Secret des affaires et données sensibles.

5 mars 2017 à 15 heures © PMF & HdA 2017

Rédacteur : Ph. Muller Feuga, Ancien Responsable de la Mission Protection du secret (MPS/HFDS/SGDSN), Ancien Auditeur au Contrôle général économique et financier des Ministères économique et financier, Membre du Groupe de travail sur le rôle des territoires non coopératifs dans la déstabilisation de la finance mondiale.

Dispositif de protection de nos entreprises et « intérêts stratégiques » : protection et utilisation des données « sensibles ». Identification et data.

« No Court in this land will allow a person to keep an advantage he has obtained by fraud. No judgment of a court, no order of a Minister, can be allowed to stand if it has been obtained by fraud. Fraud unravels everything. »1 Lord Denning, Lazarus Estates Ltd v Beasley (1956).

Le cyberespace poursuit son expansion portée par les progrès technologiques qui participent à la digitalisation de nos sociétés (sous l'influence des e-clouds computing, clouds hybrides, capteurs, parcs de terminaux, etc.), à la multiplicité des flottes de mobiles ou terminaux nomades (type BOYD[2]) et à l'interconnexion des réseaux IT (Information Technology). Ce mouvement est encouragé par la multiplication des applications accessibles aux individus ou développées dans les entreprises et les administrations. Simultanément, les cyberattaques tout comme les actions de cybercriminels (black hats ou script kiddies) sont des menaces identifiées, sans pouvoir être identifiables compte tenu des vulnérabilités des systèmes d'information (SI) basculant vers une économie de plateformes. De cette dynamique digitale, en partie animée par les échanges d'informations ou de données, les hackers ne manquent ni d'imagination, ni de maîtrise des outils. Ils recherchent la faille ou les fragilités, développent des systèmes de fraudes, d'abus ou d'escroqueries (ou cyberfraudes)[3] à partir de la réalité virtuelle ou fictive appelée l'e-economie, non sans user ou abuser de l'open data ou de la dématérialisation des échanges, notamment avec les administrations (ou e-administration). De nombreuses implications peuvent créer des dysfonctionnements ou des « dégâts collatéraux » tant dans le périmètre de la Défense qui développe des « systèmes de systèmes » ou travaille sur des « security by design » (cyberdéfense) que dans celui du civil avec l'Intérieur (cybersécurité).

Côté acteurs du marché qui retiendra notre attention, le risque dépend de l'intégration du cyberespace dans la stratégie de croissance des entreprises. D'une architecture fermée, sans lien avec l'Internet (net), installée au sein d'un établissement, d'un site industriel (type SCADA) ou commercial, ces SI évoluent sous l'effet de la concurrence

vers une interconnexion croissante. Cette évolution est souvent difficilement maitrisable, notamment par le DSI, dans les différentes couches basses ou hautes des systèmes. L'Internet permet une connectivité fiable et accroît l'efficacité et la flexibilité des acteurs économiques, donc leur compétitivité. L'interdépendance déployée sur les clouds invente de nouveaux usages, et accélère la transformation digitale qui porte vers l'entreprise cognitive assurée par l'innovation collaborative et par l'Infrastructure as a Service (IaaS) ; elle optimise serveurs et connections réseaux, bande passante, adresses IP, etc. C'est une « agilité » qui augmente considérablement l'exposition aux cyberattaques. Car la majorité des infrastructures IT conçues pour l'instantanéité n'a pas toujours été pensée dans une logique d'ouverture sécurisée. Toute personne, physique ou morale, se trouve à la tête d'un « patrimoine informationnel » croissant, des plus variés (données personnelles – dont identitaires type sécurité sociale SSN ou numéro INSEE, et e-santé, techniques, financières, commerciales, etc.), désormais comptabilisé dans le haut du bilan, Il est source de convoitises en tant qu'actifs par nature virtuelle, susceptibles de captation ou de modifications, voire de fraudes en tout genre.

Expansion du cyber et sécurité des données asymétrique

- A partir des systèmes automatisés gérés par les langages d'ordinateurs (Fortran, Cobol, etc.) apparus dès la fin des années 1950, un monde nouveau se construit avec le développement de l'informatique et des grands systèmes centralisés d'informations que les administrations veulent se doter. Ils ont les avantages offerts par tout traitement de données. Cette première phase de l'Information Age est non sans risques, soit étatiques dans la vision d'Orwell avec 1984 et la prophétie de Big Brother, soit individuels. Ces derniers sont d'abord anodins, objets de canulars d'étudiants, coupables de « félonies » et de fraudes marginales ou auteurs de tests pour « se mesurer » avec les nouvelles technologies et pour contourner les premières mesures de sécurité informatiques qui apparaissent. Mais l'interconnectivité des SI s'accélère au début des années 1980 et conduit à trois types d'actes répréhensibles : les copies illégales, souvent meilleures que l'original interpellant la propriété intellectuelle ; l'intrusion frauduleuse ou non autorisée, parfois en vue de modifications de programmes internes[4] aux conséquences difficilement mesurables ; et la malveillance relevant de la criminalité[5] sous forme de fraudes ou d'abus. La notion de cybercrime se caractérise par les tentatives de fraudes, de vols, voire d'abus de confiance ou de biens sociaux, comme sur le réseau Swift de la Citybank avec Vladimir Levin (1994), de détournement de données confidentielles avec Kevin Mitnick (1995)[6], à une échelle plus ou moins réduite au détriment de services sociaux.

- Très naturellement, sans grande connaissance des systèmes, les législations[7] se renforcent sous l'angle de la fraude intentionnelle avec l'adoption aux Etats-Unis du Comprehensive Crime Control Act qui ouvre la voie au Counterfeit Access Device and Computer Fraud and Abuse Act (1984), suivi de l'US Computer Fraud and Abuse Act (CFAA) en 1986 visant la fraude à la carte bancaire[8] et la protection des systèmes informatiques (computer systems) ; au Royaume Uni avec le Computer Misuse Act (1990), régulièrement amendé. En Europe, concernant la protection de données « sensibles » par les communications électroniques, la vigilance existe, mais reste limiter aux « données personnelles » sous l'angle de leurs traitements automatisés. La directive 95/46/CE au niveau communautaire, la Convention n°108 pour la protection des données personnelles du Conseil de l'Europe ou une déclaration du Conseil des ministres du Conseil de l'Europe de 1997 y font référence. Cette approche est confirmée au sommet de Toronto (octobre 1998) où s'exprime la volonté d'assurer une protection des données à caractère personnel[9] dans le cadre de la libre circulation des fichiers entre Etats, comme ceux des clients européens d'entreprises multinationales d'origine américaine ou ceux des cadres de leurs filiales installées en Europe (American Express, IBM, etc.), mais sans réels effets. En fait, la volonté de libérer les marchés était dominante, ignorante des risques potentiels émanant de l'évasion fiscale, du crime organisé ou du terrorisme.
- Suite à l'éclatement de la bulle de l'Internet (mars 2000) née de la dérèglementation des marchés de télécommunications et à leur conversion au numérique (NTIC), l'explosion du e-commerce dès les années 2000, l'utilisation croissante de smartphones ou de terminaux personnels concomitant à la connectivité croissante des objets (Internet des objets, IoT) et à l'intelligence artificielle (IA) participent à nourrir le Big Data : celui-ci est issu des marchés grâce aux principaux systèmes d'exploitation (Apple, Microsoft et l'Android de Google) avec la constitution de grands acteurs américains comme les GAFA ou Big Five. Leurs offres de services multiples sont d'autant plus concurrentes de ceux des opérateurs traditionnels que les réseaux wi-fi transforment ces offres en véritables commodities[10] payées selon l'usage fait, fonction des ressources de calcul puissantes. Pour la première fois dans l'histoire économique, un système de production par le biais des infrastructures informatiques industrielles crée des chaînes de valeur sans cesse en expansion : d'un monde fini et malthusien modélisé par le Club de Rome (1972), la dynamique du monde numérique crée des ressources virtuelles inépuisables avec pour unité de base la data. Elle participe ainsi à l'expansion du cyberespace face auquel l'Etat régalien semble démuni, incapable d'assurer sa souveraineté numérique,

dépassé par les capacités des « géants du Net » à un moment où la fin de l'Histoire (1989 - 1991) consacre la métamorphose du Foreign Intelligence Surveillance Act (FISA) de 1978[11] sous la présidence Clinton, puis sous celle de George W. Bush suite aux attentats du 11 septembre 2001, le premier à des fins de guerre commerciale (ou unfair compétition), le second dans la lutte contre le terrorisme. Pour ce combat, l'accès aux données personnelles devient un enjeu illustré par la bataille diplomatique autour du PNR (Passenger Name Record) entre 2001 et 2012[12].

- Les réticences européennes s'effacent surtout devant la montée en puissance des risques liés au terrorisme tandis que la crise financière de 2008 oriente les priorités d'abord vers la lutte contre le blanchiment d'argent et l'évasion fiscale (2009-2011), puis vers la sécurité physique et logique des SI (cybersécurité). En France et dans l'Union européenne, cette sécurité est abordée sous l'angle de la défense et de la sécurité nationale (2008-2013). La data devient un enjeu, mais celui-ci varie selon qu'il s'agisse d'un traitement gouvernemental de fichiers (notamment à des fins fiscales), ou selon qu'elle est captée par les acteurs du secteur privé (à des fins marketing). Les tensions entre l'UE et les EU demeurent, et s'expliquent largement par cette double asymétrie : l'Union européenne, comme chacun des Etats membres ont sous-estimé l'importance de cette nouvelle ressource (valorisée par les technologies de data mining), et ont occulté un angle de sa sécurité, se focalisant essentiellement sur la seule partie « régalienne » reconnue, limitée aux données personnelles. A l'inverse, les Etats-Unis qui, adeptes du soft power, captent et stockent une grande partie du Big Data sur leur territoire dans les data centers accentuent leur « surveillance de masse ». Assurés de la coopération des Big Five, ils agissent tous azimuts en extra-territorialisant leur droit grâce à un arsenal juridique puissant (procédure judiciaire Discovery, Cohen Act ou dispositifs Itar/Ear ou Ofac), souvent issu de la guerre froide (CoCom), tant en matière de lutte contre le terrorisme qu'envers les pays potentiellement détenteurs d'armes à destruction massive. Contrairement à l'Union européenne qui, faute d'être détentrice d'une réelle souveraineté, a privilégié l'ouverture des marchés au détriment du contrôle des investissements étrangers dans ses « intérêts stratégiques » au point de n'avoir que récemment (2013) réévalué la protection de ses informations classifiées (ICUE)[13], aux Etats-Unis la dichotomie entre défense et sécurité n'existe pas. Le « secret défense » y est inconnu ; les « intérêts fondamentaux » de la nation relèvent du Department of Homeland Security (DHS) créé en 2002 avec une gestion stricte du « secret » ou du « top secret », et une déclinaison précise du « classified », du « sensitive », du « restricted » ou du « unauthorized access », conciliant la donnée avec

l'accréditation de la personne selon son emploi et ayant « le besoin » d'en connaître (selon une échelle clairement établie[14]).

Sécurité de la data et identification dans le cyberespace

- Par négligence de la dimension extérieure dans la construction européenne, l'Union européenne a perdu la bataille des infrastructures dominées par les Etats-Unis, et même si les Chinois essaient de se placer avec China Telecom, ZTE, Huawei sur le marché des smartphones et des data centers liés à leur puissance de calcul (marquée par l'envoi de Mozi ou Quess, premier satellite quantique le 16 août 2016, effet classique d'une propagande marxiste à l'image de Sputnik en octobre 1957). Mais la transformation digitale concentre l'attention sur l'expansion exponentielle du Big Data et devrait conduire à recenser les actifs informationnels qui participent à la croissance d'une entreprise. Ces actifs par nature virtuelle ou immatérielle ne se limitent pas aux seuls éléments relevant des codes de la propriété intellectuelle, comme le laisse penser la directive sur le secret d'affaires (avril 2016), bien trop restrictive, se limitant à la définition de l'Accord de Marrakech (ou ADPIC) annexé à la Convention signée le 14 avril 1994, dix ans avant l'expansion du cyberespace. Le numérique bouscule notre droit et les dispositifs existants qui reposent sur des caractérisations conformes à l'économie industrielle (telle la nature de l'acte de captation d'informations à caractère confidentiel). L'adaptation aux réalités digitales reste lente, un « gap culturel » s'installant auprès des professionnels de la Justice, voire auprès des responsables politiques. L'existence de la dichotomie défense/sécurité dans les « vieux » pays régaliens s'oppose à la vision américaine sur les biens ou services à double usage (civil et militaire) plus conforme à la digitalisation de nos sociétés. Ainsi, les éléments constitutifs de l'atteinte aux « intérêts stratégiques » de la nation posent la question du passage de la sphère privée dominée par la libre concurrence sur le marché à un « intérêt général » légalement protégé, notamment par le code pénal. Ainsi, le caractère « stratégique », voire « essentiel » ou « fondamental » d'une donnée, d'un engagement ou d'une information (data) appartient-il strictement au domaine de la défense, ou dans une approche relevant davantage de l'Information Age repose-t-il sur le risque de mettre en danger des éléments importants du potentiel économique de la nation ? Dans le nouveau contexte de « guerre économique mondiale » (ou « unfair competition »), la captation, le détournement ou le vol de données ne prennent pas les mêmes formes que jadis ; autrement dit, restreindre l'espionnage, même « industriel », aux seules affaires militaires comme au temps de la guerre froide relève d'une dissonance cognitive qui s'explique par notre organisation administrative qui fait l'impasse

sur l'évolution de la recherche, le caractère dual de nos activités, voire sur l'intelligence économique. Cette dissonance minimise la valeur de la data : « dans le système de la défensive pour assurer la sauvegarde de nos frontières »[15], elle porte la protection comme une nouvelle ligne Maginot numérique vers les systèmes d'information en leur imposant des référentiels rédigés par l'ANSSI/SGDSN plutôt que vers la valeur de la data et les moyens de son identification.

- La protection des données personnelles introduit toutefois une méthodologie qui pourrait être retenue pour les autres actifs informationnels. En raison d'une protection inférieure à celle accordée par l'Union européenne aux données personnelles par les États-Unis où les étrangers ne bénéficient pas de la loi sur la protection de la vie privée (Privacy Act, 1974), Washington a passé un Safe Harbor arrangement ou « sphère de sécurité » avec l'UE (en 2001 sur la base de la directive 95/46 d'octobre 1995) pour se mettre en conformité avec les directives européennes sur la protection des données personnelles (19 données). Cet accord a été invalidé par la Cour de justice européenne ou CJUE (30 mai 2006)[16] qui reproche à la Commission de ne pas s'être assurée de leur bon niveau de protection aux Etats-Unis. Les révélations dans le Guardian et le Washington Post (6 juin 2013) du « lanceur d'alerte » Edward Snowden sur l'usage des programmes de surveillance de masse par la National Security Agency (NSA) et le FBI, comme PRISM, et celles des écoutes dont feraient l'objet la chancelière Angela Merkel, soulignent l'importance des articles 702 (écoute de personnes non américaines hors du territoire américain) et au §1881a (vise les services cloud computing) du FISA cité ci-dessus.
  Les conditions d'identification de la donnée et son traitement invente une méthodologie qui a attiré l'attention du Parlement européen[17]. Son rapport montre l'approche asymétrique des Etats-Unis à l'égard de la protection de leurs citoyens respectifs, et la plainte déposée par l'autrichien Maximillian Schrems (octobre 2015) contre la société américaine Facebook a conduit sa filiale en Irlande18 à se soumettre à la législation européenne. Tout comme pour plus de 4.000 entreprises américaines, dont celles installées dans la Silicon Valley, il s'agit désormais de respecter le cadre d'utilisation des données personnelles de citoyens européens dans leurs démarches commerciales, ou la gestion de leur personnel. Comme quoi l'Union européenne, il est vrai par la CJUE et non par la Commission, peut également imposer ses règles dans la protection de la data, définies dans les dernières directives Privacy Shield ou le RGDP applicable en mai 2018, et peut extra-territorialiser son droit. Un parallèle n'est-il pas à établir entre ce cadre réglementaire sur les données personnelles, « actif sensible », et celui sur la protection des autres données « sensibles »

relatives à la collecte d'informations, personnelles ou non, par ou sur les entreprises européennes, notamment les plus « stratégiques » ?

- La data (ou information) quelle que soit son contenu et donc sa valeur intrinsèque est créée, collectée et « exploitée » par les algorithmes de plus en plus complexes développés par ces géants de la toile (web) dans sa partie référencée, mais aussi dans la partie non indexée (dark web) pour toute sorte de trafic, d'activités illégales, voire criminelles (cybercriminalité) comme la recherche d'informations (deep web) avec les risques de manipulations, d'utilisations frauduleuses, d'informations fictives (fake news) ou de falsifications à grande échelle. Ce qui pose la question des liens entre, d'une part, l'identification autour des concepts de l'authenticité, de l'intégrité, de la confidentialité, de la traçabilité et, d'autre part, de la protection et de la sécurité de l'information ou data dans le cyberespace, notamment en termes d'accès autorisé ou non. Ici, sphère du privé et le régalien se rejoignent pour participer à la définition d'une politique publique en la matière, avec pour vecteur de certification la « smart blockchain ».
  La montée des réseaux sociaux et de l'utilisation croissante des smartphones ou terminaux à des fins professionnelles ou privées (BOYD) complique cette approche dans l'alternative privacy versus security, mais les technologies du numérique en constante évolution apportent des réponses utiles au régalien. Toute data (donnée ou information) engendrée se rattache à une personne physique, ne serait-ce que par le premier « clic » de la souris (hors IA, encore que celle-ci ne peut être qu'initiée par une personne physique même dans un processus long et complexe). La protection de ladite donnée, personnelle ou non, peut donc être rattachée à l'existence d'un éventuel « consentement » (explicite ou non ?) dans leur utilisation (ce qui a contrario peut définir un « vol » ou une « substitution » ou une « subtilisation », avec des sanctions pénales[19]).
  Or, de tels éléments constitutifs de la data peuvent être tracés et conservés si le SI le permet ou si leur traçabilité a été programmée : avec le numérique, ces éléments prennent des formes nouvelles, particulièrement encadrées pour le traitement des données personnelles. La législation nationale (loi Informatique et libertés de 1978, modifiée en 2005), transposée au niveau européen avec le RGDP à partir de mai 2018, conduit pour tout actif informationnel à être protégé de toute intrusion frauduleuse[20], détournement, soustraction, copie hors usage personnel[21], etc.
  La gestion de ces données fait apparaître une nouvelle fonction au sein des administrations, comme au sein des entreprises avec le Chief Data Officer (CDO) ou le Data Management Officer (DMO), au rôle parfois limité à la seule

gestion des données personnelles (CIL ou futur DPO). Ces responsables doivent s'inscrire dans l'organigramme de l'entité et être chargés d'assurer les éléments constitutifs de son patrimoine informationnel dont il a la charge, ainsi que sa sécurité selon son degré de sensibilité en lien avec le DSI et le DRH.

- Cette démarche se réalise en amont de la naissance d'une data : elle s'appuie sur le respect d'une succession de compliances, sur l'établissement de cartographies des risques, etc., mais aussi sur la sensibilisation du personnel, sur la rédaction des contrats et annexes de sécurité. Il revient ainsi à l'entreprise de connaître la valeur de ses actifs, de les protéger selon qu'il relève du « secret des affaires » ou d'autres secrets ou confidentialités selon les trois dispositifs existants en France (IGI n° 1300, PPST et SAIV avec les PIV) pour pouvoir caractériser toute atteinte à une information « protégée », le plus souvent conservée sous forme numérique ce qui pose la question de l'application des textes juridiques souvent décalés par rapport aux rapides évolutions de la réalité numérique.

  La sécurité des « informations sensibles » ou « stratégiques » dans le cyberespace ne peut pas relever que des services de l'Etat, organisés en statuts et en « silos », selon le principe du top down, souvent décalés de ces évolutions technologiques et surtout de l'existence de ces data et de leur localisation. Rares sont en France les services, au croisement du public et du privé, capables de conduire une politique publique de protection de l'information et d'appréhender la question en un partenariat « gagnant-gagnant » comme la DGFiP ou la DGCCRF (concurrence et répression de la fraude), et hors du périmètre de la Défense (avec la DGA et la DCNS) qui a su en partie structurer la gestion et la protection des « actifs informationnels ». Chaque data a son cycle de vie qui doit être appréhendé dans une approche bottom up par les « métiers » en fonction de sa finalité, et de l'importance de sa valeur pour l'entité. Or, les Etats européens se sont engagés essentiellement dans une cybersécurité défensive des contenants (SI) en éditant des référentiels et des mesures précises comme l'utilisation de protocoles de transfert sécurisés ou le chiffrement des données. Mais est-ce suffisant, alors que les craintes liées à l'utilisation abusive des données, au profilage ou à l'automatisation des décisions, ne font que s'amplifier menaçants nos « intérêts » économiques ?

Conclusion

Une approche uniquement technique ne peut porter ses fruits ce qui exige une « rupture » culturelle. En ce qui concerne les données personnelles, le cadre est désormais bien établi pour répondre aux craintes engendrées sur le nécessaire respect de la vie privée dans les traitements à des fins mercantiles : rassurer les

individus en leur donnant l'assurance de ne pas croiser, exploiter ou échanger leurs données à leur insu et contre leur volonté ce qui est aujourd'hui le sens de la privacy pour les citoyens.
Mais seule une partie des data « sensibles » se trouve ainsi protégée, et tout un large pan d'actifs informationnels en principe couvert par le « secret des affaires » ne l'est pas. Selon la même méthodologie retenue pour les données personnelles, une seule question intéresse les entreprises, les administrations et toute autre entité tout en interpelant les autorités : quelles sont les informations « sensibles » ou « stratégiques » accessibles, et à qui ?
D'où une interrogation qui s'impose : quels sont les obstacles à résoudre pour assurer au mieux la défense et la sécurité de nos « intérêts stratégiques »22 ? quelles mesures à prendre dans la protection de nos données stratégiques, et comment les identifier ? et quelle est leur compatibilité avec les directives européennes ?

Notes et références

1 Lord Denning, *Lazarus Estates Ltd v Beasley* [1956] 1 QB. 702; [1956] 2 W.L.R. 502; [1956] 1 All ER. 341.

2 Dès 2012, une étude de la SSI ThreatMetrix évalue la pratique croissante du Boyd ou *Bring your own device*, càd *« apportez vos appareils personnels »*, source d'efficacité, de mobilité et de productivité pour l'entreprise. Selon Bearing Point & Forrester (ex KPMG Consulting), le DSI ignore le plus souvent leur usage réel par les deux-tiers des salariés, dont les cadres dirigeants afin d'accéder aux ressources de leur entreprise (à inscrire dans une charte éthique d'usage, annexe au contrat de salarié) faute d'un recensement et suivi du parc de terminaux utilisés par les salariés, et d'une gestion sérieuse des autorisations de connexions (MDoAM ou Mobile Device or Application Management).

La protection de la donnée se situe en amont des configurations de tout terminal (OS, messagerie, carte 3G USB, connection WiFi, etc.) et passe moins par le durcissement des réseaux ou des SI avec leurs terminaux que par la gestion des accès aux applications : c'est une approche multidimensionnelle de la sécurité dans l'écosystème digital (DEM, Digital Ecosystem Management).

3 Cf. *« Comment des hackers russes ont détourné des millions de dollars grâce à la fraude publicitaire »* (21 décembre 2016).

4 En 1981, avec Ian Murphy, alias *Captain Zero*, sur les SI d'AT&T.

5 Comme les virus *Brain* (janvier 1986) ou *Morris* (1988).

6 David S. Wall, *Cybercrime, thze transformation of Crime in the Information Age,* Polity Press, 2007).

7 La première législation est celle du *Land* de Hesse en Allemagne fédérale (*Das Hessische Datenschutzgesetz*, octobre 1970, *in* Alexander Genz: *Datenschutz in Europa und den USA.* Deutscher Universitäts-Verlag. Wiesbaden 2004), puis en Suède (1976). En janvier 1974, les Etats-Unis adoptent le *Privacy Act* limité aux fichiers détenus par l'Administration fédérale et prévoient un droit d'accès pour les citoyens. n France, le débat est amorcé : *« Dans quelques années le citoyen sera totalement incapable de contrôler l'utilisation pratique et généralisée des renseignements fournis par le matériel informatique »* (Michel Poniatowski, proposition de loi tendant à la création d'un Comité de surveillance et d'un Tribunal de l'informatique, AN, 30 octobre 1970. Annexe au procès-verbal de la séance du 25 novembre 1970, n° 1454). Le projet 'élaboration est dévoilé en 1974 (*Le Monde*, 21 mars 1974 intitulé : *« S.A.F.A.R.I. ou la chasse aux Français »*) : système prévoyant l'institution d'un identifiant unique (n° sécurité sociale) pour interconnecter les fichiers publics, acronyme de Système automatisé pour les fichiers administratifs et le répertoire des individus, c'est-à-dire une base de données centralisée de la population en utilisant le fichier INSEE de numéros de sécurité sociale comme identifiant commun à tous les fichiers administratifs. Devant le refus, ceci conduit à la création d'une commission *Informatique et liberté* chargée de proposer une réglementation sur l'utilisation des moyens informatiques pour mettre en place un garde-fou contre les abus de l'informatique, *via* l'institution d'une autorité administrative de contrôle indépendante grâce à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

8 https://www.the-parallax.com/2016/03/16/where-did-the-cfaa-come-from-and-where-is-it-going/

9 Assurer la protection *« contre la trop grande curiosité d'entreprises et de pouvoirs publics »* conformément aux *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel »* (OCDE, 1980).

10 *« For all the talk of computing as a utility, it seems that the motto 'You get what you pay for' applies as much to infrastructure-as-aservice (IaaS) as it does to any other commodity. The computing you get for Amazon's low prices may not be as cost-effective as that of other providers, depending on what you're using it for. »* http://diginomica.com/2013/08/14/iaas-provider-offers-cloud-bargain/

11 Le FISA encadre les procédures des surveillances physiques et électroniques de collecte d'informations (SIGINT) à l'étranger sous le contrôle de sept, puis de onze juges de la Cour fédérale *United States Foreign Intelligence Surveillance Court* (FISC ou FISA Court) dont les interprétations, dans le respect du 4éme amendement de la Constitution des Etats-Unis, restent classifiées pendant trente ans. Le *Patriot Act* de 2001 l'a renforcée, l'amendement de 2008 l'a étendue jusqu'à fin 2017.

12 Présentée en 2011 par la Commission européenne, la directive est votée en avril 2016 par le Parlement européen.

13 Décision du Conseil du 23 septembre 2013 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne (2013/488/UE).

14 Appelées *« security clearances »* relevant des agences ou départements ministériels comme le Department of Defense (DoD) qui en

concentre 80%, le Department of Homeland Security (DHS), le Department of Energy (DoE), le Department of Justice (DoJ), la National

Security Agency (NSA), la Central Intelligence Agency (CIA).

15 Cf. l'ouvrage *« Défense des frontières, Haut Commandement- Gouvernement 1919-1939*, par Paul Émile Tournoux, Nouvelles Editions

Latines, Paris, 1939.

16 Les États-Unis tentent alors de passer des MoU bilatéraux avec la République tchèque, le Royaume-Uni, l'Estonie, l'Allemagne et la

Grèce (2008).

17 *« Rapport Fighting Cyber Crime and protecting privacy in the cloud »*, Parlement européen, octobre 2012. Les auteurs montrent que tout fournisseur de services de *cloud computing* coupable d'avoir averti les autorités européennes sur l'existence de dispositif de surveillance de masse est passible d'outrage à la Cour fédérale relative au renseignement étranger (FISA Court) et serait sous le coup de la loi *Espionage Act* (1917) interdisant toute publication d'informations classifiées, dont celles sur les méthodes de renseignement. Cette loi, ainsi que le *Patriot Act* (2001) peuvent s'appliquer *« secrètement »* à toute entreprise étrangère à partir du moment où elle a une activité commerciale sur le sol américain.

18 Dans un premier temps, la Haute Cour de Justice irlandaise a demandé à la Cour de justice de l'Union Européenne (CJUE) si elle pouvait mandater une autorité nationale de contrôle pour enquêter sur un cas pareil vis-à-vis d'un pays tiers. La CJUE a déclaré que les autorités nationales ont les pouvoirs intacts dans ce domaine, ce qui donnait le feu vert à la justice irlandaise pour enquêter auprès des Etats-Unis. En vérifiant la décision, la Cour de Justice a constaté que la Commission n'avait pas fait le nécessaire pour s'assurer que les Etats-Unis respectaient effectivement un niveau de protection des droits fondamentaux des internautes équivalent à celui de l'UE (la réglementation américaine permet aux autorités d'accéder *« au contenu de communications électroniques »*, ceci étant une atteinte aux droits fondamentaux en Europe).

19 Cf. les arrêts suivants : Cass. crim., 9 sept. 2003, n°02-87.098 ; Cass. Crim., 4 mars 2008, n°07-84.002 ; Cass. Crim., 16 juin 2011, n°10-85.079), la Chambre criminelle de la Cour de cassation a consacré le *« vol »* immatériel, par soustraction de données informatiques sans le consentement de son propriétaire, voire en matière de condamnation pour *« espionnage économique »* in Trib. Corr. Clermont- Ferrand, 26 sept. 2011 avec la démonstration de Me Olivier de Maison Rouge. Cf. également Cass. Crim, 20 mai 2015, n°14-81336. Une exclusion dans cette qualification, le strict cadre de la défense prud'homale : la Cour de cassation a rappelé que ce n'est pas à l'employeur de démontrer que le salarié a téléchargé davantage que pour les besoins de sa cause, mais c'est bien au salarié de prouver que ce transfert était limité strictement au soutien de son argumentation (Cass soc., 31 mars 2015, n°13-24410).

20 A démontrer techniquement, pour des raisons indépendantes de la volonté de l'hacker (défaillance pour cause de d'erreur matérielle de paramétrage du serveur hébergeant l'extranet de l'entité), il peut se rendre sur le site, sans contourner ou *« casser »* un quelconque filtre informatique (code d'accès utilisateur, droits de l'administrateur et mot de passe inopérants au moment des faits).

21 Cf. GI Créteil, 11ème ch. Corr, 23 avril 2013 « *puisque ces données, élément immatériel, demeuraient disponibles et accessibles à tous sur le serveur, ne peut constituer l'élément matériel du vol, la soustraction frauduleuse de la chose d'autrui, délit supposant, pour être constitué, l'appréhension d'une chose* ».

22 Le substantif retenu doit être décliné selon qu'il s'agit d'intérêts *« fondamentaux »*, *« vitaux »*, *« stratégiques »*, *« sensibles »*, *« essentiels »* ou de *« l'intérêt général »* qui vise à la satisfaction des premiers, mais s'inscrit dans une approche à moyen ou long terme. Dans le Livre IV du Code pénal consacré aux crimes et délits contre la Nation, l'Etat et la Paix publique, *« les intérêts fondamentaux de la nation »* s'entendent d'une manière générale *«de son indépendance, de l'intégrité de son territoire, de sa sécurité, de la forme républicaine de ses institutions, des moyens de sa défense et de sa diplomatie, de la sauvegarde de sa population en France et à l'étranger, de l'équilibre de son milieu naturel et de son environnement et des éléments essentiels de son potentiel scientifique et économique et de son patrimoine culturel »* (art. 410-1). Sur la nécessité de préserver ou de défendre de tels *« intérêts »* de la France, cf. différents textes comme la décision n° 2006-543 DC du Conseil constitutionnel relative au secteur de l'énergie, et notamment la continuité et la sécurité d'approvisionnement en énergie (loi relative au secteur de l'énergie) ; celle n° 2011-192 répondant à une QPC sur le secret défense ; ou encore l'avis n° 08-A05 du Conseil de la concurrence (du 18 avril 2008) relatif au projet de réforme du système français de régulation de la concurrence et au contrôle concurrentiel des concentrations *« dans un secteur sensible justifiant un droit de regard de l'Etat au nom d'intérêts fondamentaux tels que la défense nationale et la sécurité publique ».*