La lutte contre l'espionnage économique : entre protection privée et sécurité nationale

par Bertrand Warusfel
Professeur agrégé de droit public à l'Université de Vincennes-Saint-Denis (Paris VIII),
Vice-président de l'Association française de droit de la sécurité et de la défense

On mésestime généralement l'importance des actes d'espionnage économique, tant en volume qu'en qualité. Parce qu'ils sont souvent difficiles à détecter et encore plus difficile à prouver, ces agissements directement contraires à la morale et au droit des affaires sont peu étudiés par la doctrine et, lorsqu'ils sont traités sur le plan contentieux, sollicite des régimes juridiques de nature très variable.

Il ne s'agit pas ici de se livrer à une étude exhaustive du phénomène de l'espionnage économique, ni même de son traitement juridique. En revanche, on s'attachera à montrer en quoi cette réalité délictuelle peut par certains côtés avoir un lien avec la sécurité nationale, au sens où cette notion – introduite dans notre droit positif en 2009[1] – implique la prise en compte d'un vaste périmètre de menaces au titre desquelles peuvent figurer certaines formes de l'espionnage économique.

On se demandera donc si la mobilisation des instruments juridiques de droit commun de l'entreprise peut être complétée, le cas échéant, par des outils juridiques relevant spécifiquement du droit dérogatoire de la sécurité nationale et si la nouvelle protection légale du secret des affaires[2]) ne pourrait pas être une opportunité pour créer le chaînon manquant entre les outils de droit privé et le régime spécial de la sécurité nationale. Une protection insuffisante contre les

1. Sur le contour de cette notion, voir notamment notre article : Bertrand Warusfel, « La sécurité nationale, nouveau concept du droit français », *in Mélanges Pierre-André Lecocq : Les différentes facettes du concept juridique de sécurité,* Lille2, décembre 2011, pp. 461-476.
2. Issue de la transposition de la directive de l'Union européenne du 8 juin 2016.

formes les plus poussées de l'espionnage économique (**I**) est complétée par les dispositions de sécurité nationale (**II**), les apports et les limites de la nouvelle protection du secret des affaires (**III**) devant être mesurés.

I. Une protection insuffisante contre les formes les plus poussées de l'espionnage économique

Si l'on définit l'espionnage économique comme l'ensemble des pratiques offensives visant à acquérir par tous moyens des informations relatives à une entreprise en vue de nuire à sa position concurrentielle, on s'aperçoit, tout d'abord, qu'aujourd'hui, de tels actes peuvent prendre des formes très variées, les unes assez classiques alors que d'autres sont beaucoup plus nouvelles. Face à la diversité des formes d'espionnage économique (**A**), quelques moyens juridiques de droit commun (**B**) donne une efficacité limitée face aux formes les plus poussées d'espionnage économique (**C**).

A. Diversité des formes d'espionnage économique

Parmi les pratiques classiques, on connaît le débauchage de salariés (pour les recruter) ou la corruption de ceux-ci (pour qu'ils fournissent des données confidentielles de leur employeur en restant en poste) mais aussi le détournement de supports d'information (documents ou fichiers), voire la pénétration non autorisée dans des lieux confidentiels de l'entreprise-cible.

Mais à ces agissements s'ajoutent de plus en plus d'autres modalités plus difficiles à détecter et à contrer comme les pratiques d'« ingénierie sociale » et de « *misrepresentation* »[3] qui consistent à développer des contacts avec des représentants de l'entreprise visée en usant de fausses qualités pour dissimuler l'objectif offensif véritable (par exemple, en se faisant passer pour un futur client à qui l'entreprise aura à cœur de faire des offres de services détaillées et susceptibles de révéler certains aspects de sa stratégie ou de ses technologies). Plus encore, faut-il désormais compter aussi avec différentes formes de cyber-attaque (qu'il s'agisse de la pénétration dans le réseau interne de la cible, de l'implantation de mouchards ou encore de l'interception de tout ou partie de ses flux de données).

B. Quelques moyens juridiques de droit commun

Les outils classiques du droit de l'entreprise peuvent être sollicités pour répondre à une partie de ces menaces. Schématiquement, on connaît des

3. Voir, notamment, Jérôme Dupré, « Intelligence économique et responsabilité : le cas de la *misrepresentation* », *Droit & Défense,* 97/2, pp. 60-63.

dispositions de droit du travail qui permettent à l'employeur de se prémunir contre de possibles trahisons internes (notamment, *via* l'obligation de loyauté, les clauses de confidentialité, les dispositifs de non-concurrence).

Plus spécifiquement, le droit pénal apporte sa contribution notamment grâce à l'infraction d'abus de confiance[4], souvent sollicitée pour réprimer les agissements déloyaux tant d'un salarié ou ancien salarié que d'un partenaire professionnel quel que soit son statut (consultant, stagiaire, …) ou même de vol (y compris en matière immatérielle depuis que la jurisprudence de la chambre criminelle de la Cour de cassation accepte de qualifier le vol d'informations

Quelques dispositions de droit pénal spécial peuvent également s'avérer utile comme l'incrimination d'atteinte à un secret de fabrique (bien qu'elle reste d'application assez rare) ou surtout les dispositions réprimant la fraude informatique, et particulièrement les articles 323-1 du code pénal (sur l'accès frauduleux à un système numérique) et son article 323-3 qui réprime notamment le fait sans autorisation « *d'extraire, de détenir, de reproduire, de transmettre* » des données.

À cela s'ajoutait uniquement, jusqu'à présent, la possibilité de poursuivre devant le juge civil au titre de l'action en concurrence déloyale certains actes de détournement d'informations confidentielles ou de désorganisation du concurrent. Plus rarement certaines dispositions civiles relevant du droit de la propriété intellectuelle pouvaient être mobilisées pour faire cesser certaines atteintes frauduleuses au patrimoine information d'une entreprise, comme par exemple, en cas de décompilation d'un logiciel protégé, d'atteinte au droit du producteur d'une base de données ou encore en matière de revendication d'un droit de propriété industrielle déposé frauduleusement par le concurrent.

C. Une efficacité limitée face aux formes les plus poussées d'espionnage économique

Mais, jusqu'à l'entrée en vigueur de la récente loi du 31 juillet 2018 instituant une nouvelle protection légale du secrets des affaires (dont nous évoquerons plus loin l'impact qu'elle pourrait avoir en matière d'espionnage économique), cette panoplie assez hétérogène d'outils de droit commun s'était révélée assez peu efficace pour assurer la protection des entreprises contre les formes les plus poussées de l'espionnage économique.

Deux caractéristiques alternatives permettent d'identifier les actes d'espionnage économique les plus graves.

– d'une part, le fait que lesdits actes soient effectués ou commandités depuis l'étranger. Et ce pour une raison d'importance des enjeux et d'efficacité de la riposte judiciaire (laquelle risque d'être d'autant moins effective que l'adversaire sera hors d'atteinte de la juridiction française). À cela s'ajoutant, comme on

4. Art. 314-1 C. pén.

l'évoquera plus loin, la possibilité que l'attaque transfrontière puisse impliquer aussi un État étranger ;

– d'autre part, on doit considérer comme particulièrement graves et préjudiciables les attaques qui sont le fait non pas du concurrent lui-même mais d'intermédiaires professionnels agissant pour le compte de commanditaires (souvent difficiles à identifier) et ayant généralement des compétences particulières pour mettre en œuvre des techniques de recueil d'informations, souvent issues de la pratique des services de renseignement d'État.

Face à des attaques transfrontalières et/ou menées par des « *officines* » spécialisées de renseignement, les instruments de droit commun évoqués plus haut sont partiellement inefficaces et ce pour plusieurs raisons. Tout d'abord, il s'agit souvent de pratiques qui sont difficiles à détecter, voire à prouver. Ensuite, le commanditaire reste difficilement atteignable par une sanction judiciaire (soit qu'il demeure inconnu caché par l'écran que constitue le prestataire, soit qu'il soit implanté hors du territoire).

C'est aussi le quantum des peines potentielles qui peut être sans commune mesure avec le niveau de préjudice encouru par l'entreprise victime. Au pénal, seul l'article 323-3 du code pénal (qui punit, en particulier, l'extraction de données par voie numérique) est punissable de 5 années d'emprisonnement, alors que la sanction du simple accès frauduleux n'est que deux années au maximum (contre trois pour l'abus de confiance, qui permet en revanche une amende importante de 375.000 €). Sur le terrain civil, seule la démonstration précise du niveau de préjudice subi par l'entreprise victime pourra fonder une demande d'indemnisation significative, ce qui se heurte souvent au fait que le préjudice découlant directement de l'acte d'espionnage demeure difficile à déterminer.

On pourrait, en revanche, penser que les dispositions légales sanctionnant les atteintes à la sécurité nationale, et plus particulièrement aux « intérêts fondamentaux de la nation » (expression pénale, à notre sens, des objectifs de sécurité nationale) pourraient compléter utilement la répression des actes d'espionnage économique les plus offensifs. Mais la réalité est assez différente et nous montre qu'il demeure encore un écart entre les protections offertes par les différentes branches du droit privé et celle qui découle de la préservation des intérêts de sécurité nationale.

II. Une protection complétée par les dispositions de sécurité nationale

Depuis 1994 (date de l'entrée en vigueur du nouveau code pénal), les dispositions expresses des articles 410-1 et suivants du code pénal paraissent de nature à prendre en compte les menaces majeures s'appliquant en matière d'espionnage

économique. Mais, par-delà le sens littéral des textes, un quart de siècle d'hésitation jurisprudentielle nous a montré que ces textes ne sont pas effectivement suffisamment adaptés aux formes contemporaines d'espionnage économique. Une protection affirmée par les textes (**A**) est confrontée à une pratique en recul par rapport aux ambitions initiales (**B**).

A. Une protection affirmée par les textes

On en développera pas le cas particulier des secrets économiques ou technologiques classifiés qu'une entreprise peut détenir (voire produire elle-même) en application d'un marché public dit « *marché classé* », au sens de l'instruction générale interministérielle sur la protection du secret de la défense nationale[5]. Dans ce cas, en effet, les secrets économiques éventuellement visés par les actes d'espionnage économiques sont aussi des secrets de la défense nationale dont la protection pénale est spécifiquement assurée par les articles 413-10 à 413-12 du code pénal, qui font encourir des peines de trois à sept années d'emprisonnement, du simple fait qu'une compromission de ce secret de défense a pu être constatée.

En revanche, on évoquera plus longuement la protection pénale des « *intérêts fondamentaux de la nation* », qui – parmi les révolutions textuelles introduites par le nouveau code pénal, voté en 1992 – vise, au-delà des menaces classiques pouvant affecter les fonctions régaliennes de l'État, un périmètre élargi où l'on retrouve en particulier les *« éléments essentiels de son potentiel scientifique et économique* ».

Par référence à cette définition, les articles 411-5 à 411-8 répriment différentes formes d'intelligence avec une puissance étrangère (article 411-5) ainsi que la livraison d'informations à celle-ci (article 411-6 à 411-8) lorsqu'elles touchent notamment ces éléments essentiels du potentiel scientifique et économique national.

Il est donc bien prévu par ces textes qu'une pratique d'espionnage mené par une « puissance étrangère », une « *entreprise ou organisation étrangère ou sous contrôle étranger* » ou « *leurs agents des renseignements* » et qui porte sur tout élément immatériel (« *renseignements, procédés, objets, documents, données informatisées ou fichiers* ») touchant les éléments essentiels du potentiel scientifique et économique national, puisse être sanctionnée par des peines allant de dix à quinze ans d'emprisonnement.

Ces dispositions peuvent parfaitement réprimer certaines formes d'espionnage économique. Pour autant, leur application en la matière dépend de deux conditions qui – dans la pratique – se révèlent difficiles à respecter. Tout d'abord,

5. Arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale, *JORF* n° 0279 du 2 décembre 2011.

l'incrimination ne vaut qu'à l'encontre des opérations de renseignement économique menée par ou au profit d'un acteur étranger. Or, lorsqu'il s'agit d'un service gouvernemental, la preuve de son implication peut s'avérer difficile à rapporter (notamment si l'opération se déroule essentiellement par voie numérique) tandis que s'il s'agit d'une entreprise étrangère, il sera souvent difficile de distinguer clairement la frontière entre ce qui relève d'un comportement concurrentiel agressif (pouvant être réprimé de manière autonome par des dispositions civiles évoquées précédemment) et ce qui s'apparente à une véritable opération de renseignement économique qui pourrait relever des sanctions du livre IV du code pénal. L'un des « *marqueurs* » de l'espionnage à proprement parler est sans doute la dimension « *conspirative* » des relations entre le commanditaire étranger et la ou les sources ou intermédiaires français, ce qu'un commentateur des dispositions pénales considérées décrit comme « *des faits matériels, répondant, le plus souvent, à la clandestinité et à la répétition d'efforts qu'un agent étranger peut entreprendre auprès d'un ressortissant français* » en vue de parvenir à s'assurer par exemple l'accès à une information confidentielle[6].

Mais, la seconde difficulté est, en pratique, plus importante puisqu'elle touche à la délimitation même de ce que sont les éléments essentiels du potentiel scientifique et économique national.

B. Une pratique en recul par rapport aux ambitions initiales

Faute d'une importante jurisprudence, il faut donc se retourner vers les quelques appréciations doctrinales ou administratives autorisées qui se sont exprimées sur cette question. L'une des plus approfondies a été le commentaire fait par la Commission nationale de contrôle des interceptions de sécurité (CNCIS, aujourd'hui disparue au profit de la nouvelle CNCTR) puisque « *la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France* » figurait aussi parmi les motifs que la loi du 10 juillet 1991 reconnaissait comme pouvant légitimer une demande d'interception de sécurité[7].

Pour la CNCIS, « *l'article 410-1 du code pénal permet d'étendre la protection du Code pénal non seulement aux différents secteurs de l'économie au sens étroit du terme mais également à la recherche scientifique et aux innovations techniques ou technologiques sur lesquelles reposent précisément la force ou la compétitivité du pays* ». *Après avoir étudié plus particulièrement les articles 411-5 à 411-8, elle a*

6. Serge Reyne, « Atteinte aux intérêts fondamentaux de la nation », *Répertoire de droit pénal et de procédure pénale*, Dalloz, 2009, n° 46.

7. Dans son article 3, devenue après la codification de la sécurité intérieure, l'article L. 241-2 CSI jusqu'à son abrogation par la loi du 24 juillet 2015 relative au renseignement, qui a fait néanmoins de la protection des « *intérêts économiques, industriels et scientifiques majeurs de la France* » l'un des motifs pouvant justifier la mise en œuvre d'une technique de renseignement (nouvel art. L. 811-3 3° CSI).

considéré également que « tout forme d'espionnage, y compris économique comme le transfert illicite de technologie, est clairement incriminée par ces articles, où est effectivement visée, la fourniture de procédés ».

Mais, s'agissant de la détermination des activités économiques ou scientifiques pouvant être considérées comme relevant des « éléments essentiels » du patrimoine national, la CNCIS a adopté une position assez prudente. S'il elle admettait que le « transfert illicite d'un procédé de fabrication, détenu exclusivement par un groupe national leader dans sa spécialité, est bien de nature à porter gravement atteinte aux éléments essentiels du potentiel scientifique et économique de la France », elle n'en estimait pas moins que « *l'activité de l'entreprise menacée doit enfin être liée à la défense de notre indépendance nationale au sens de l'article 5 de la Constitution de la V^e^ République ou à la sécurité nationale* » et que les textes réglementaires sur le contrôle des investissements étrangers devait être pris en considération pour déterminer les « *secteurs d'activité dont l'intérêt justifie la surveillance de leur financement au moyen d'investissements étrangers* »[8], ce qui « *peut, par analogie, représenter un travail d'approche qualitative des secteurs constituant les éléments essentiels du potentiel scientifique et économique de la France* »[9].

Même si la liste de ces secteurs sensibles a été une nouvelle fois élargie en novembre 2018[10], une telle référence restreint nécessairement (et, en partie, à juste titre) le périmètre des domaines d'activité à propos desquels des actes d'espionnage économique pourrait être réprimés fortement au titre de l'atteinte aux intérêts fondamentaux de la nation[11].

Bien que la part dans les demandes formulées par les services de renseignement au titre des intérêts économiques essentiels a assez fortement augmenté depuis que la nouvelle CNCTR contrôle un périmètre élargi de demandes de mise en œuvre de techniques de renseignement[12], cette dernière demeure encore assez restrictive sur ce terrain du contre-espionnage économique, comme en témoigne ce passage du rapport annuel pour 2017 de la délégation parlementaire au renseignement : « *la délégation s'interroge sur le nombre conséquent d'avis défavorables formulés par la CNCTR par rapport aux demandes adressées au titre*

8. La liste de ces secteurs est aujourd'hui fixée par l'article R. 153-2 du code monétaire et financier.

9. CNCIS, *Rapport annuel 2014*, pp. 114 à 116.

10. Par le décret n° 2018-1057 du 29 novembre 2018 relatif aux investissements étrangers soumis à autorisation préalable.

11. Pour être complet, il y a sans doute lieu de compléter cette liste de secteurs économiques par la liste des domaines scientifiques et techniques dans lesquels peuvent être créés des « *zones à régime restrictif* » (ZRR), au titre de l'article R. 413-1 du code pénal (annexe II de l'arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation, pris en application du décret n° 2011-1425 du 2 novembre 2011).

12. En 2017, le motif des intérêts économiques, industriels et scientifiques majeurs représentait 12 % des demandes étudiées par la CNCTR (CNCTR, *2^e^ rapport d'activité 2017*, p. 52) et en 2018, 9 % (CNCTR, *3^e^ rapport d'activité 2018*, p. 67).

des autres finalités de la politique publique de renseignement. D'autant qu'en 2015, à l'occasion de l'examen du projet de loi relatif au renseignement, le législateur a fait le choix d'une définition large des intérêts économiques, industriels et scientifiques en préférant le qualificatif « majeurs » *au qualificatif* « essentiels », *considéré comme plus restrictif. Interrogé, sur ce point, par la délégation, le président de la CNCTR a indiqué que la CNCTR avait choisi, en la matière, de n'adopter aucune doctrine générale au profit d'une approche pragmatique, au cas par cas. Pour chaque demande dont elle est saisie, la CNCTR fonde son appréciation, non pas sur ce que l'État aurait défini comme présentant un intérêt majeur, mais sur une appréciation* « propre » *de ce qu'elle estime comme tel* »[13].

Au-delà de ces interprétations doctrinales plus ou moins extensives, une affaire contentieuse a marqué les esprits en matière d'espionnage économique. Il s'agissait de la tentative par un ancien ingénieur du centre de recherches de Michelin de revendre à plusieurs de ses concurrents étrangers certains de ses secrets technologiques. Identifié par la DST suite à la plainte de l'entreprise, il avait poursuivi et renvoyé devant le tribunal correctionnel tant pour la violation de secrets de fabrique que pour abus de confiance et plus encore atteinte aux intérêts fondamentaux de la nation (sur le fondement de l'article 411-7 C. pén).

Pour autant, la chambre correctionnelle du tribunal de Clermont-Ferrand ne retint contre lui que l'abus de confiance et rejeta avec un certain détail de motivation l'incrimination d'atteinte aux intérêts fondamentaux de la nation. Elle a relevé notamment que « la démarche de M. A. de s'adresser à ces trois sociétés, était plus dictée par la considération qu'il s'agissait de concurrents directs de la Manufacture Michelin que par celle qu'il s'agissait d'entreprises étrangères » et que « *s'il est indéniable que les informations rassemblées par M. A., présentaient un caractère de confidentialité important, de sorte que leur divulgation à une entreprise concurrente était de nature à porter atteinte à la stratégie commerciale de l'entreprise Michelin, il n'en résulte pas pour autant que M. A. ait également porté atteinte aux intérêts fondamentaux de la nation* »[14].

Allant encore un peu plus dans l'analyse, les juges correctionnels ont estimé qu'il « *ne peut être tenu pour établi que les informations recueillies par M. A. dans le cadre de son activité professionnelle au sein de la Manufacture M., présentaient un caractère à ce point stratégique qu'elle mettaient en jeu des éléments essentiels du potentiel économique français* » et que « *le seul fait du classement en ERR n'induit pas nécessairement que des éléments essentiels du potentiel économique de la France, au sens de l'article 410-1 du Code pénal, soient concernés* ».

13. Délégation parlementaire au renseignement, *Rapport annuel 2017*, p. 54. On relativisera cependant quelque peu cette critique de la DPR au regard de notre sujet, en signalant que les réticences de la CNCTR, relevées par le rapport, ont sans doute trait aussi aux demandes de techniques offensives, et non pas seulement aux demandes justifiées par la lutte contre l'espionnage économique étranger.
14. TGI Clermont-Ferrand, ch. corr., 21 juin 2010, note Michel Véron, *Droit pénal* n° 11, novembre 2010, comm. 116.

Comme l'a relevé l'un des commentateurs de cette décision (devenue définitive), elle a donné « *à l'infraction définie par l'article 411-7, ainsi qu'à toutes celles du même chapitre et bâties sur le même modèle, une portée très étroite, non par rapport aux actes matériels mis en œuvre, mais en considération de la finalité des moyens utilisés* »[15].

III. Les apports et les limites de la nouvelle protection du secret des affaires

C'est dans ce contexte qu'ont été adoptées successivement la directive du 8 juin 2016, puis la loi française qui l'a transposée, le 30 juillet 2018, créant une protection légale du « *secret des affaires* »[16].

On relèvera que si ce nouveau dispositif va incontestablement renforcer la capacité des entreprises à protéger leurs secrets et à lutter juridiquement contre les actes de renseignement économique, il ne comporte pas en lui-même de dispositions particulières qui pourrait directement contribuer à la protection de la sécurité économique nationale. Mais un renforcement limité de ce dispositif pourrait être facilement envisagé pour combler l'écart qui existe toujours entre les protections privées de droit commun et les dispositions dérogatoires de sécurité nationale. Ainsi, un renforcement de la prévention et de la répression des atteintes aux secrets économiques (**A**) s'ajoute à un dispositif de droit commun qui pourrait être utilement complété (**B**).

A. Un renforcement de la prévention et de la répression des atteintes aux secrets économiques

Les nouveaux textes ont créé un secret des affaires qui bénéficie d'une protection particulière dès lors, que – en application du nouvel article L. 151-1 du code de commerce, l'information considérée est effectivement secrète[17], que ce caractère confidentiel lui confère une « *valeur commerciale, effective ou potentielle* » et qu'elle a fait l'objet « *de mesures de protection raisonnables, compte tenu des circonstances, pour en conserver le caractère secret* ».

Une telle définition du secret des affaires est suffisamment large pour pouvoir couvrir non seulement des secrets économiques purement concurrentiels mais

15. M. Véron, note précitée.
16. Loi n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires, *JORF* n° 0174 du 31 juillet 2018 (complété par le décret n° 2018-1126 du 11 décembre 2018, *JORF* du 13 décembre 2018).
17. Au sens où elle ne doit pas être « *en elle-même ou dans la configuration et l'assemblage exacts de ses éléments, généralement connue ou aisément accessible pour les personnes familières de ce type d'informations en raison de leur secteur d'activité* » (art. L. 151-1 1° C. com.).

aussi certaines informations économiques qui, par leur importance ou le secteur concerné, seraient également de nature à intéresser les éléments « *majeurs* » ou « *essentiels* » de la sécurité nationale économique du pays.

Certes, le critère de la valeur commerciale peut paraître quelque peu restrictif, puisque l'intérêt général s'attachant à la protection des intérêts fondamentaux de la nation[18] pourrait *a priori* couvrir également des informations sensibles dépourvues de valeur commerciale. Pour autant, même dans les secteurs très régaliens comme les industries de défense et de sécurité, la grande majorité de leurs informations sensibles sont aussi des données qui peuvent avoir, d'une manière ou d'une autre, une valorisation économique. L'écart ne devrait donc pas être trop prononcé[19].

Par ailleurs, l'injonction d'adopter des mesures de protection pour assurer la confidentialité des secrets de l'entreprise ne peut qu'aller dans le sens d'une moindre exposition de l'entreprise concernée et de ses données internes à la menace de l'espionnage économique. Lorsqu'une entreprise qui aurait dans une partie de son périmètre la nécessité de respecter les règles de la protection du potentiel scientifique et technique de la nation (PPST, évoquée plus haut) voire de protéger le secret de la défense nationale, voudra également protéger ses autres secrets, il lui suffira donc de décliner peu ou prou les mesures déjà prises en son sein pour respecter les réglementations de la PPST ou du secret de défense et d'y adapter tout ou partie de ses moyens de sécurité au cas particulier des secrets des affaires. En d'autres termes la logique de classification des documents et des informations et d'habilitation des personnes y ayant accès peut tout à fait être transposée (avec un niveau d'exigences plus léger) à la protection des seuls « *secrets des affaires* »)[20].

En d'autres termes, et contrairement à d'autres dispositifs (comme celui réprimant, en droit pénal, les actes de cybercriminalité), la loi ne protègera pas toutes les entreprises et tous leurs informations confidentielles, mais uniquement celles qui auront préalablement organisé une politique de sécurité en leur sein de façon à pouvoir – en cas d'atteinte – demander la protection de la loi devant les tribunaux. Cette incitation légale à la prévention devrait naturellement accroître la résilience des entreprises françaises face aux différentes formes d'espionnage économique. La loi du 30 juillet 2018 est donc bien conforme de

18. Que le Conseil constitutionnel considère comme étant un objectif à valeur constitutionnel.

19. Sur le recouvrement pouvant exister – malgré leurs différences de nature juridique – entre protection des secrets privés d'entreprise et le secret de défense ainsi qui comporteraient un « *objet commun* » (à savoir la PPST), v. Barré-Pépin, « Secret industriel et commercial – secret d'entreprise et des affaires – et secret de la Défense », *in* André Larceneux et Juliette Olivier-Leprince (dir.), *Le secret nucléaire*, EUD, p. 17.

20. Voir, par exemple, le guide de la chambre de commerce et d'industrie Paris-Ile de France : Secret des affaires – Guide pratique à l'usage des TPE/PME/ETI, 2018, pp. 12-18 (qui décrivent un « *référentiel* » de politique de sécurité des informations).

ce point de vue aux espérances que les praticiens de l'intelligence économique avaient placées en elle, qu'ils appelaient de leur vœu au titre du volet défensif de l'intelligence économique[21], ou de ce que nous avons aussi appelé « *l'intelligence juridique* »[22].

B. Un dispositif de droit commun qui pourrait être utilement complété

Pour autant (et quoi que certains de ses promoteurs aient voulu dire), la nouvelle loi sur le secret des affaires n'est pas un « *Cohen Act à la française* ». En effet, la loi américaine *Economic Espionage Act* of 1996 a la particularité d'avoir associé dans un même texte la répression de l'atteinte concurrentielle à un « *trade secret* » et celle de l'espionnage économique mené par un État ou une organisation étrangère.

Ainsi, si son paragraphe 1832 sanctionne de dix années de prison quiconque détourne un secret d'affaires « *dans l'intérêt économique de quelqu'un d'autre que son propriétaire* », son paragraphe 1831 punit de quinze années de prison, celui qui commet les mêmes agissements « *sachant que l'infraction profite à un gouvernement, une organisation ou un agent étranger* »[23].

Comme nous l'indiquions alors, le législateur américain a ainsi choisi « d'extrapoler son dispositif contre l'espionnage économique d'État à partir de la protection des secrets d'affaires (soit une approche de bas à haut). Tout le contraire de la démarche française qui avec le concept des intérêts fondamentaux de la nation a tenté d'élargir la protection des secrets de l'État vers le bas sans pour autant renforcer son dispositif de protection des secrets de fabrique et instaurer (encore) un véritable « *trade secret* » à la française »[24].

De plus, et même si les sanctions civiles prévues par la loi de 2018 ne sont pas négligeables (notamment avec la possibilité d'obtenir une indemnisation large du préjudice subi – comme en matière de contrefaçon, mais aussi la possibilité d'obtenir l'interdiction et le retrait des produits qui seraient considérés comme ayant été développés en utilisant le secret des affaires détourné[25],

21. Sur la place des préoccupations d'intelligence économique dans la genèse de la protection du secret des affaires, v. notre article : Bertrand Warusfel, « Les enjeux juridiques et politiques de la protection des secrets d'affaires » *in* J. Lapousterle & B. Warusfel (dir.) *La protection des secrets d'affaires – perspectives nationales et européennes*, LexisNexis, 2017, pp. 2-14.
22. V. notamment Bertrand Warusfel, « L'intelligence juridique : une nouvelle approche pour les praticiens du droit », *Le Monde du droit*, 1er/15 avril 2010.
23. Traduction et commentaire in Bertrand Warusfel, « La loi américaine sur l'espionnage économique », *Droit & Défense*, n° 97/1, pp. 64-67.
24. B. Warusfel, *idem,* p. 64.
25. Nouveaux articles L. 152-6 (indemnisation) et L. 152-3 (interdictions) du code de commerce.

le législateur français n'a pas prévu de dispositions pénales complémentaires à l'action civile que la directive de juin 2016 imposait (à juste titre) de mettre en place[26].

C'est sans doute à ce niveau qu'un double complément à la protection civile établie pourrait venir renforcer l'arsenal de protection des entreprises françaises face aux risques croissants d'espionnage économique.

En prévoyant la possibilité, à titre alternatif, d'une action pénale pour poursuivre les mêmes faits (ou seulement certains d'entre eux, définis limitativement par la loi), on donnerait à la victime un choix d'action plus large (comme en matière de contrefaçon de propriété intellectuelle, qui peut être poursuivie à la fois au civil et au pénal) et on permettrait notamment de bénéficier, dans les cas justifiés, des moyens d'investigation des services de police judiciaire spécialisés.

On peut penser, en effet, que face à ce que nous avons appelé plus haut « *les formes les plus poussées* » d'espionnage économique, seule une enquête judiciaire active mettant en œuvre des moyens d'investigation lourds (interceptions, surveillances, perquisitions, gardes à vue, …) voire la mise en branle de mécanismes de coopération transfrontalière pourraient permettre de recueillir les preuves et de confondre réellement les auteurs et les commanditaires d'opérations menées avec un certain niveau de clandestinité.

De plus, et en se rapprochant de l'approche américaine du Cohen Act, il serait certainement intéressant de prévoir une circonstance aggravante lorsque les actes d'espionnage poursuivis sont d'une part commis au profit de l'étranger.

Cette logique avait inspiré la proposition de loi initialement déposée par Jean-Jacques Urvoas (puis reprise un temps à titre d'amendement à la future loi « *Macron* ») et qui proposait la création d'un article du code pénal qui aurait comporter les deux alinéas suivants :

« *I. – Le fait pour quiconque de prendre connaissance ou de révéler sans autorisation ou de détourner toute information protégée au titre du secret des affaires au sens de l'article L. 151-1 est puni de trois ans d'emprisonnement et de 375 000 € d'amende.*

II. – La peine est portée à sept ans d'emprisonnement et 750 000 € d'amende lorsque l'infraction est de nature à porter atteinte à la souveraineté, à la sécurité ou aux intérêts économiques essentiels de la France ».

À notre sens, la seule faiblesse d'une telle rédaction tenait à la référence à « *la souveraineté, à la sécurité ou aux intérêts économiques essentiels de la France* » (formule tirée de la loi du 26 juillet 1968) alors que l'on retrouve désormais des termes très proches dans la définition des intérêts fondamentaux de la nation,

26. Sur les perspectives pénales qui pouvaient être envisagées, v., notamment, Jean Lapousterle, « La protection pénale des secrets d'affaires », *in* J. Lapousterle et B. Warusfel (dir.), 2017, précité, pp. 124-141.

lesquels sont protégés par d'autres dispositions qu'il ne faut pas concurrencer, au risque de créer plus de confusion là où il faut au contraire créer un dispositif distinct et complémentaire.

Notre proposition serait plutôt de ne pas prévoir de critère touchant à la nature des secrets protégés mais à simplement prévoir l'application de cette circonstance aggravante dans le cas où l'atteinte poursuivie paraît commise par ou au profit d'un État, d'une entreprise ou d'une organisation étrangère (et sans doute en se limitant – pour éviter toute contrariété possible avec le droit de l'Union – aux entités étrangères hors de l'Union européenne).

Cela ne serait pas totalement nouveau dans sa logique, puisque l'on sait que les infractions relatives à la cybercriminalité prévoient une circonstance aggravante lorsque l'atteinte est commise à l'encontre d'un « *système de traitement automatisé de données à caractère personnel mis en œuvre par l'État* »[27]. Par ailleurs, on connaît déjà la loi du 26 juillet 1968 précitée (dite « *loi de blocage* ») qui réprime pénalement la communication de certaines informations à des entités ou autorités étrangères[28].

Ainsi complétée par une disposition pénale et une circonstance aggravante visant plus particulièrement l'espionnage économique dans ses formes les plus poussées, et particulièrement au profit d'entités étrangères, la nouvelle protection du secret des affaires pourrait venir s'intégrer de manière harmonieuse dans un dispositif complet, tant civil que pénal, de protection des secrets d'entreprise contre les différentes formes de l'espionnage économique.

27. Articles 323-1, 323-2, 323-3 et 323-4-1 du code pénal.
28. Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères (modifiée par la loi du 16 juillet 1980).