efcse.eu

Penser la guerre économique : data is digital (III)

Auteur : Philippe MUELLER FEUGA, Expert

Ancien Responsable de la Mission Protection du secret (MPS/HFDS/SGDSN), et Auditeur au Contrôle général économique et financier des Ministères économique et financier (ER), Membre du Groupe de travail sur le rôle des territoires non coopératifs dans la déstabilisation de la finance mondiale. Membre du Working Group EFCSE - Gouvernance de l'information. Secrétaire général du Club des officiers de sécurité (ClOS).

8 Juin 2018

Quels outils ou quelle stratégie de puissance pour une Union européenne à étrangeté constitutive ?

L'acte final de la nouvelle directive européenne sur « la protection des secrets d'affaires » en tant que « protection des savoir-faire et des informations commerciales non divulgués »i a été votée le 8 juin 2016. Protection strictement a minima reprenant les termes de l'accord sur les droits de propriété intellectuelle (ADPIC) passé dans le cadre du Traité de Marrakech avec l'OMC (1994), elle est le résultat d'un travail « consensuel » en vue d'une réglementation unique et cohérente visant à harmoniser les règles applicables entre tous les Etats membres de l'Union européenne (UE), mais éloignées du contexte numérique où fondamentalement data is digital. Mais pour quels résultats, et avec quelle stratégie face aux « hors limites » ?

Le déni des réalités européen

Ce texte doit impérativement être transposé par la France (au plus tard le 9 juin 2018). Mais sa transposition est une opportunité pour favoriser l'émergence d'un dispositif de protection du « secret » (comprendre de « la confidentialité »). Il doit dépasser la notion de « savoir-faire » et être élargi à tous les actifs informationnels de haut de bilan – non éligibles à la protection du Code de la défense et du Code de la propriété intellectuelle (CPI) – des entreprises partie prenante de nos « intérêts stratégiques »ii. Le recours à l'art. 346 (TFUE) souligne le problème croissant de la primauté du droit européen sur les droits internes des Etats membres. A contrario, ce recours n'aurait plus de sens si l'UE adoptait des mesures nécessaires « à la protection des intérêts essentiels de sa sécurité et qui se rapportent à la production ou au commerce d'armes, de munitions et de matériel de guerre ». Ou tout simplement à la protection de ses « intérêts essentiels » relevant d'une « sécurité nationale », éminemment de nature « régalienne » ou « souveraine ».

Opportunité pour entériner dans l'UE une rupture avec les dispositifs actuels ad hoc hérités d'une approche « en silos » reposant sur l'exception, éloignés d'un renforcement stratégique de puissance pour l'UE, notamment en matière de gestion de l'information. L'exception défense définie par l'art. 346 (TFUE) souligne la double faiblesse européenne à surmonter : à défaut d'une « sécurité nationale » transposée au niveau européen, c'est une protection du « secret » trop limitative au « secret défense », et une conception de la sécurité ou de la défense trop « nationale » pour un marché intérieur régi selon le principe de libre-circulation. Cette conception doit être élargie « avec agilité » aux activités « sensibles » utiles à la sécurité européenne, comprise comme une « sécurité nationale » au même titre que les autres grandes puissances. Une sorte de

« mix national defense » (mix ou dual, civil et militaire) capable de forger une indépendance stratégique et de construire une cyberdéfense protégeant notre capital informationnel. Les outils existent, et sont nombreux, mais nécessitent une orientation stratégique ferme par une autorité renouvelée comme le SGDSN.

La transformation digitale justifie cette rupture pour mieux garantir les « intérêts stratégiques » d'un Etat dont les acteurs économiques sont soumis à une concurrence déloyale (unfair competition) ayant pour cible ou comme moyen l'information (ou data). La protection de l'information comprise aux Etats-Unis est au cœur du débat. L'UE ayant perdu la bataille des infrastructures (l'Internet), la question n'est pas le seul durcissement des systèmes d'information (SI) comme l'imposent les agences nationales telles l'ANSSI ou l'ENISA (agence européenne chargée de la sécurité des réseaux et de l'information) sous forme de référentiels ou dans le cadre de la LPM (art. 22 de la loi de programmation militaire, 2014-2019), ni d'améliorer la résilience de ces réseaux. Il s'agit d'assurer désormais la sécurité des actifs informationnels « confidentiels » en tant que « secret » sans qu'il soit « défense » contre l'idéologie de l'open data. Ou de transparence forcenée. Le « secret » est une source de progrès et d'innovations, mais doit associer les acteurs du secteur privé dans un partenariat d'égal à égal avec les autorités. Le cyberespace – reconnu comme le cinquième territoire de confrontations ou de compétition – modifie la sécurité d'activités gérées en réseaux, qu'elles soient le fait d'opérateurs civils « d'importance vitale » ou relevant des armées à capacités de combat by design conçues en systèmes de systèmes (programme Scorpion) pour une hyper-connectivité du combattant sur les champs de bataille. La collecte, le stockage, l'échange, le traitement et la transformation de grands volumes d'informations de toute nature et de tout format (du big data au data lake), associés à l'intelligence artificielle (IA), sont des processus technologiques d'une « sécurité nationale » devenue « cyber ». La gestion de la complexité croissante des systèmes d'équipements, du savoir-faire et de la compétitivité des entreprises des secteurs ou sous-secteurs « critiques » – utilisant des « biens » nécessairement à finalité duale ou à double usage (BDU) – sont de la responsabilité de leurs dirigeants ou Comex, mais dépend de l'engagement des pouvoirs publics dans l'établissement du cadre réglementaire – telles les directives nationales de sécurité (DNS) – et en tant qu'acheteurs ou régulateurs principaux.

A l'ère de la digitalisation (Digital Age), les entreprises confrontées à leur production mondialisée refusent tout autant une ouverture illimitée des données (open data) qu'une protection du « secret » ou du « confidentiel » par la construction d'une ligne Maginot numérique (sorte de Great Firewall chinois) sanctuarisant leur écosystème de confiance à bâtir. Or, celui-ci se compose à terme de l'ensemble de leurs clients ou fournisseurs sécurisés (dont la sous-traitance) partageant des actifs « confidentiels », participant à la « sécurité nationale » et aux « intérêts stratégiques » d'un « Etat », fut-il l'Union européenne. Un Etat de droit capable de légiférer sur un espace défini, capable d'exercer ses compétences souveraines et de défendre ses acteurs économiques. Capable d'édifier une « autonomie stratégique » grâce à la cyberdéfense, l'intelligence économique, au smart power (basée sur la maitrise des data et de leurs flux) et à la cyber-dissuasion (incluant la cyber-résilience et la cyberwarfare, reconnue en France en 2017) par le renforcement de la puissance technologique… Ce que l'UE n'a pas réussi à réaliser tout en hésitant sur la « neutralité du net » qui définit le marché de la data. Celui-ci repose sur trois piliers : l'utilisateur du web communiquant de données, certaines étant confidentielles ou « secrètes » ; l'éditeur de contenu et de services en échange de données personnelles ; et l'annonceur ciblant ces données afin de mener des campagnes marketing. Aux Etats-Unis, l'abrogation de la « neutralité du net » (2017) offre aux sociétés de télécommunications fournisseurs de services Internet entre l'internaute et les éditeurs (Google, Facebook, Twitter, etc.) un énorme avantage en tant qu'acteurs américains.

Autrement dit, l'UE qui conserve un temps de retard sur les Etats-Unis doit élever le concept de « sécurité nationale » à l'espace européen, et définir une stratégie de puissance en intégrant la dimension extérieure dans la construction du marché unique (intérieur). Mais elle bute sur l'existence de droits souverains, comme « l'idée constitutionnelle de la France »

(CC, Décision n° 2006-540 du 27 juillet 2006). Dans une logique de rupture, l'UE doit se ressaisir. Elle est conduite à défendre ses « intérêts économiques essentiels » et à les élargir au-delà du périmètre des activités de défense, non limitées à la seule « production ou au commerce d'armes, de munitions et de matériel de guerre ». Cette sécurité face au double enjeu digital conduit à la mise en œuvre d'écosystèmes de confiance, en tant que nouveaux « territoires » dans le cyberespace. Le cyberespace sera spatial et à câbles optiques, et un grand programme du type Starlink avec le consortium privé OneWeb (2018) après le succès de SpaceXiii est parfaitement concevable, porté par tous les Etats membres.

Pour un concept du « secret » européen de puissance souveraine porté par la « sécurité nationale »

Le frémissement observé depuis quelques mois marque-t-il un tournant dans l'approche européenne des souverainetés de ses Etats membres ? Le retour du régalien (hors plan fiscal ou de la concurrence anti-monopole visant les GAFA+M) est illustré par une série de textes adoptés depuis 2014 à consonance sécuritaire [le Règlement eIDAS n° 910/2014 sur la confiance dans les transactions électroniques ; la directive (UE) 2016/1148 sur la sécurité des réseaux et des systèmes d'information ou « directive NIS »], mais reste inachevé. Le règlement n° 2016/679 sur la protection des données personnelles (ou RGPD) modifie le rapport de force en créant une extra-territorialisation du droit européen. Signes d'une rupture avec la pratique étroite d'une sécurité nationale encore trop partielle, non coordonnée, source de vulnérabilités multiples. Et faute de pouvoir s'appuyer sur une intelligence économique offensive à l'opposé de ce qui est pratiqué par d'autres puissances (Etats-Unis, Chine). La directive (UE) 2016/943 sur « la protection des secrets d'affaires » à transposer avant le 9 juin 2018 reste décalée par rapport aux enjeux du cyberespace et aux menaces sur nos actifs informationnelsiv sous-estimées.

Par oubli ou abandon de la dimension extérieure dans le « projet européen » initial, les institutions européennes l'ont fragilisé car elles n'ont jamais défini ce que pourrait être une « indépendance ou autonomie stratégique », en partenariat avec le secteur privé. Le commissaire Michel Barnier chargé du Marché intérieur et des Services avait dans un premier temps critiqué l'article « discrétionnaire » 346 TFUE (mai 2011) sous prétexte d'intégrer les marchés européens des équipements de défense au sein du marché unique. En juillet 2013, face à un euroscepticisme croissant, les commissaires Michel Barnier et Antonio Tajani sont plus nuancés, et évoquent la nécessité d'avoir une base industrielle (BITDE) compétitive qui permette à la politique de sécurité et de défense commune de rester opérationnelle, dans un contexte budgétaire difficile. Simple constat qui confirme une tardive prise de conscience des menaces extérieures multiformes ou « hors limites ». Les domaines d'action restent nombreux mais doivent conduire à une prise de conscience et des décisions de sauvegarde (accord SWIFT, agence de crédit aux exportations européennes comparable à l'ExIm Bank américaine, etc., limitation des aides européennes aux sociétés non européennes, etc.), ainsi qu'une réflexion sur les conditions de gestion des informations de nos entreprises à mener en lien avec la pratique d'Euler-Hermès ou les greffes des tribunaux de commerce. Complété d'un dispositif inter-Etats membres comparable au CFIUS qui a une vision de la sécurité nationale plus globalev que dans l'UE où elle reste embryonnaire.

A défaut d'une sécurité de nature « nationale » ou souveraine pour l'UE, la France assure sa propre sécurité et son indépendance. Mais la sécurité nationale reste également parcellaire, concentrée sur la DGA (strictement défense, relevant toujours de l'Etat-nation souverain) en raison du parti pris « frileux » des DAJ (direction des affaires juridiques) ministérielles dans l'application des directives européennes et du risque d'interprétation restrictive par la Cour de Justice de l'UE (CJUE). Pourtant la seule à défendre le principe de la primauté du droit européen, primauté toute relative à la lecture de l'art. 346 (TFUE) transposé dans le nouvel espace numérique. Ce parti pris ne peut qu'affaiblir notre puissance technologique, à commencer sur le contrôle des investissements étrangers (procédure IEF). L'initiative prise par la France et l'Allemagne en

juillet 2017 accélère la prise de conscience au niveau européen, mais la perception du concept de « puissance » comme celui du « secret » n'a pas la même résonnance à Paris, à Berlin ou à Bruxelles.

Les organismes ou entités qui en assurent la tutelle (SGDSN et CNR) manquent d'autorité suite à la confusion née des Livres blancs de la défense et de la sécurité de 2008 et de 2013, au passage du SGDN au SGDSN (2009), à une incertitude sur le sort de l'intelligence économique (de la DIIE au SISSE) et au manque de propositions audacieuse dans les deux dernières Revues stratégiques (octobre 2017), dont celle de la cyberdéfense (février 2018). Le rapport Urvoas (2013) dénonçait déjà la mauvaise gestion des REF (renseignements économiques et financiers) par Bercy, plus précisément par la direction générale du Trésor (DGT). Pourtant les techniques de contrôle ou de protection ne manquent pas, mais la question du suivi des engagements reste posée. Des initiatives régaliennes sont heureuses, conformes au concept d'autonomie stratégique appliquée à la « data sensible ». Mais certains éléments propres au pays (statuts, carriérismes, rétention d'information) empêchent toute « agilité » et efficacité dans la gouvernance et la coordination des politiques publiques qui s'ajoutent à une organisation en « silos » entre ministères, et même en leur sein. La méconnaissance du monde des affaires dans un environnement de guerre économique hybride empêche toute imagination dans la protection de nos actifs ou conduit à des erreurs fatales suite à des dissonances cognitives (comparables à la période des années 1930) de responsables politiques décisionnaires nationaux (cas du rattachement de la Coface à BPI-France), ou européens (modalités de l'accord Swift de 2001 dans le cadre de la lutte anti-terroriste). L'absence d'une véritable professionnalisation des effectifs du SGDSN et le manque de partenariat entre entreprises et d'échanges d'experts public/privé conduisent à des incohérences, et à l'abandon de grands projets ou grands programmes selon l'exemple du CEA (1946) ou du CNES (1961). Autre rupture qui est à conduire par les Etats membres, comme la France et l'Allemagne avec une ambition de puissance, notamment sur le plan satellitaire absent dans les deux revues stratégiques précitées (le succès de Space X devrait être une source d'inspiration) ou IA pour rattraper le retard de l'UE.

Pour autant, si le concept « sécurité nationale » lui-même n'a jamais vraiment bénéficié d'une définition précise partagée par tous les protagonistes entre une vision étroite mais salutaire (armées) et une vision stratégique globale (politique), la situation de l'UE – placée au cœur d'une « compétition déloyale » et ciblée dans son savoir-faire et ses technologies – autorise les Etats-nations membres à porter ce concept autour de la protection de l'information conformément aux nouveaux enjeux.

Ce sont les seuls capables de raisonner en « puissance » et de garantir une « sécurité » conforme aux impératifs de la « sécurité nationale » transposée à l'UE, elle-même mieux régulée autour de deux principes fondamentaux : le principe de subsidiarité inversé à l'intérieur, et le principe de réciprocité à l'extérieur.

Avertissement

La présente note a pour objectif d'interroger la notion même de « sécurité nationale » portée à l'échelle européenne, et de tenter de l'introduire dans la construction européenne à un moment où le doute sur l'efficacité des institutions européennes conduit à l'euroscepticisme.

Un de ses objectifs est d'élever la protection de toute « donnée sensible » au niveau de cette sécurité au-delà du périmètre « secret défense », c'est-à-dire du noyau dur de la DGA (direction générale de l'armement) et porté par l'IGI n° 1300, ainsi que par les textes règlementaires ayant pour objet la PPST (protection du patrimoine scientifique et technique) et les OIV

(opérateurs d'importance vitale) définis dans les DNS (directive nationale de sécurité), ou les référentiels ad hoc de l'ANSSI sur la sécurité des systèmes d'information.

La présente note, comme les suivantes sur ce thème, est conçue de manière à être indépendante les unes des autres, tout en gardant une logique « d'indépendance et de puissance technologiques » en France, et peut-être pour l'UE, à solidifier.

Notes et références

[i] Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites.

[ii] Le substantif retenu doit être décliné selon qu'il s'agit d'intérêts *« fondamentaux »*, *« vitaux »*, *« stratégiques »* ou *« 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 ».*

[iii] *Ce projet vient d'obtenir la validation de son gigantesque plan de constellation satellitaire par les autorités spatiales américaines (février 2018).*

[iv] *Cf. les deux précédentes tentatives d'instaurer le secret des affaires (proposition de loi Carayon en 2012, et la loi Macron en 2015). L'adoption de la directive en juin 2016 a fait l'objet d'intenses débats autour de la menace sur le secret des sources des journalistes et la protection des lanceurs d'alerte (whistleblower).*

[v] *Le CFIUS est indifférent à la nationalité des entreprises. Ainsi, en février 2017, Cree Inc., société américaine d'éclairage LED et de semi-conducteurs, a annoncé qu'elle mettait fin à son accord de vente de sa division Wolfspeed Power & RF à Infineon Technologies AG pour 850 millions de dollars. Entre temps, le CFIUS a soulevé des objections à l'acquisition.*

Ce résultat souligne que le risque CFIUS peut exister dans des transactions impliquant des acheteurs de pays qui sont alliés aux États-Unis. Il souligne également l'intérêt du CFIUS pour les transactions impliquant des technologies sensibles, en particulier dans le secteur des semi-conducteurs.

Depuis 2016, sur les conclusions du CFIUS, le Président américain a bloqué un certain nombre d'autres transactions dans l'industrie des semi-conducteurs impliquant des acheteurs chinois, notamment Aixtron-Fujian Grand Chip, GCS-San'an et Lumileds-GO Scale. Le CFIUS indique que ses préoccupations de sécurité nationale ne sont pas limitées aux acheteurs chinois et peuvent survenir dans des transactions avec toutes sociétés, même de pays étroitement liés aux Etats-Unis.