BULLETIN DU DROIT DES SECRETS D'AFFAIRES

BSA

TRIMESTRE 3
07
Juin 2017

« Dire le secret d'un autre est une trahison, dire le sien est une sottise » Voltaire.

Sommaire

EDITORIAL

Secret des affaires et sécurité numérique: des enjeux communs

Par **Olivier de MAISON ROUGE**
Avocat, Docteur en droit.

Il s'agit à la fois de protéger des données sensibles – touchant par exemple aux domaines des communications électroniques, de l'énergie, ou des innovations industrielles stratégiques – et de veiller à la sécurité économique des entreprises ou institutions concernées par le traitement de ces données.
Jean-Baptiste CARPENTIER, CISSE, in DGE et vous, n°18 – Avril 2016

Rarement il aura été donné de se satisfaire d'une telle unité de temps et de lieu. En effet, grâce aux effets combinés de plusieurs textes européens adoptés en moins de 3 mois au printemps 2016 (« le printemps des données »), il a été forgé un socle unifié du droit de la donnée. Car l'élément central du droit de l'information qualifiée – en ce qu'elle renseigne l'acteur économique de manière à lui permettre de se positionner sur son environnement concurrentiel – demeure bel et bien la donnée comme matériau de base.

D'ailleurs, voici une décennie, Jean-Pierre JOUYET et Maurice LEVY ne s'y trompaient pas en avançant dès 2006 :
« Aujourd'hui, la véritable richesse n'est pas concrète, elle est abstraite. Elle n'est pas matérielle, elle est immatérielle. C'est désormais la capacité à innover, à créer des concepts et à produire des idées qui est devenue l'avantage compétitif essentiel. Au capital matériel a succédé, dans les critères essentiels de dynamisme économique, le capital immatériel ou, pour le dire autrement, le capital des talents, de la connaissance, du savoir. » [1]

Or, ces informations étant par nature immatérielles, elles sont de nos jours concentrées sur des supports numériques. Dès lors, à l'heure où la protection de la vie privée est une réponse à l'intrusion, on assiste à une convergence organiques des modes opératoires cybersécurité / protection des données personnelles / protection des secrets d'affaires.

Voici les 3 textes fondateurs de ce nouveau droit de la donnée que sont le RGPD, la directive sur la protection du secret des affaires et la directive NIS, où l'UE a pris soin de protéger toutes les données, qu'elles soient personnelles ou sensibles, d'une part, et leur support numérique, d'autre part.

Sauf sur le secret des affaires (cf. BSA #6), la France n'a pas été en retard dans ces domaines. Elle a même été pionnière.

C'est pourquoi, dans ce nouveau BSA, nous entendons apporter un éclairage sur les éléments de sécurité numérique de la donnée, autrement dit la cybersécurité, devenue à la mode, mais au-delà un enjeu vital, où données personnelles et données stratégiques de l'entreprises sont les deux faces d'une même pièce, elle-même gouvernée par des règles de sécurité numérique ■

[1] LEVY Maurice et JOUYET Jean-Pierre, *L'économie de l'immatériel: la croissance de demain* Rapport, Décembre 2006

REGARDS CROISÉS

La cybercriminalité, criminalité du XXIème siècle

P.2

VEILLE

Rappel des textes européens en matière de cybersécurité

P.5

A LA BARRE

Le secret professionnel dans tous ses états

P.5

INSTITUT DE L'IE
Institut international d'intelligence économique et stratégique
International Institute for competitive and strategic intelligence
www.institut-ie.fr

LA CYBERCRIMINALITE, CRIMINALITE DU XXIE SIECLE

Par le général (2S) Marc WATIN-AUGOUARD

Fondateur du FIC (Forum International de la Cybersécurité)

A un ministre de l'intérieur qui, il y a une quinzaine d'années, se félicitait de la baisse de la délinquance, un de ses conseillers répondit : « elle ne diminue pas, elle s'évapore ». Belle illusion d'optique, en effet, que celle des chiffres officiels de la criminalité et de la délinquance ! Ils sont l'agrégat des plaintes des victimes et des constatations d'initiative des gendarmes et policiers. Mais, dans l'espace numérique, les victimes sont-elles conscientes de l'être, souhaitent-elles véritablement déposer plainte ? Connaît-on le « chiffre noir », celui des infractions commises mais non révélées ? Les enquêteurs sont-ils assez nombreux pour mener toutes les investigations nécessaires ?

Oui, la criminalité s'évapore pour se métamorphoser en cybercriminalité ! Le moteur de cette mutation est l'intelligence du prédateur qu'il ne faut jamais sous-estimer : depuis l'origine de l'humanité, il cherche à optimiser le profit par rapport au risque pénal. Chaque étape de l'évolution de la structure économique de la société a été marquée par une dominante : le secteur primaire a été celui des atteintes aux personnes (meurtre, assassinat, viols, esclavage, etc.). Avec le développement du secteur secondaire, l'artisanat puis l'industrie ont favorisé les atteintes aux biens (vols, recels, dégradations). Le développement du secteur tertiaire a été, quant à lui, propice à la délinquance en « col blanc » (escroqueries, faux, blanchiment, etc.). Chaque fois, le prédateur a procédé à des arbitrages pour « gagner plus en risquant moins ».

L'émergence du secteur quaternaire, le secteur lié au « tout numérique », n'échappe pas à ce glissement. Le délinquant comprend que, grâce au « réseau des réseaux », il n'a jamais été aussi près de sa victime et aussi loin de son « juge ». Il est devant nous, sur nous, dans nous (par ex., au travers d'un pacemaker connecté), mais il peut agir de très loin, depuis un Etat « cyber voyou » peu enclin à la coopération policière et judiciaire. Que craindre d'un vol à main armée dans une agence bancaire qui rapportera au mieux quelques centaines d'euros comparé à une escroquerie sur internet, à un ransomware qui peuvent se solder par plusieurs centaines de milliers d'euros ? Dans le premier cas, les assises et la réclusion criminelle ; dans le second, un risque infime d'être arrêté, faute d'avoir pu remonter à temps la filière.

Cette « tectonique des plaques » est encore peu perceptible. Bien que la prise de conscience semble gagner toutes les couches de la société, la transformation numérique, dont on ne mesure pas assez la vitesse et l'ampleur, va radicalement changer notre vie durant la prochaine décennie. Il faut donc s'y préparer et s'organiser pour faire face aux enjeux. Pour cela, il faut d'abord une prise de conscience politique. Si l'Etat n'est plus en mesure d'assurer la sécurité des personnes physiques et morales et des biens, il perdra sa légitimité au regard de citoyens qui se tourneront vers d'autres régulateurs. Les organisations civiles et militaires doivent également épouser cette transformation, car il en va de leur survie. Combien d'entreprises sont déjà victimes de spoliateurs (escroqueries au « faux président », vols de données, d'éléments essentiels de leur propriété intellectuelle) et ont, pour certaines d'entre elles, subi un préjudice tel qu'elles ont cessé d'exister ?

Ce que recherche aujourd'hui le prédateur, c'est la donnée, matière vive de la transformation numérique : la donnée pour sa valeur, pour ce qu'elle représente, pour ce qu'elle permet de faire (données bancaires), pour le profit que l'on peut tirer lorsqu'elle est « prise en otage » par un chiffrement malveillant. Par cette donnée, il est possible de s'en prendre aux personnes, aux services et aux biens. La cybercriminalité a toujours un impact sur le monde réel.

Dans ce contexte, le prédateur a hélas ! un temps d'avance. Son imagination est plus prompte, sa réactivité plus forte, sa capacité d'adaptation plus aiguisée. Il est dans son temps, alors que les organisations tardent à sortir du XXe siècle. Tout simplement parce que les élites (déconnectées selon Laure Belot) n'ont pas le numérique dans leur « ADN », comme les générations montantes. La prise en compte au sein du COMEX de la stratégie de cybersécurité n'est pas encore partagée. Même s'il est, ici ou là, trop lent, un mouvement se dessine pourtant. En témoigne l'intérêt croissant que suscite le Forum international de la cybersécurité (FIC) chez les dirigeants des secteurs public et privés. En 2007, lors de sa création, cette manifestation suscitait de la curiosité. En 2017, plus de 7000 experts sont venus à Lille écouter notamment trois ministres, un commissaire européen, des acteurs centraux de la lutte contre la cybercriminalité et de la cyberdéfense.

Oui, il y a un frémissement, mais il est encore trop faible. La formation à la cybersécurité est aujourd'hui insuffisante, notamment au sein de l'université et des grandes écoles. Aucun diplôme ne devrait être homologué sans exiger qu'une partie du contenu lui soit consacrée, à hauteur des enjeux en cause. Est-il normal que de futurs cadres ayant la responsabilité de données à caractère personnel ou de données sensibles arrivent sur le marché de l'emploi, vierges de toute connaissance ad hoc ?
Les organisations doivent se restructurer pour augmenter leur résilience, leur aptitude à résister à une cyberattaque, à maintenir ou à reprendre leur activité en cas de sinistre cyber. Si elles veulent une cyber-assurance, elles devront respecter des normes, aujourd'hui imposées aux opérateurs d'importance vitale (OIV), mais dont les effets en cascade devraient agir sur tout le tissu économique.

Dans l'espace numérique, la sécurité est individuelle mais aussi collective. Pour atteindre un niveau optimal, le partenariat public-privé doit se développer, selon une dynamique et une profondeur inédites. Dans le « monde réel », l'Etat apporte une contribution majoritaire à l'offre de sécurité. Dans le cyberespace, les acteurs privés détiennent la plupart des réponses techniques ou organisationnelles. Parfois, ce sont des « hackers éthiques ».

La conjugaison de toutes les compétences est seule de nature à protéger et à défendre un espace numérique où acteurs étatiques, terroristes, mafieux, délinquants s'allient parfois contre nature mais pour servir leurs propres intérêts.

Pour lutter contre la cybercriminalité, il faut certes répondre à la question « comment ? » : comment mieux contrer un adversaire, comment attribuer une cyberattaque, comment y répondre par les voies judiciaires en mettant en œuvre une coopération internationale ? Mais il faut aussi répondre à la question « pourquoi ? », c'est-à-dire donner du sens. Nous ne maîtriserons pas la criminalité du XXIe siècle si nous ne « reformatons » pas la société, notamment autour de quelques valeurs : la confiance, la loyauté, la responsabilité, la solidarité.

2 Laure BELOT, *La déconnexion des élites,* Les Arènes, Ed.

LA PROTECTION NUMÉRIQUE DES DONNÉES PERSONNELLES

Par Myriam Quéméner, magistrat, docteur en droit

Expert en matière de lutte contre la cybercriminalité pour le Conseil de l'Europe, la Chancellerie et l'Ecole nationale de la magistrature (ENM)

Dernier ouvrage paru : Criminalité économique et financière à l'ère numérique (Economica, 2015)

La cybersécurité est aujourd'hui un véritable défi tant pour les individus que pour les entreprises qui évoluent dans le cyberespace et exercent aujourd'hui leurs activités dans un écosystème sans cesse davantage multiconnecté.

La sécurité des opérations, des transactions et des données critiques s'avère essentielle, à l'intérieur comme à l'extérieur de l'entreprise. La confiance est devenue le socle indispensable et le législateur tant national d'européen est venu renforcer[3] la protection des données personnelles. Ces instruments visent aussi bien les données personnelles des particuliers (I) que des entreprises (II).

I. La protection des données des particuliers

La sécurité numérique des données personnelles se renforce constamment soit par le recours à de nouvelles infractions comme l'usurpation d'identité en ligne créée par la Loppsi II (1) et par de nouveaux textes comme le règlement général sur la protection des données anticipé par la loi pour une République numérique(2).

1. La protection de l'identité numérique

Tout d'abord concernant les individus, il faut rappeler que la protection de l'identité numérique est une préoccupation grandissante. Ainsi l'usurpation d'identité en ligne est aujourd'hui facilitée par le recours aux réseaux sociaux et vise tant les particuliers que les entreprises ou les institutions.

L'article 226-4-1 du Code pénal vise « le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier », y compris « sur un réseau de communication au public en ligne ». La notion de « données de toute nature » s'entend non seulement du nom et du prénom, mais également de toute donnée susceptible de contenir des informations sur l'identité d'une personne, comme une adresse électronique, une adresse IP ou encore un identifiant / mot de passe. Les peines encourues sont d'un an d'emprisonnement et de 15.000 euros d'amende. S'agissant de l'élément intentionnel, l'infraction exige un dol spécial : l'usurpation doit être faite « en vue de troubler la tranquillité de la victime, ou de porter atteinte à son honneur ou à sa considération ».

De nombreuses applications de ce texte ont été faites par les juridictions. Par exemple, le tribunal de grande instance de Paris[4] a considéré qu'une jeune femme s'était rendue coupable, entre autres, d'usurpation d'identité par la création de « multiples profils sur les réseaux sociaux en utilisant les noms exacts ou modifiés ou encore le pseudonyme » de son ex-concubin et de son ex-amant notamment, ainsi que leurs photos. Ayant également employé des propos injurieux à leur égard, les juges ont estimé que l'élément intentionnel du délit d'usurpation d'identité était caractérisé. La cour d'appel de Paris a confirmé ce jugement par décision du 13 avril 2016[5].

Si l'usurpation d'identité numérique des citoyens a souvent pour but une vengeance personnelle, elle peut se traduire au sein des entreprise et des institutions, par des fraudes de plus grande ampleur comme par exemple les escroqueries au président qui sont le résultat de manipulations, usurpations d'identité et procédés d' ingénierie sociale .

2. L'évolution de la règlementation en matière de données personnelles

Le règlement général sur la protection[6] des données (RGPD) (Rég. UE 2016/679 du 27-4-2016) applicable à compter du 25 mai 2018 instaure une nouvelle règlementation européenne qui vise à enforcer la protection des données personnelles. Ce Règlement généralise l'obligation de notification des failles de sécurité visant les données à l'autorité de contrôle compétente[7] et impose une nouvelle obligation de communication aux personnes concernées par une violation de leurs données personnelles. Le RGPD remplace la directive sur la protection des données 95/46 / CE et est conçu pour soutenir le marché unique, harmoniser les lois sur la confidentialité des données en Europe, protéger et responsabiliser la confidentialité des données des citoyens de l'Union européenne (UE) et réorganiser la manière dont les organisations abordent la confidentialité des données pour les citoyens de l'UE partout où ils travaillent dans le monde.

Ces obligations s'appliquent à tous les responsables de traitement, c'est-à-dire à tout organisme qui « détermine les finalités et les moyens du traitement » (Art. 4, 7° du RGPD), et non plus seulement aux entreprises fournissant des services de communications électroniques, comme c'est le cas en France.

Le responsable du traitement doit notifier toute violation de données à caractère personnel à l'autorité de contrôle compétente dans les meilleurs délais en l'espèce à la CNIL[8], et si possible, 72 heures au plus tard après en avoir pris connaissance. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans ce délai, il convient de l'informer des motifs du retard.

Dans l'éventualité où le responsable du traitement ne remplirait pas cette obligation de notification des violations de données personnelles à la personne concernée, l'autorité de contrôle peut intervenir et exiger du responsable du traitement qu'il procède à cette communication.

La réforme européenne de la protection des données contribuera à renforcer la confiance des personnes dans les services en ligne, ce qui donnera un élan salutaire à la croissance, à l'emploi et à l'innovation dans l'Union européenne. Le règlement général de protection des données va mettre fin à la fragmentation juridique actuelle et à une grande partie des charges administratives.

Parmi les personnes concernées, les mineurs bénéficieront d'une protection accrue. Alors qu'ils ont tendance à rendre accessibles de nombreuses données à caractère personnel les concernant, ils disposent avec ce texte d'un « droit à l'oubli » renforcé. Il suffira qu'ils apportent la preuve de leur âge, au moment où ils ont mis en ligne un certain nombre d'informations. L'accès (transparence et guichet unique), la suppression (droit à l'oubli) ou encore le transfert (droit à la portabilité) de données par la personne concernée seront facilités. Les sanctions prévues sont également accrues en cas de non respect de ces droits.

La loi pour une République numérique du 7 octobre 2016 crée de nouveaux droits informatique et libertés et permet ainsi aux individus de mieux maîtriser leurs données personnelles. Elle renforce les pouvoirs de sanctions de la CNIL et lui confie de nouvelles missions.

Ce nouveau texte inscrit le droit à « l'autodétermination informationnelle réaffirmant ainsi que la personne est le centre de gravité de la législation sur la protection des données et renforce la maîtrise par celle -ci de ses données. Concrètement, la loi reconnait aux personnes la possibilité d'organiser le sort de ses données après la mort ;un droit à l'oubli renforcé pour les mineurs ;plus d'information et de transparence sur le traitement des données ;la possibilité d'exercer ses droits par voie électronique.

Elle contribue également à une meilleure ouverture des données publiques. Certaines

---

3 J-F Guédon , renforcement de la protection des données personnelles , AJ Pénal 2016 , p.53

4 TGI Paris, 21-11-2014, 24e ch. corr.n°10183000010

5 CA Paris, 13-4-2016

6 Le RGPD (ou GDPR) est le *Règlement Général pour la Protection des Données* (ou General Data Protection Regulation)

7 Article 33 du RGPD

8 https://www.cnil.fr

dispositions anticipent le règlement européen sur la protection des données personnelles applicable en mai 2018.

II. La protection des données des entreprises : une démarche européenne

1. Le règlement « eIDAS »

Le règlement eIDAS, en application depuis le 1er juillet 2016, instaure un cadre européen en matière d'identification électronique et de services de confiance. Dorénavant, les règles qui définissent l'identité numérique sont claires et reconnues entre les États membres de l'Union européenne.
Le Règlement « eIDAS » n°910/2014 du 23 juillet 2014 a pour ambition d'accroître la confiance dans les transactions électroniques au sein du marché intérieur. Il établit un socle commun pour les interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques. Le règlement eIDAS concerne principalement les organismes du secteur public et les prestataires de services de confiance établis sur le territoire de l'Union européenne. Il instaure un cadre européen en matière d'identification électronique et de services de confiance, afin de faciliter l'émergence du marché unique numérique.
Le règlement eIDAS est essentiellement consacré à l'identification électronique et aux services de confiance. Il traite également, dans une moindre mesure, des documents électroniques en leur accordant un effet juridique.
L'Agence nationale de sécurité des systèmes d'information[9] (ANSSI) intervient dans l'application du règlement comme garante de la sécurité pour le volet « identification électronique » et comme organe de contrôle pour le volet « services de confiance ».

2. La directive NIS

Adopté le 16 juillet 2016 par le parlement européen, la directive NIS (Network and Information Security) devra être transposé au plus tard le 9 mai 2018. Elle prévoit que les opérateurs de services ainsi que les places de marché en ligne, les moteurs de recherche et les services Cloud seront soumis à des exigences de sécurité et de notification d'incidents.
Cette directive est destinée à assurer un « niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne ». Les « opérateurs de services essentiels » et certains fournisseurs de services numériques seront bien soumis à des exigences de sécurité et de notification d'incidents de sécurité.
L'ANSSI développe des recommandations en matière de cybersécurité comme par exemple dans le domaine de l'Internet des objets. Ces préconisations sont fondamentales pour éviter les vulnérabilités élémentaires régulièrement constatées dans les objets, mais également pour rappeler qu'il est indispensable de bien définir les exigences de sécurité et de résilience attendus pour le service rendu par ces objets pour déployer au bon niveau les mesures de sécurité appropriées.

Perspectives

La protection des données personnelles doit aujourd'hui être une priorité essentielle pour les Etats et c'est ce qu'à bien compris la commission européenne en annonçant très récemment une campagne d'information sur ce sujet[10].Cependant, un savant équilibre doit être trouvé entre cette nécessaire protection mais aussi la nécessité de pouvoir accéder à des données qui constituent aussi des éléments de preuve numérique utiles en particulier dans le cadre d'enquêtes pénales.

La Commission européenne va collaborer étroitement avec les États membres, les autorités nationales de protection des données et les parties prenantes afin que ces règles soient uniformément appliquées dans l'ensemble de l'UE. Par ailleurs, les citoyens doivent connaître leurs droits et savoir comment les défendre lorsqu'ils estiment que leurs droits ne sont pas respectés.

[9] www.ssi.gouv.fr

[10] http://www.euractiv.fr/section/justice-affaires-interieures/news/jourova-i-will-launch-a-massive-information-campaign-on-data-protection

VEILLE

Rappel exhaustif des textes européens en matière de cybersécurité, objet du présent dossier :

- La directive 2013/40 relative aux attaques contre les systèmes d'information ;
Le règlement 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance :
- La directive 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ;
- Le règlement 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ;
- La directive 2016/1148 du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (NIS).

La cybersécurité au rapport

Dans son rapport annuel pour 2015, l'ANSSI (agence nationale de la sécurité des systèmes d'information) a fait état pour la première fois publiquement de ses activités et recensé les atteintes dont les systèmes d'informations ont été victimes en France. Il ressort que plus de 4 000 signalements ont été enregistrés sur la période (en hausse de 50%), 2 300 codes malveillants constatés et une vingtaine d'attaques majeures relevant majoritairement de l'espionnage économique http://www.ssi.gouv.fr/administration/actualite/rapport-dactivite-de-lanssi-2015-une-annee-charniere-pour-la-concretisation-des-actions-engagees/

L'agence rappelle également sa mission essentielle auprès des OIV (opérateurs d'importance vitale, prévus par la loi de programmation militaire), lesquels sont tenus d'assurer un niveau optimum de sécurité, avec le soutien et les conseils des 460 agents de l'ANSSI (600 prévus en 2018) https://www.lenouveleconomiste.fr/lesdossiers/cybersecurite-la-protection-imposee-des-oiv-32155/

Par décret n°2016-66 du 29 janvier 2016, pris en Conseil des ministres du 27 janvier 2016, il a été mis fin à la Délégation interministérielle à l'intelligence économique (D2IE) et il a été créé un Service à l'information stratégique et à la sécurité économiques (SISSE) avec à sa tête un commissaire.

Ledit Commissaire élabore et propose, en lien avec le SGDSN et les autres ministères concernés, la politique publique en matière de protection et de promotion des intérêts économiques, industriels et scientifiques de la Nation. Il en anime la mise en œuvre et en évalue l'efficacité, conformément aux orientations définies par le comité directeur du service de l'information stratégique et de la sécurité économiques.

A ce titre, il est associé à la définition et à la mise en œuvre, par chaque ministère concerné, des politiques publiques ayant une influence directe sur les intérêts mentionnés au premier alinéa, notamment dans les domaines suivants : (…)

3°° La défense de la souveraineté numérique ;

A LA BARRE

De la stricte confidentialité

Deux récentes affaires démontrent la fermeté des juridictions quant au respect des obligations de confidentialité (ce qui n'est pas sans mettre en exergue une certaine asymétrie voire une schizophrénie au vu des décisions recensées dans le post ci-dessus).

• Dans le premier cas, une société commerciale avait confié à un prestataire la refonte de son site d'e-commerce. Le contrat de réalisation de prestations de conception, hébergement et maintenance intégrait une clause de confidentialité, imposant au webdesigner une obligation de non-divulgation de certaines informations liées à cette mission. Ayant opéré un changement d'hébergeur en cours d'exécution du contrat, le Tribunal de commerce de Paris a estimé qu'il y avait eu violation de l'obligation de confidentialité.

T. com Paris, 15 févr. 2016, Destock Mubles / Blue Acacia

• Dans une autre espèce, relevant de la matière pénale cette fois, un inspecteur des impôts avait avisé un contribuable d'éléments de son dossier relatifs à la vérification opérée par un autre inspecteur du service sur ce même contribuable. En d'autres termes, l'inspecteur avait révélé des informations qui étaient couvertes par le secret professionnel. En conséquence, il a été condamné pour ce motif.

Cass. Crim., 1er mars 2016, n°14-87577

Le secret professionnel dans tous ses états

Obligation inhérente à toute fonction et/ou activité économique, le secret professionnel est en principe rigoureusement imposé par certaines catégories professionnelles obligées « par état » (avocats, activités médicales, ministre du culte).

http://www.institut-ie.fr/bsa/BSA_02_12_2012.pdf

Elle est rendue nécessaire à raison de la protection de la connaissance de l'intimité d'une personne qui se dévoile à l'égard d'un professionnel (aveux, confession, état médical, …).

En réalité, ce qu'il convient davantage de dénommer « confidentialité » professionnelle, tend désormais à couvrir un large champ d'application, eu égard aux informations connues au sein de la structure, ce qui rejoint la préoccupation majeure menée à travers nos travaux d'étude sur la protection des données de l'entreprise.

Ainsi, parmi quelques extensions récentes, nous relevons :

- L'obligation de discrétion en ligne d'un agent public : le fait, pour un policier, de révéler des informations relatives aux services où il exerce ses fonctions justifie un licenciement pour faute (CE, 3e et 8e ch., 2 mars 2017).

- De même, un fonctionnaire de police ne peut se retrancher derrière le droit à la liberté d'expression pour avoir frauduleusement consulté le ficher des infractions pénales (STIC), à des fins personnelles (CE, 31 mars 2017).

- La confidentialité des correspondances entre avocats couvre également les pièces et annexes joints aux courriers échangés (CA Aix-en-Provence, 25 avr. 2017).

- Le Conseil constitutionnel a validé les obligations de secret entourant les fonctions de défenseur syndical en matière prud'homale et les sanctions attachées, prévues par l'article L 1453-8 du Code du travail (Cons. constit., 7

avr. 2017, n°2017-623 QPC).

- Le nouveau Code de déontologie de l'Inspection du travail a notamment introduit des obligations de confidentialité pesant sur les inspecteurs du travail à raison des secrets de fabrication et procédés d'exploitation dont ils ont connaissance dans l'exercice de leur mission (Décret 2017-541 du 12 avril 2017).

- Enfin, le nouveau Code de déontologie de la profession de Commissaire aux comptes enferme (et reprend) les mêmes astreintes de secret et de discrétion, en dehors des cas d'alerte prévus par la Loi (Décret 2017-540 du 12 avril 2017).

Vol de document par un salarié : il faut l'élément intentionnel

En l'espèce, un salarié d'un célèbre joaillier, designer en orfèvrerie, avait conservé par devers lui, après son départ de l'entreprise, un ensemble de créations graphiques de son ex employeur.

Ce dernier avait porté plainte pour vol et abus de confiance, sur les bases légales et jurisprudentielles désormais établies s'agissant de l'obtention et du détournement illicite d'informations de l'entreprise http://demaisonrouge-avocat.com/2015/01/13/lespionnage-economique-encore-et-toujours-reprime-par-labus-de-confiance/ / http://www.institut-ie.fr/bsa/BSA_00_03_2012.pdf

Ayant été relaxé par la Cour d'appel, la partie civile formait alors un pourvoi en cassation. Ayant relevé que la société n'avait pas institué en interne de référentiel spécifique rappelant aux salariés l'interdiction de sortir les documents de l'entreprise, ou pouvant lui permettre de rappeler son droit de propriété sur les créations de salariés, le pourvoi a été rejeté au motif que *« le prévenu a pu se croire propriétaire des dessins qu'il avait lui-même signés et qu'il n'est pas établi qu'il ait utilisé à des fins différentes de celles pour lesquelles ils lui avaient été remis »*.

D'où la nécessité impérieuse de se doter d'un politique interne de sécurité du patrimoine informationnel.

Cass. Crim., 23 mars 2016, n°14-88357

Nous relevons ici une étonnante décision, de 2015, de la Cour de cassation, établissant une confidentialité plutôt extensive du secret professionnel de l'expert-comptable, à laquelle la première chambre civile ne nous avait pas habitués.

En l'occurrence, le litige initial portait sur la démonstration à faire de la volonté d'une partie à l'instance de céder son fonds de commerce, ce que réfutait le commerçant (du moins son mandant). Pour attester de l'intention de vendre du cédant qui s'était rétracté, l'acquéreur produisait un courrier adressé par le vendeur à son expert-comptable faisant état de sa volonté de céder son commerce.

Ce courrier avait vraisemblablement été obtenu auprès de l'expert-comptable par le cessionnaire.

Ce faisant, la Cour a estimé que l'expert-comptable avait trahi la confiance de son client et avait violé le secret professionnel auquel il était astreint, énonçant que *« quel que soit l'objet de la mission dont il est chargé par contrat, l'expert-comptable est tenu à un secret professionnel relativement aux faits qu'il n'a pu connaître qu'en raison de la profession qu'il exerce »*.

Cass. Civ. 1ère, 10 sept. 2015, n°14-22699

Enfin, en matière industrielle et commerciale, la CJUE a estimé pour sa part que l'accès à l'information (des populations) devait primer sur le secret industriel. Il s'agissait d'une demande communication sur des pesticides, formulée par les associations écologistes. La Cour a précisé que la notion «d'émissions dans l'environnement» couvre *«le rejet dans l'environnement de produits ou de substances, tels que les produits phytopharmaceutiques ou biocides et les substances que ces produits contiennent, pour autant que ce rejet soit effectif ou prévisible dans des conditions normales ou réalistes d'utilisation»*.

CJUE, 23 novembre 2016 Aff. C 442/14 et C 673/13

Secret des affaires et marchés publics

Nous avons déjà été amené à commenter la règlementation et la jurisprudence de la CADA relatives à la communication des pièces du dossier d'adjudications dans le cadre des appels d'offres, tel que cela ressort de nos études et de nos ouvrages.

La loi du 17 juillet 1978 fait à ce titre de la Commission le garant de la préservation des secrets industriels et commerciaux des entreprises dans le cadre de la passation du marché. Il lui appartient de juger de la pertinence des demandes de communication formulées par les entreprises mises en concurrence, puis écartées de l'attribution du marché public.

En l'espèce, le Conseil d'Etat a estimé que la CADA avait jugé à bon droit que *« si notamment l'acte d'engagement, le prix global de l'offre et les prestations proposées par l'entreprise attributaire sont en principe communicables, le bordereau unitaire de prix de l'entreprise attributaire, en ce qu'il reflète la stratégie commerciale de l'entreprise opérant dans un secteur d'activité, n'est quant à lui, en principe, pas communicable »*.

CE, 30 mars 2016, n°375529

Sur la base de ce même principe, à nouveau réaffirmé, en dépit du fait qu'une entreprise puisse être déclarée comme étant en situation de monopole ou de quasi-monopole, ses rivaux ne peuvent pas avoir accès aux informations communiquées dans le cadre de la procédure d'infraction aux règles de libre concurrence.

L'affaire visait à annuler une décision de refus de transmission de l'ARFEP (autorité de régulation des télécoms) d'offres techniques locales d'Orange que souhaitaient se faire communiquer d'autres opérateurs.

CE, 10e et 9e ch., 21 avr. 2017

La captation de savoir-faire : un acte de parasitisme

La directive européenne n°2016/943 du 8 juin 2016 relative à la protection des savoirs-faires et des secrets d'affaires n'a pas bouleversé les voies de recours précédemment empruntées pour sanctionner civilement les actes illégitimes de captation des savoir-faire d'une entreprise concurrente (bien que s'étant largement inspiré de la propriété intellectuelle, la réparation civile repose toujours sur l'action en concurrence déloyale).

Cette affaire illustre de quelle manière les tribunaux apprécient dans les faits ces agissements déloyaux :

En l'espèce, une entreprise rivale avait débauché 5 salariés outre un ingénieur, lesquels constituaient le service de R&D de son concurrent. Il s'est avéré que cette opération a eu pour effet de s'attribuer, à moindre frais, les savoirs développés chez un tiers.

En vertu du principe de réparation intégrale, eu égard au sommes investies sur ce projet pour la victime des actes parasitaires, celle-ci s'est vue attribuer une somme de 750 000 € de dommages et intérêts.

Cass. Com. 8 nov. 2016, n°15-14.437

S'agissant du secret professionnel, la cour de cassation a rappelé qu'une mesure *in futurum* prononcée sur le fondement de l'article 145 du Code de procédure civile ne pouvait se heurter au secret des affaires, d'une part, mais devait

néanmoins exclure des saisies opérées les correspondances échangées entre un avocat et son client.

Cass. Civ 1e, 3 nov. 2016, n°15-20.495

L'abus de confiance, toujours et encore motif de sanction pénale de divulgation de données confidentielles

« constitue un abus de confiance le fait, pour une personne, qui a été destinataire, en tant que salariée d'une société, d'informations relatives à la clientèle de celle-ci, de les utiliser par des procédés déloyaux dans le but d'attirer une partie de cette clientèle vers une autre société ».

Cette décision confirmant une fois encore le recours au droit pénal général pour protéger notamment le secret des affaires et sanctionner le délit de révélation et/ou utilisation frauduleuse.
En l'espèce, les juges sont allés assez loin dans l'interprétation du texte en caractérisant le détournement d'une clientèle.

Cass. Crim., 22 mars 2017, n°15-85.929

LU, VU ET ENTENDU

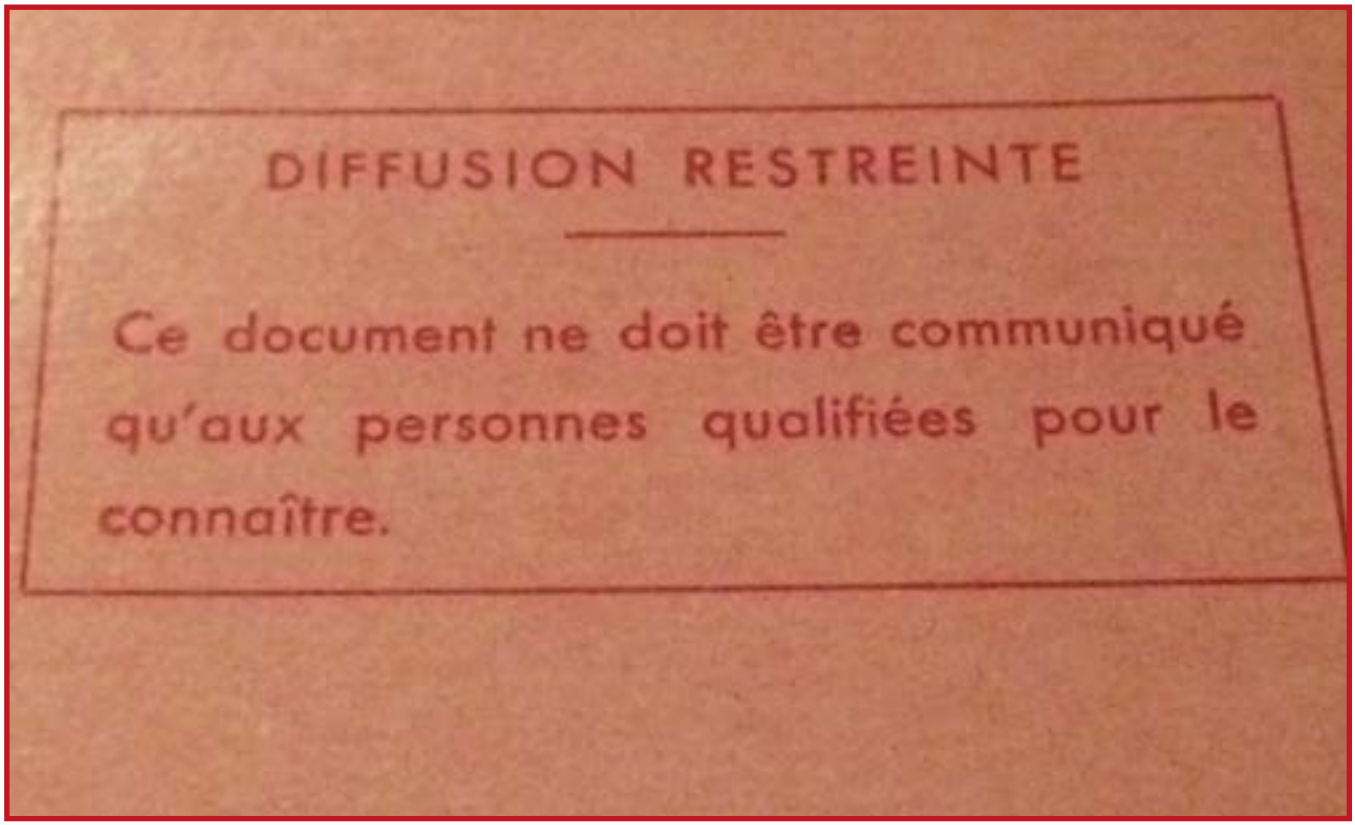
Dans le même esprit, en application de la Loi de programmation militaire (LPM), une première série d'arrêtés a été rendus en vue de déterminer les Opérateurs d'Importance Vitale (OIV), lesquels doivent se soumettre désormais à des règles de sécurité informatique drastiques. Le but recherché, avec le concours de l'ANSSI, est de protéger les sites et davantage encore les activités sensibles du potentiel économique et scientifique de la France en cas d'atteinte extérieure (voire intérieure au vu les temps actuels) et plus précisément assurer le bon fonctionnement des services essentiels en cas de crise http://www.ssi.gouv.fr/entreprise/protection-des-oiv/protection-des-oiv-en-france/
La règlementation adoptée le 1er juillet 2016 identifie 250 métiers susceptibles de répondre aux critères d'exigence retenus, en matière notamment de santé, eau, énergie et alimentation.

Il en est ainsi dans le dossier de la DCNS (constructeur naval de la marine militaire) relatif au sous-marin Scorpène, modèle vendu récemment à l'Inde.

Il apparait que 22.400 fichiers – non couverts par le secret de la défense nationale faut-il cependant le préciser – ont été transférés frauduleusement. Cette fuite – qui est un comble pour un submersible – se serait produite à l'occasion des négociations exclusives suite à un appel d'offres, avec l'Australie. Serait-ce un acte de malveillance pour gêner la conclusion d'une commande historique ?

BRIBES ET CHUCHOTEMENTS

Par ailleurs, le Secrétariat général de la défense et de la sécurité nationale (SGDSN) a rendu son premier rapport public d'activité pour l'année 2015, cette année ayant été marquée tant par l'adoption des lois renseignement (juillet et novembre) mais encore par de nombreux attentats terroristes :
A lire avec attention également le rapport de la délégation parlementaire au renseignement pour l'année 2016, qui aborde la question du renseignement économique et le rôle du SISSE.

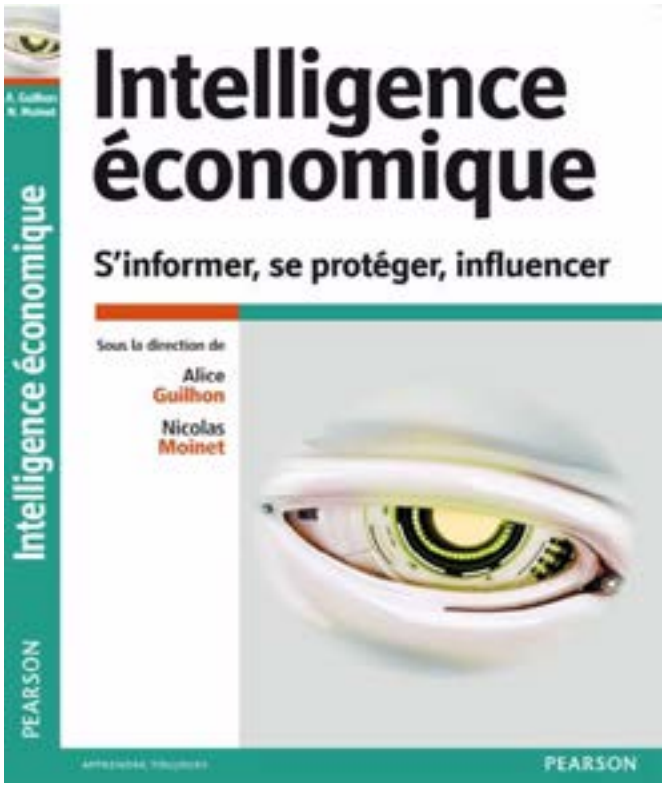


PUBLICATIONS

INTELLIGENCE ÉCONOMIQUE :
S'INFORMER, SE PROTÉGER, INFLUENCER

http://www.skema-bs.fr/actualite-skema/edition-intelligence-economique-s-informer-se-proteger-influencer

Sous la direction de Alice Guilhon, Directrice Générale de SKEMA, et Nicolas Moinet, IAE-Université de Poitiers, et paru aux Editions Pearson



Bulletin d'abonnement

Merci de nous renvoyer ce coupon réponse dûement complété

Nom Prénom

Société

Adresse

Code Postal Pays

Tél. Mob.

Courriel

☐ Je m'abonne au BSA pour l'année civile, pour 4 numéros trimstriels, à compter du numéro 1

Réglement de 100 € à envoyer par chèque à l'ordre de D²

D² - data x digital
5 rue Bonnabaud
63 000 Clermont-Ferrand

BSA

BULLETIN DU DROIT DES SECRETS D'AFFAIRES

Une publication de

INSTITUT DE L'IE
Institut international d'intelligence économique et stratégique
International Institute for competitive and strategic intelligence
www.institut-ie.fr

Editeur :
D² - data x digital
5 rue Bonnabaud,
63 000 Clermont-Ferrand

Conception :
EG communication
www.eg-communication.fr

Directeur de Publication :
Thomas Janier

Responsable de la rédaction :
Olivier de Maison Rouge

Prix : 25,00 €

Dépôt légal à parution

Date de parution : juin 2017

ISSN : 2259-3624

BSA