chef de projet, management, top management...).

En effet chacun est amené dans l'exercice de sa mission à prendre des décisions qui peuvent avoir des conséquences majeures sur la protection mise en place contre la cybercriminalité. Il est donc primordial que leur soient expliqués les concepts, les risques et les axes de solution. Cette sensibilisation vise aussi à limiter les comportements à risque. En parallèle, l'organisation de sessions de formation sur l'évolution des moyens de protections vis-à-vis des nouveaux usages permet de maintenir un niveau de compétence en interne nécessaire au maintien d'une PSSI pertinente.

Étant donné qu'il n'existe pas de « législation internationale » qui encadre l'utilisation de l'outil informatique et que chaque pays a sa propre législation qui s'appuie sur des lois plus ou moins restrictives voire laxistes pour certains pays, une PSSI doit spécifier les principes techniques à implémenter afin de protéger les actifs sensibles de l'entreprise en respect de la législation locale.

Les principales menaces connues à ce jour pour une entreprise sont les attaques de type « *Distributed Denial of Service* » (DDoS)[27] impactant la disponibilité d'un service et les « *Advanced Persistent Threats* » (APT)[28] dont la finalité est le vol d'information ou l'exfiltration, vers un pays étranger, de données stratégiques[29] d'une entreprise pouvant s'accompagner de la perte de propriété de celle-ci. Pour contrer ce genre de menaces, il existe un certain nombre d'outils techniques disponibles sur le marché que les auteurs n'ont pas cru nécessaires de détailler ici.

(27) Une attaque par déni de service *(denial of service attack,* d'où l'abréviation DoS) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. Lorsque plusieurs machines sources sont utilisées pour l'attaque on parle alors de DDoS (*distributed denial of service attack*)

(28) Une *Advanced Persistent Threat* (APT) est une intrusion informatique souvent initiée *via* un code malveillant dont la finalité est de demeurer le plus longtemps possible au sein du SI introduit afin d'y extraire des données sensibles ou financièrement intéressante.

(29) Les Données stratégiques sont constituées par toutes les informations numériques concernant les actifs stratégiques (brevets, marques, contrats, filiales, compétences, effectifs ...), actifs sur lesquels repose l'essentiel de la rentabilité ou de l'activité d'une entreprise. Le concept de données sensibles ne peut pas être employé dans ce contexte car en droit français des données sensibles sont des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à leur santé ou à leur vie sexuelle.

Ce qu'il faut retenir de l'arsenal de contre-mesures techniques, c'est que les outils efficaces pour lutter contre les attaques suivent le rythme d'apparition des nouvelles menaces. Pour prétendre à un niveau de protection conforme à la politique de sécurité, les choix organisationnels d'une entreprise doivent veiller à préserver un niveau de compétence technique en adéquation avec la complexité des attaques. De plus, la mise en place de solutions techniques sans identification des actifs à protéger comme un dispositif humain à même de les exploiter représente une initiative vaine.

© INHESJ – Septembre 2014 – Ingérence et politique de sécurité des systèmes d'information

OPTIONS D'UNE ENTREPRISE RETENUES PAR LES AUTEURS POUR METTRE EN PLACE UNE POLITIQUE DE SÉCURITÉ AU NIVEAU INTERNATIONAL

Partie 2

Afin de proposer les différentes options, les auteurs vont en premier lieu exposer les politiques de sécurité et d'organisations les plus adaptées à la problématique au sein d'une entreprise puis les différents cas d'usage et solutions techniques à implémenter en regard de ces stratégies et politiques.

Politique de sécurité et organisation au sein d'une entreprise

Selon les statistiques publiées par le CLUSIF en 2012, la fonction SSI est portée par 1 à 2 personnes pour 72% des entreprises ayant répondu à la question de l'effectif de l'équipe chargée de la sécurité de l'information permanente en leur sein.

Pour 54% d'entre elles, la fonction RSSI est clairement identifiée.

La nomination d'un RSSI est incontestablement la première action d'une entreprise qui désire mettre en œuvre toutes les actions nécessaires à la protection de ses données sensibles.

Seul un RSSI désigné et motivé par une lettre de mission claire peut définir une politique de sécurité et la faire vivre. Bien qu'il n'agisse pas seul – le rôle de RSSI est à considérer comme un chef d'orchestre – son positionnement dans l'organigramme est le reflet de la maturité de l'entreprise.

Toujours selon le CLUSIF, dans une étude menée entre 2008 et 2012, le rattachement hiérarchique du RSSI se fait très majoritairement auprès de la Direction générale ou de la DSI. Dans des cas plus rares, le RSSI est rattaché à une direction administrative ou financière.

Il a été constaté que l'évolution du rattachement hiérarchique d'un RSSI dans le temps se fait d'abord au sein d'une DSI – lorsque l'entreprise prend conscience de la nécessité de se sécuriser – et lorsque la culture sécurité est ancrée, le poste peut se structurer davantage et évoluer vers la DG ou vers une Direction Gestion des Risques.

Quoi qu'il en soit, le RSSI doit œuvrer pour le décloisonnement des modes de fonctionnement de tous les acteurs de la sécurité.

Il peut – il doit pouvoir – s'appuyer sur des porteurs et des référents dans l'organisation qui relaieront la mission selon les compétences requises, et permettront aux collaborateurs d'identifier plus facilement leurs « interlocuteurs sécurité » afin d'assurer que le processus de sécurité soit agile et performant.

Ainsi que nous l'avons évoqué, il est désormais établi que le système d'information est un support-clé et incontournable de l'activité des métiers de l'entreprise. Tout dysfonctionnement du SI, qu'il soit involontaire ou délibéré, peut potentiellement compromettre, dans le meilleur des cas, l'atteinte des objectifs de l'entreprise et parfois même menacer sa survie. Il convient donc de protéger le SI à hauteur de la valeur des biens qu'il recense. Pour autant, les besoins de protection vis-à-vis du SI diffèrent d'un métier à l'autre au sein d'une même entreprise. Il est donc pertinent d'adapter la protection du SI au juste nécessaire, sous peine de dépenses inappropriées et de contraintes sécuritaires injustifiables auprès des utilisateurs.

La gestion des risques est précisément le moyen d'identifier les risques les plus élevés et de décider des mesures de sécurité à mettre en place en fonction des priorités de menaces redoutées par l'entreprise.

L'analyse des risques liés au SI est une mission stratégique, fruit d'un travail d'équipe impliquant des acteurs-clés tels que :

- le propriétaire de l'information sensible potentiellement menacée ;
- la filière RSPI (Responsable de la sûreté du patrimoine informationnel) ;
- la filière RSSI (Responsable de la sécurité des systèmes d'information) ;
- le *risk manager* ;
- le responsable IT pour le métier concerné ;
- le responsable IT pour le métier Opérations (au sens ITIL[30] du terme) ;
- le métier juridique de l'entreprise ;
- le métier achat de l'entreprise.

(30) L'ITIL (*Information Technology Infrastructure Library*) est un ensemble d'ouvrages recensant les bonnes pratiques du management du système d'information.

Seule la collaboration simultanée de ces acteurs clés peut garantir une analyse exhaustive des risques business, dont on déduit des risques IT pertinents et adaptés à la réalité des métiers et des menaces existantes.

À ce niveau d'identification des risques mêlant stratégie de sécurité et par métier, on peut envisager de construire un référentiel des risques intégrant nativement la notion d'ingérence et la couverture associée et qui pourra ensuite être réutilisé à d'autres mailles dans l'entreprise.

Ainsi, la gouvernance sécurité pourrait-elle préconiser de procéder à une gestion de risque par projet, chaque projet s'inspirant alors des risques génériques puisés dans le référentiel s'appliquant au domaine qu'il couvre.

Les risques identifiés dans le cadre d'un projet sont des éléments d'informations qui peuvent s'avérer très structurants pour sa conduite. Citons par exemple le cas où un risque identifié peut ensuite être traduit comme un pré-requis dans le cahier des charges ou encore un ensemble d'exigences non fonctionnelles

(comme le respect de bonnes pratiques ou de contraintes de sécurité) dans un référentiel d'exigences pour développer une nouvelle application.

Il résultera de la démarche d'analyse de risque la définition d'un politique de sécurité qui couvrira à minima les thèmes suivants :

- organisation de la sécurité ;
- gestion des risques SSI ;
- sécurité et cycle de vie ;
- assurance et certification ;
- aspects humains ;
- planification de la continuité des activités ;
- gestion des incidents ;
- sensibilisation et formation ;
- exploitation ;
- gestion des identités et des moyens d'authentification ;
- journalisation ;
- infrastructures de gestion des clés cryptographiques,

Lorsque la politique de sécurité est définie et déclinée en mesures de sécurité, il convient qu'elle soit connue de tous au juste nécessaire afin que chacun devienne un acteur averti de la sécurité de son entreprise et concoure au déploiement de la culture sécurité.

La PSSI ainsi définie et connue de tous, doit être pérenne et savoir s'adapter au contexte, dont on a vu qu'il évolue en permanence, d'une part parce que la menace cyber est en pleine expansion et d'autre part car les entreprises sont elles-mêmes inscrites dans un processus permanent d'adaptation à leur environnement. De fait, les réorganisations internes, les évolutions de structure, les nouveaux marchés, les changements de stratégie ou d'objectifs, les modifications budgétaires sont autant de raisons nécessaires et suffisantes pour réajuster le SMSI, réengager un exercice d'analyse de risques et réévaluer l'adéquation du dispositif sécurité en place.

Afin de s'assurer de la pertinence du SMSI mis en œuvre et des mesures de sécurité qui en découlent, la norme ISO 27xxx préconise une gouvernance de la sécurité impliquant les décideurs auxquels il conviendra de fournir les bonnes informations de suivi au moyen d'indicateurs bien conçus, c'est à dire en adéquation avec les objectifs de sécurité.

Un exemple d'indicateur à mettre en place a été évoqué dans la démarche d'analyse de risque : il s'agit de suivre le risque résiduel et surveiller l'évolution du risque en prenant en compte tant l'actualité que la veille, chacun pouvant indiquer de nouvelles menaces, ainsi que le suivi des incidents de sécurité pour lesquels l'entreprise aura préalablement veillé à mettre en place un dispositif d'identification.

Par la suite afin d'avoir un suivi de la mise en œuvre de la PSSI et de sa bonne déclinaison au sein de l'organisation, une démarche de mise en place d'indicateurs permettra de gagner en visibilité, prioriser les périmètres qui ne

seraient pas au niveau minimal acceptable au sein de la structure et permettre une meilleure communication aux équipes opérationnelles comme à la direction justifiant les actions entreprises.

Dans un premier temps il convient de choisir les bons indicateurs. À ce stade, il est pertinent de capitaliser sur les travaux que de nombreux organismes ont d'ores et déjà produits. On distinguera néanmoins deux grandes familles d'indicateurs : les indicateurs plutôt axés sur la sécurité opérationnelle et ceux permettant de mesurer le niveau de maturité sécurité de l'organisation. Parmi les référentiels, normes, outils ou bonnes pratiques aidant à la mise en œuvre d'indicateurs on pourra citer CobiT[31], ISO 27002, les travaux de l'ETSI[32] ou du club R2GS[33].

Parmi ces références un choix pertinent des indicateurs sera rendu possible par l'analyse de risque qui aura été préalablement réalisée et d'une manière générale par une bonne connaissance des attentes de sécurité au sein de l'organisation. Dans la démarche il faut être pragmatique : il ne servira à rien de mesurer des éléments dont on sait qu'ils n'évoluent pas car ils font alors partie du risque résiduel. Il en va de même sur le choix d'indicateurs qui n'apporteraient qu'une simple mesure sans prendre en compte le contexte de l'organisation et un suivi dans le temps.

En fonction du modèle d'organisation choisi pour la répartition des équipes de sécurité, il peut être intéressant également de scinder les indicateurs par plaques, pays, entités. En rapprochant les objectifs de sécurité avec un angle de vue qualité, c'est l'organisation dans son ensemble qui bénéficiera de l'émulation et des bonnes pratiques de chacun plutôt que d'avoir une transmission descendante de l'ensemble des mesures à appliquer. Il ne faut pas oublier qu'au sein d'une organisation c'est la somme des compétences de chacun qui garantit la réussite du schéma directeur et de sa composante sécurité.

Autre dispositif jugé essentiel par les auteurs : la veille. Dans une approche globale de la problématique et quel que soit le modèle de l'organisation (nationale ou internationale), la veille est un élément clé permettant une meilleure gouvernance de la politique de sécurité. Qu'elle soit sectorielle, concurrentielle ou globalement orientée sécurité, la veille permet de réajuster le niveau de risque de l'organisation, anticiper de nouvelles menaces. Elle permet par ailleurs un travail de capitalisation sur la réaction de nos pairs face à des problématiques qui peuvent se présenter dans l'entreprise.

Cette veille peut être mutualisée avec des cellules de veille interne à l'organisation ou bien dédiée aux équipes sécurité. Si tel est le cas, il peut être intéressant de mettre en place une souscription ou la mise en place d'une cellule CERT qui *a minima* permettra de bénéficier de la veille réalisée par les autres CERTs. La veille pourra aussi être partagée par les équipes en charge de la sécurité opérationnelle ou plus globalement du SOC. En effet, c'est en se nourrissant de son expérience en matière de gestion, identification et traitement d'incident de sécurité que l'organisation s'améliorera dans sa capacité de détection et dans sa capacité à proposer des remèdes appropriés. La veille contribue activement à la capitalisation et au principe d'amélioration continue qui constitue une des briques de l'efficacité du SMSI.

(31) CobiT (*Control Objectives for Information and related Technology*) permet un découpage du Système d'Informations en différents processus permettant l'aide à la décision, la garantie de mise en œuvre de la sécurité et de ses mesures de contrôle.. Cela permet d'initier un socle commun de références et d'indicateurs qui permettront d'apprécier le niveau de maturité de l'organisation et ainsi pouvoir plus facilement la comparer.

(32) L'ETSI (*European Telecommunications Standards Institute*) a pour vocation la production de normes de télécommunications. Il a permis la définition d'un standard d'indicateurs sécurité (ISI : Information Security Indicators).

(33) Club de Réflexion et de Recherche en Gestion Opérationnelle de la Sécurité : reprend les travaux de l'ETSI pour définir le cadre d'une démarche d'indicateurs sécurité.

Cas d'usage et solutions techniques

Nous avons eu l'occasion d'exposer précédemment les impacts potentiels de l'ingérence des législations étrangères sur l'atteinte des objectifs d'une entreprise et sa politique de sécurité sous un angle juridique. Nous avons également développé l'éventail des contre-mesures législatives existantes à ce jour.

À la maille de l'entreprise, il est possible et souhaitable également de capitaliser sur les constats antérieurs et mettre en place des bonnes pratiques innovantes non pas par leur concept mais par leur modalités de mise en œuvre.

Ainsi, nous avons évoqué dans le paragraphe précédent l'importance de la communication et des actions de sensibilisation de la politique de sécurité, voyons maintenant un cas d'usage dans une société internationale constamment confrontée à des problématiques d'ingérence dans le cadre de ses négociations commerciales, chez qui l'entité juridique a mis au point un processus judicieux.

Grâce à la sensibilisation des équipes commerciales et des équipes achats, il est devenu possible dans le cadre de négociations contractuelles de circonscrire les aspirations des entreprises et/ou des administrations étrangères en invoquant soit les dispositions de lois de police[34], soit des dispositions d'ordre public[35].

(34) Lois d'application immédiate, essentielles à la sauvegarde de l'ordre politique, économique et social d'un État.

(35) En droit civil, signifie les règles juridiques qui s'imposent pour des raisons de moralité, de sécurité impératives dans les rapports sociaux et auxquelles il est impossible de déroger par des conventions personnelles.

Ainsi cette entreprise, dans le cadre des négociations contractuelles avec un important client américain et pour éviter de devoir satisfaire aux demandes de renseignements de l'administration des États-Unis en application des dispositions de *Patriot Act* portant sur ses employés, a préféré passer son contrat par sa filiale américaine de telle sorte que la législation américaine s'appliquait uniquement à ses propres nationaux.

La mobilité des collaborateurs, particulièrement dans le cas d'une entreprise à vocation internationale représente un autre cas d'usage important. Ce thème a d'ailleurs été étudié par l'ANSSI.

Il convient d'être particulièrement vigilant lors des déplacements. En effet, les risques augmentent dès lors qu'un collaborateur véhicule des données sensibles en dehors de son périmètre interne, les effets de l'ingérence peuvent prendre toute leur dimension.

Lors des déplacements internationaux, certains pays se sont arrogés lors des passages aux frontières le droit d'accéder « librement » aux données même chiffrées. Il convient dès lors de l'anticiper dans la politique de sécurité et de communiquer largement sur les comportements à adopter en conséquence.

Selon les cas, on peut envisager de faire utiliser aux collaborateurs mobiles des matériels dédiés à la mission et ne comportant que les strictes informations nécessaires à celle-ci et prévoir que ces matériels seront au retour de mission analysés et reformatés en vue d'une prochaine mission.

Suivant la mission et le pays dans lequel elle a lieu, des mesures plus drastiques peuvent être envisagées, telles qu'interdire de voyager avec toutes sortes de matériels (portable, téléphone, tablettes, clé USB), ces derniers étant fournis sur place par la représentation locale de l'entreprise. Les données nécessaires seront récupérées par l'intermédiaire d'une connexion sécurisée ou par un webmail en https qui ne sera utilisé que pour récupérer des fichiers chiffrés qui seront ensuite supprimés.

Sur place, sans se considérer en environnement hostile, il convient d'adopter des mesures de prudence pour s'assurer de conserver le caractère sécurisé des données. Ainsi, ne pas considérer les coffres d'hôtel comme des lieux sûrs, éviter les connexions dans des cybercafés, ne pas utiliser de clé USB dont on ne connaîî pas l'origine...

Tout comme à l'arrivée dans un pays étranger, il convient d'adopter la même prudence au départ. Ainsi, mieux vaut voyager sans équipement ou à défaut sans document, *a fortiori* confidentiel et penser à supprimer les historiques de navigation et d'appel ...

En cas de suspicion, il convient de faire analyser son poste afin d'éviter d'introduire « le ver dans le fruit » lors du retour sur le réseau d'entreprise.

Abordons maintenant des cas d'usages plus techniques qui nous apparaissent les plus structurants pour traiter la problématique de cet exposé. L'ensemble des dispositifs de sécurité qu'une entreprise doit mettre en œuvre doit répondre au principe désormais reconnu indispensable de défense en profondeur. Seuls les principes étroitement liés à une exposition externe (internationale) du SI sont abordés. Pour répondre aux exigences internationales de sa politique de sécurité, une entreprise doit appliquer le principe de défense en profondeur, qui consiste à exploiter plusieurs techniques de sécurité afin de réduire le risque lorsqu'un composant particulier de sécurité est compromis ou défaillant.

Pour ce faire il convient d'imposer la protection des données stratégiques afin de se prémunir des « *backdoors* »[36] implémentées par les éditeurs étrangers dans leurs solutions.

Il faut également tenir compte des réglementations existantes sur les biens et technologies à double usage[37] dont l'arrangement de *Wassenaar*[38], établi en 1996, est le principal outil juridique permettant, sur le plan international, de réguler les transferts de ces technologies.

Dès lors que le principe de défense en profondeur est acquis, il nous paraît nécessaire d'aborder la difficile question de la localisation des données, question qui en appelle une autre, à savoir le choix éventuel du recours au *Cloud* et le choix du type de *Cloud*.

Le *Cloud computing* est un modèle d'accès à travers internet à des ressources informatiques partagées telles que des réseaux, des serveurs, du stockage, des applications et des services. Ce modèle favorise la disponibilité permanente des ressources et un accès théorique à des ressources sans limites, si bien que les entreprises peuvent voir dans le *Cloud computing* un moyen d'augmenter leur efficacité, de réduire le « *time to market* » et de faciliter l'innovation en réduisant l'investissement initial. Autre atout du *Cloud computing*, les entreprises n'ont plus besoin d'immobiliser du capital, le modèle économique étant basé sur le paiement à l'usage.

(36) Dans un logiciel, une porte dérobée (de l'anglais *backdoor*, littéralement porte de derrière) est une fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au logiciel.

(37) Les biens et technologies à double usage (ou biens à double usage ou encore technologies à double usage sont des produits et technologies qui peuvent être utilisés tant à des fins civiles que militaires.

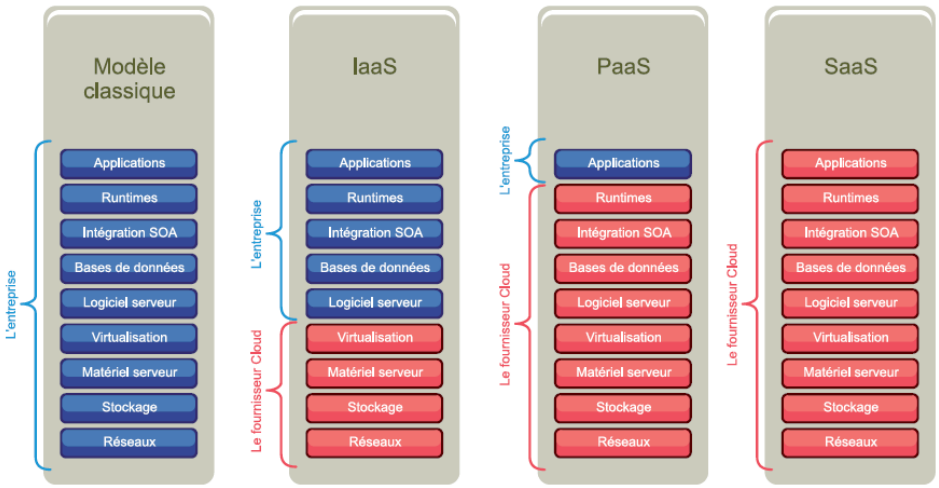
(38) A la date de 20 janvier 2012, le groupe comprend 41 États membres : l'Afrique du Sud, l'Allemagne, l'Argentine, l'Australie, l'Autriche, la Belgique, la Bulgarie, le Canada, la Corée du Sud, la Croatie, le Danemark, l'Espagne, l'Estonie, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Irlande, l'Italie, le Japon, la Lettonie, la Lituanie, le Luxembourg, Malte, le Mexique, la Nouvelle-Zélande, la Norvège, les Pays-Bas, la Pologne, le Portugal, la République tchèque, la Roumanie, le Royaume-Uni, la Russie, la Slovaquie, la Slovénie, la Suède, la Suisse, la Turquie,et l'Ukraine.

L'état de l'art veut que les données soient hébergées (cloisonnées) dans des zones de sécurité adaptées à leur niveau de sensibilité. En ce qui concerne les données stratégiques d'une entreprise française, données à forts enjeux donc les plus convoitées par les États ou la concurrence, il est préférable que la PSSI stipule que ces données stratégiques doivent demeurer au sein des infrastructures d'hébergement (*datacenters*...) sous gouvernance de l'entreprise présentes sur le sol français.

En effet, la localisation des données a des répercussions juridiques fortes puisque certains pays disposent de règles permettant à leur gouvernement d'accéder à tous types de données hébergées sur le territoire national. C'est le cas notamment des États-Unis sous couvert du *Patriot Act*, mais également d'un grand nombre de pays européens.

Si l'entreprise ne possède pas ses propres infrastructures d'hébergement, une alternative peut être l'hébergement de ces ressources stratégiques en externe au sein de *clouds* souverains (*cf. le projet Andromède en France*), ceux-ci garantissant une localisation globale des données en France, leurs *datacenters* y étant tous situés.

Pour mémoire, il existe trois modèles différents : l'Infrastructure *As A Service* (IaaS), la *Platform As A Service* (PaaS) et le *Software As A Service* (SaaS).



Il existe trois types de *cloud* en fonction du degré de mutualisation des infrastructures, à savoir, le cloud public, le *cloud* communautaire, le *cloud* privé. Evidemment, chaque modèle de service et de déploiement a ses avantages et inconvénients financiers et opérationnels, mais ces points ne seront pas abordés dans le présent document.

Tous ces avantages ne doivent pas masquer de nouvelles formes de risque pour chaque type de *cloud*, chaque modèle de service et chaque type d'accès. Les menaces ciblent les architectures de type *cloud* sur les quatre critères de la PSSI (disponibilité, intégrité, confidentialité, traçabilité). Certaines spécificités du *cloud* présentent des menaces pour l'atteinte aux besoins de sécurité imposés par la classification des informations et des ressources manipulées. Seuls les aspects de la contractualisation de service *cloud* soumis à des contraintes de législations étrangères seront traités dans ce document.

Le point commun à l'ensemble des offres de *cloud computing* est qu'elles privilégient l'utilisation du réseau internet dont la gouvernance est, à ce jour, sous tutelle américaine. La NTIA a annoncé que les États-Unis abandonneront le contrôle de l'ICANN en 2015, et que l'organisme actuellement rattaché au Département du Commerce de l'administration américaine sera alors placé entre les mains d'une organisation internationale dont les formes juridiques restent à déterminer.

Le critère de confidentialité est aujourd'hui le plus grand frein à la migration de certains services hébergés dans l'entreprise vers le *cloud*. La menace est en réalité de nature différente selon le profil de l'attaquant, le prestataire retenu pour l'hébergement des données ou un attaquant externe.

La politique de sécurité liée au *cloud computing* devra non seulement prendre en compte les aspects de localisation des données mais également la localisation des équipes qui en assure l'exploitation et la maintenance car elles ont accès aux données de l'entreprise.

Au sens de la réglementation européenne, les données confiées à un tiers restent la propriété du client. Or, dans les pays tels que les États-Unis, ces mêmes données relèvent de la propriété des prestataires et ces derniers ne sont pas soumis à des obligations de protection.

Les équipes du fournisseur en charge de l'exploitation des infrastructures étant généralement composées d'individus de nationalité différentes et en tenant compte qu'un individu, indépendamment du lieu où il se trouve est tenu à des devoirs qui incombent à sa nationalité, il en découle un réel risque d'exfiltration et de divulgation de données stratégiques pour l'entreprise qui contractualise un service dans le *cloud*.

Pour traiter la problématique de la localisation de l'hébergement, il est particulièrement structurant de faire le choix du type de *cloud* en fonction de la classification des données. Ainsi, par exemple les données stratégiques de l'entreprise ne peuvent pas être éligibles à une solution autre qu'une solution de *cloud* privé.

Il convient également pour limiter les effets de l'ingérence de prendre en compte la notion de chiffrement des données dans le *cloud*. Celle-ci devant se faire de manière totalement indépendante du fournisseur de *cloud*. Ce dernier ne doit pas posséder les clés de chiffrement et le déchiffrement devra se faire impérativement sur le poste client.

La politique traitera également des aspects d'accès au service *cloud* qui se fera exclusivement *via* des protocoles sécurisés (chiffrés) et une authentification forte sera requise.

En ce qui concerne le prestataire, le risque principal est dû au contexte juridique dans lequel le service est offert. Le risque juridique est à considérer dans un contexte international car la loi applicable et la juridiction compétente dépendent de la localisation des traitements.

Sans exigence du client sur la localisation de ses données, le fournisseur de service pourrait rendre la prestation de n'importe quel pays et appliquer la réglementation locale.

Dans un contexte international, il nous apparaît indispensable pour une entreprise d'avoir recours à des mécanismes d'authentification renforcés et résilients. Dans le cas d'accès à des données stratégiques, il s'agira de mécanismes d'authentification forts qui permettront de sécuriser le mot de passe « classique », qui peut être copié, intercepté, donné, « craqué »... et qui n'offre donc qu'un niveau de sécurité limité.

On parle d'une authentification forte quand le mécanisme est basé sur au moins deux éléments parmi ce que vous savez (code PIN, par exemple), ce que vous avez (carte à puce, par exemple) et ce que vous êtes (élément biométrique comme une empreinte digitale, par exemple). L'implémentation d'un outil d'IAM (Identity and Access Management) permettra à l'entreprise de gérer les identités et les accès des utilisateurs aux applications comme au SI de façon centralisée.

Chaque utilisateur s'authentifie une fois, et son identité est alors distribuée dans toutes les applications informatiques de l'entreprise.

Une autre brique technique nous apparaît indispensable : le chiffrement.

Il constitue un autre moyen d'amener une entreprise à mettre en place une politique de sécurité répondant aux besoins de travail dans un contexte international. La méthode du chiffrement permet de protéger des fichiers, une partition ou la totalité d'un disque dur ou encore les communications numériques (messagerie, téléphonie) à l'aide de moyens cryptographiques [39].

(39) Cryptographie : branche des mathématiques qui s'occupe spécifiquement de protéger des messages.

Le chiffrement peut être efficace mais ne peut pas non plus être considéré comme le meilleur bastion pour la protection des données notamment lorsque l'on parle d'ingérence. La limite de cette mesure est justement due au respect des législations locales, certains pays (Chine, Iran, ...) interdisent tout mécanisme de chiffrement (ou exclusivement les mécanismes que les autorités du pays sont à même de déchiffrer) sur leur territoire national et ce pour tout type de support (disques, clés USB ...).

La politique de sécurité doit mentionner le chiffrement les données stratégiques par des algorithmes nationaux certifiés par l'ANSSI dans le cas de la France. Ceci est à mettre en parallèle avec l'hébergement des données dans un *cloud* souverain ou dans le *datacenter* de l'entreprise.

Il est un aspect de la sécurité des SI qui n'a pas été abordé jusqu'à présent dans ce développement et qui trouve cependant toute sa justification, c'est le *Plan de Reprise d'Activité* (PRA).

Un *Plan de Reprise d'Activité* doit permettre à l'entreprise un redémarrage d'activité à partir de données saines suite à une ingérence (intrusion, attaque destructrice,...).

Pour que le PRA soit efficient il est important qu'il n'échange pas de données de manière dynamique avec les infrastructures récurrentes et que l'intégrité des données transportées (supports bandes, disques ...) sur le site de PRA soit garantie.

La PSSI doit prévoir la réalisation régulière de tests de vulnérabilité et de conformité sur l'ensemble de ses infrastructures et applications ainsi qu'un suivi des plans de remédiation afin de détecter et corriger au plus tôt les failles de sécurité et de s'assurer du respect de la bonne application de la PSSI.

Ces tests de vulnérabilité s'inscrivent dans une démarche de contrôle continu du dispositif de l'entreprise. Ils permettent de contrôler la surface d'exposition de l'entreprise au sens large mais aussi dans chaque pays au sein duquel elle est présente et permet également d'être plus agile dans la réaction face à une menace. Les tests de vulnérabilité peuvent être commandités à une société tierce, de confiance et indépendante et avec laquelle les aspects contractuels devront être particulièrement soignés. Il est intéressant d'intégrer les équipes d'audit et de contrôle interne à la démarche quitte à les faire monter en compétence sur la composante sécurité et capitaliser sur le dispositif.

Enfin il est important pour chaque entreprise délivrant une nouvelle application ou service manipulant des données stratégiques qu'un test de vulnérabilité soit réalisé avant la mise en production du service. Il sera encore plus pertinent d'accompagner le projet tout au long de la démarche de mise en œuvre afin de garantir que les nouveaux besoins métier ne deviennent pas de nouvelles failles dans le dispositif de sécurité.

L'ensemble des mesures techniques décrites ci-dessus ne peut pas garantir une protection sans faille du système d'information. Les mesures organisationnelles préconisées viennent compléter le dispositif global que les auteurs de cette étude recommandent de mettre en œuvre dans les entreprises exposées au risque de l'ingérence des législations étrangères.

Le principal atout d'un dispositif de sécurité efficace sera son agilité, entendons par là, d'une part la capacité à décloisonner les responsabilités trop souvent organisées en silo (informatique, juridique, achats, métiers...) et sa maturité, qui ne pourra être obtenue que par un processus d'amélioration continue.

Au cœur du système, il apparaît bien que l'humain est un des facteurs de risque élevé pour le maintien du niveau de sécurité des SI – 80% du risque SSI se situe en interne, entre la chaise et le clavier entendons-nous dire fréquemment.

Parce que l'humain est diagnostiqué comme le maillon faible du système sécurité global, les actions de communication et de sensibilisation prennent alors toutes leurs dimensions, nous en avons déjà débattu.

Un focus particulier devra être fait auprès des dirigeants pour expliquer l'impact possible de l'ingérence sur la stratégie de l'entreprise et la nécessité de faire évoluer la politique de sécurité en conséquence.

L'utilisateur en tant que maillon faible sera la cible première des attaquants qui essaieront de pénétrer le réseau par leur intermédiaire. Un utilisateur averti comprenant les risques sera plus à même de détecter et informer d'une attaque.

La compréhension des enjeux et fondements de la sécurité et l'association avec les intérêts personnels sont des d'éléments clés pour une sensibilisation réussie. Elle ne doit pas uniquement faire des recommandations mais expliquer la raison en démontrant par l'exemple.

CONCLUSION

Les auteurs de ce document ont mis l'accent sur l'existence et les effets de l'ingérence des législations étrangères sur la politique de sécurité des entreprises. Si, de prime abord, il pourrait sembler que le combat est perdu d'avance et que les moyens qui s'offrent à l'entreprise sont illusoires face à l'implacable volonté de domination des États ou l'incroyable essor de la cybercriminalité, des solutions existent bel et bien.

Comme nous l'avons souligné, la fonction « Sécurité » doit être identifiée dans l'entreprise, partagée avec chaque collaborateur et comprise de tous. C'est une démarche collégiale qui doit être mise en œuvre pour identifier les risques, définir les enjeux de sécurité, la politique de sécurité, ses indicateurs de suivi et l'amélioration continue du dispositif.

Si la limitation des effets de l'ingérence tient à la nature de l'organisation sécurité et de ses moyens opérationnels, elle s'appuie également sur les solutions techniques à disposition de l'entreprise. À travers l'étude de quelques cas d'usages, il nous paraît important d'insister sur la nécessaire vigilance concernant les aspects contractuels de nos prestations, la communication et sensibilisation des populations internes, la mobilité des collaborateurs, les solutions de chiffrement et d'authentification, l'usage du *cloud*, la résilience des infrastructures, complété des actions permanentes de surveillance et de veille.

Comme les auteurs du présent développement l'ont démontré, sur le plan juridique il existe bon nombre de solutions permettant de mettre en échec l'ingérence des législations étrangères sur les politiques de sécurité des SI des entreprises. Leur mise en œuvre est toutefois bien souvent soumise à des impératifs économiques, qui l'emportent sur l'application des principes de droit.

La mauvaise connaissance des problématiques liées à la sécurité des systèmes d'information, tant au niveau gouvernemental, administratif que judiciaire ne rend pas cette tâche aisée au niveau de l'entreprise, qui bien souvent se trouve démunie et dépourvue d'assistance efficace lorsqu'elle décide de se refuser à subir des exigences déraisonnables de ses partenaires, fournisseurs ou clients.

L'appareil judiciaire et administratif doit impérativement opérer une évolution pour se mettre à « l'heure de l'internet », sans quoi la mise en place d'une politique de sécurité au niveau international restera toujours bancale, voire illusoire.

Face au relatif attentisme des autorités – tant nationales qu'européennes ou internationales - concernant une solution globale à la problématique d'ingérence, les entreprises doivent se mobiliser pour assurer leur défense ; elles doivent l'envisager seules. Une plus grande coopération des acteurs de la sécurité au sein des différentes entreprises est un magnifique vivier d'échange et d'enrichissement pour s'inspirer des retours d'expérience de chacun afin de se protéger au mieux des nouvelles menaces, y compris celles liées à l'ingérence des législations étrangères.

ÉCOLE MILITAIRE
1 place Joffre
Case 39
75700 PARIS 07 SP
Tél.: 33 (0)1 76 64 89 00 – Télécopie : 33 (0)1 76 64 89 27
www.inhesj.fr