



**HAL**  
open science

## Secret industriel et commercial -secret d'entreprise et des affaires -et secret de la Défense

Martine Barré-Pépin

► **To cite this version:**

Martine Barré-Pépin. Secret industriel et commercial -secret d'entreprise et des affaires -et secret de la Défense. in: Le secret nucléaire, André Larceneux et Juliette Olivier-Leprince (Dir.) , EUD, pp.71-107, 2014. hal-01704235

**HAL Id: hal-01704235**

**<https://hal.science/hal-01704235v1>**

Submitted on 8 Feb 2018

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

## Secret industriel et commercial - secret d'entreprise et des affaires - et secret de la Défense

Martine BARRÉ-PÉPIN

À l'instar du secret militaire, dans l'ordre public de la défense de la Nation, de la souveraineté, du territoire et des citoyens, le secret industriel et commercial, dans le secteur de la libre entreprise, de la concurrence et des activités privées, empêche ou contrarie l'accès à des informations, des données et des lieux. Les deux types de secret sont également de nature à limiter la portée des obligations légales d'information, de concertation et de participation du public au processus de prise des décisions ayant un impact sur la santé et l'environnement. Et, alors qu'ils relèvent de finalités et d'ordres essentiellement différents, leurs champs respectifs sont néanmoins susceptibles de se recouper ou se superposer. Dans le domaine notamment de technologies duales, caractéristiques du secteur nucléaire, de sa recherche et de ses applications civiles (énergie, santé, TIC) et/ou militaires (armements), le secret industriel et le secret défense se confondent de sorte que le régime de l'un se substitue à l'autre : le régime formaliste, plus rigoureux et impératif, du secret défense prévaut alors.

Dans la dialectique qui oppose publicité et confidentialité, diffusion et réservation, publication ou accès du public à des informations, données commerciales ou stratégiques et maintien du secret, le régime juridique de l'information s'organise entre accessibilité, conformément aux droits du public à l'information, libertés et principes fondateurs des obligations légales de transparence, et inaccessibilité tenant à la protection et à la non-divulgaration de secrets privés.

Cinq points seront développés ci-après.

*La typologie des secrets privés (I).* Le secret de la vie privée et le secret industriel, commercial et des affaires sont de nature radicalement différente. Le secret industriel en particulier se distingue du secret défense, répondant à une logique d'appropriation privative, concurrentielle, et non à des intérêts nationaux fondamentaux. Déterminé par la possession, une maîtrise de fait, il n'obéit à aucune procédure formaliste de détermination par classification et habilitation.

*L'encadrement juridique du secret industriel et des affaires est l'actualité législative (II).* L'information réservée par des entreprises est objectivement cachée ou relativement couverte par des clauses de secret. Le non-respect de conventions de confidentialité est, en droit, très difficilement « réparable » et, en fait, irrémédiable. Et les jurisprudences française et européenne en bornent les effets excessifs. Aussi, en renfort de dispositions peu appropriées aux violations de secrets d'entreprises, une récente proposition de loi réprimant l'atteinte au « secret des affaires » pourrait instaurer une classification « d'informations à caractère économique protégées », sur le modèle du régime du secret-défense.

*Le secret industriel n'a pas de caractère absolu - il est soumis aux impératifs participatifs (III).* Les obligations d'information en limitent la portée. Les entreprises ne peuvent opposer des secrets à l'administration et/ou au public que dans et sous certaines conditions. En matière environnementale, en particulier dans la filière nucléaire, les tribunaux opèrent un équilibre entre les intérêts en présence, aménageant de la sorte le clivage « besoin de protection des entités et activités civiles » et « droit du public à l'information dans le cadre des lois et institutions de transparence ». De nature à restreindre les obligations d'information et de communication qui incombent aux exploitants d'installations nucléaires, INB et INBS, des dispositions précisent par qui et comment le secret

industriel et des affaires peut en pratique être invoqué et quand il est opposable en droit<sup>1</sup>.

*Les principes de souveraineté et de territorialité sont inhérents au brevet, titre octroyé par l'État (IV). Le régime de la brevetabilité des inventions impose la description de résultats innovants et leur divulgation par un office national, l'INPI, en contrepartie de l'exclusivité revendiquée par l'inventeur ou l'ayant-droit. La procédure de dépôt de demande de brevet donne lieu à un contrôle du Ministère de la Défense, avec maintien temporaire et prorogeable au secret, en vue d'une éventuelle classification de la technologie visée, le brevet n'est alors pas délivré. Dans les stratégies d'entreprises, l'option du dépôt d'une demande et de la propriété industrielle est antinomique du secret industriel.*

*Le secret industriel et le secret défense ont un objet commun, la défense du patrimoine ou potentiel scientifique et technique – PST – de la nation (V). Les notions, objectifs et pratiques d'intelligence économique, territoriale et stratégique transcendent, en réalité et en droit, le clivage civil/militaire. À l'égard des puissances étrangères, les systèmes de protection des données relèvent de la responsabilité du Secrétariat Général à la Défense Nationale, avec la Haute Fonction de Défense et de Sécurité des ministères, et des services de la Direction Centrale du Renseignement Intérieur. Ainsi, dans le secteur nucléaire, des technologies duales et de rupture – avec l'enjeu de la suprématie -, le secret industriel est « absorbé » par le secret défense dont le régime s'impose alors.*

---

<sup>1</sup> M. Barré-Pépin, L'opposabilité des secrets privés en matière environnementale, *Infra p. ???*

## **I/ Typologie des secrets privés – secret de la vie privée et données personnelles, secret industriel, commercial et des affaires**

Au regard du principe participatif et des obligations de transparence, les secrets doivent constituer des exceptions aussi limitées que possibles à une règle d'accès à l'information, par conséquent être délimités. Répondant à des intérêts particuliers d'individus ou d'entreprises et non à des impératifs de défense, les secrets privés présentent un même caractère de relativité - ils ne sont communicables qu'aux seuls intéressés. Or l'indétermination de leur objet, en particulier pour le secret industriel et commercial, rend difficile la mesure de la restriction afférente ainsi qualifiée de « passif environnemental occulte ». A cet égard, la teneur et la légitimité du secret revendiqué sont cruciales<sup>2</sup>. Le secret de la vie privée (1) et le secret industriel et des affaires (2) sont de nature et présentent des dimensions radicalement différentes parce que la protection qui s'y attache touche, soit aux droits fondamentaux de la personne concernée, soit à la propriété privée, aux actifs comptables et stratégiques, à la concurrence et à la compétitivité d'entités économiques. L'un relève de l'ordre de l'être et met en jeu la liberté des individus, l'autre, de l'ordre de l'avoir et du secteur marchand, intéressant les biens de l'entreprise et sa position sur des marchés.

À l'instar du secret des statistiques portant sur des renseignements individuels ayant trait à la vie personnelle et familiale, aux faits et comportements d'ordre privé<sup>3</sup>, le secret médical qui s'inscrit dans le droit au respect de la vie privée de toute personne prise en charge par un professionnel de santé répond aussi à l'intérêt général, à des impératifs de santé publique, de prévention et gestion de risques sanitaires. Il est régi par le code de la santé publique<sup>4</sup> et soumis à des règles déontologiques de l'Ordre professionnel des médecins<sup>5</sup>. Partagé par les soignants prenant part aux soins, c'est aussi un secret professionnel dont la violation relève de l'article 226-13 du code pénal<sup>6</sup>. D'une manière générale, la protection de tous les secrets privés est en droit relayée et renforcée par l'obligation - qui incombe à leurs dépositaires professionnels - de ne pas les révéler.

1 – Le secret inhérent au respect de l'intimité de la vie privée et à la protection des données personnelles « sensibles » - d'opinion, d'orientation ou d'appartenance - relève de l'exercice de la liberté et de la volonté individuelles. La révélation d'informations relatives à la vie privée requiert le consentement exprès et spécial de l'intéressé ; en principe, une autorisation n'est jamais donnée qu'à des personnes déterminées et elle est limitée à des utilisations spécifiées. En revanche, les données

---

<sup>2</sup> Secret commercial ou industriel, secret financier, secret médical... sans oublier le secret défense, le plus "méchant" de tous ! L'accès à certains dossiers s'avère aujourd'hui encore difficile. D'autant qu'il peut arriver que nous ne connaissions même pas l'existence d'un dossier. Et dans ce dernier cas, comment demander à le consulter ? (...), Didier Champion, directeur de l'environnement et de l'intervention de l'IRSN et Monique Sené, vice-présidente de l'Association nationale des commissions locales d'information, ANCLI. IRSN, Magazine Repères n°3, Septembre 2009.

<sup>3</sup> Loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques, Article 6 : *Sous réserve des dispositions des articles 40, 56, 76, 97 et 99 du code de procédure pénale et de celles de l'article L. 213-3 du code du patrimoine, les renseignements individuels figurant dans les questionnaires revêtus du visa prévu à l'article 2 de la présente loi et ayant trait à la vie personnelle et familiale et, d'une manière générale, aux faits et comportements d'ordre privé ne peuvent, sauf décision de l'administration des archives, prise après avis du comité du secret statistique et relative à une demande effectuée à des fins de statistique publique ou de recherche scientifique ou historique, faire l'objet d'aucune communication de la part du service dépositaire avant l'expiration d'un délai de soixante-quinze ans suivant la date de réalisation de l'enquête ou d'un délai de vingt-cinq ans à compter de la date du décès de l'intéressé, si ce dernier délai est plus bref.*

<sup>4</sup> Article L1110-4 : *Toute personne prise en charge par un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et du secret des informations la concernant.*

<sup>5</sup> Article 4 (article R.4127-4 du code de la santé publique) : *Le secret professionnel, institué dans l'intérêt des patients, s'impose à tout médecin dans les conditions établies par la loi.*

*Le secret couvre tout ce qui est venu à la connaissance du médecin dans l'exercice de sa profession, c'est-à-dire non seulement ce qui lui a été confié, mais aussi ce qu'il a vu, entendu ou compris.*

<http://www.conseil-national.medecin.fr/article -4-secret-professionnel-913>

<sup>6</sup> *La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15000 euros d'amende.*

personnelles et fichiers « circulent », s'échangent librement, comme des marchandises<sup>7</sup> sous réserve du respect de la législation informatique et libertés protégeant, en Europe, les individus qui ont les droits de s'y opposer et d'y accéder. Et les personnes concernées doivent consentir à la réutilisation de leurs données contenues dans les documents communiqués, à moins qu'elles ne soient anonymisées. La maîtrise par chacun de la destination - autrement dit des usages qui peuvent être faits - des propos, images et informations relatives à sa vie privée est limitée en droit par la liberté de la presse et le droit du public à l'information d'actualité et surtout par les intérêts supérieurs de la justice. En pratique et sauf à engager des poursuites pénales contre des atteintes à la personne suivant les procédures prévues par la LCEN<sup>8</sup>, la diffusion de telles images et informations sur internet et les réseaux sociaux, qu'elle soit de leur fait ou non, échappe à tout contrôle de la part des intéressés.

En matière environnementale cependant, la protection de la vie privée ne figure pas parmi les motifs de refus de communication d'une information relative à des émissions qui sont visés à l'article L.124-5-II du code de l'environnement<sup>9</sup>. En revanche, les documents se rattachant à une activité privée qui portent une appréciation ou un jugement de valeur sur une personne physique nommément désignée ou facilement identifiable (ou font apparaître le comportement d'une personne dès lors que la divulgation de ce comportement pourrait lui porter préjudice) ne sont pas communicables. En ce qui concerne le secret professionnel médical, les médecins et professionnels de santé apparaissent davantage comme les détenteurs, maîtres des données et dossiers personnels, que comme les dépositaires d'informations que leur soumettent ou leur confient des patients, eux-mêmes souvent confrontés à des difficultés pour accéder à leur dossier. Pourtant, le secret médical est inopposable au patient. Le malade doit au contraire être informé des examens et traitements qui lui sont proposés pour obtenir son consentement libre et éclairé et la loi Kouchner<sup>10</sup> lui a reconnu un droit d'accès direct aux informations et données le concernant<sup>11</sup>.

Le Haut comité pour la transparence et l'information sur la sûreté nucléaire a souligné la nécessité d'engager une réflexion sur la transparence dans le secteur médical et la qualité de l'information apportée aux patients, qu'il s'agisse d'information préalable à un traitement, d'information sur la dosimétrie et d'information en cas d'incident. Dans son rapport « Transparence et secrets dans le domaine nucléaire », il pointe en particulier la question des données de dosimétrie et du dossier médical du travailleur exposé à des ambiances de rayonnement<sup>12</sup>. Du fait que l'exposition médicale et l'exposition professionnelle relèvent de deux univers sans lien et de cadres réglementaires différents, seul le patient peut faire la somme totale de ses expositions. Le code du travail définit des valeurs limites et les conditions de surveillance des travailleurs exposés visant à vérifier le respect de ces limites. Et la possibilité de consulter les données dosimétriques est strictement réglementée<sup>13</sup>. Il peut y avoir contradiction entre la protection au titre du secret médical qui les couvre et la maîtrise de l'exposition individuelle de travailleurs exposés du même coup, par l'effet mécanique de l'augmentation de leurs résultats et du dépassement d'un seuil réglementaire, au risque de la perte de

---

<sup>7</sup> Directive 95/46/CE du 24 octobre 1995 relative à protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

<sup>8</sup> Loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

<sup>9</sup> CADA, Rapport annuel pour 2010, La communication d'un rapport de mesurage sonométrique effectué au domicile de personnes privées, qui comporte des informations relatives à l'environnement, ne peut pour cette raison être refusée que pour les motifs énumérés au II de l'article L. 124-5 du code de l'environnement, parmi lesquels ne figure pas la protection de la vie privée (avis 20101472 du 8 avril 2010).

<sup>10</sup> Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé. Articles L1111-6 et suivants du code de la santé publique.

<sup>11</sup> Sur ces questions, HCTISN, Rapport Transparence et secrets dans le domaine nucléaire – Secret médical et droit d'information du patient, p. 24 et 25 ; Avis du 8 octobre 2009 relatif à l'information des populations et des patients associés aux événements intervenant dans le domaine de la radiologie ou de la médecine nucléaire.

<sup>12</sup> HCTISN – Transparence et secrets dans le domaine nucléaire – Le secret médical des travailleurs face à la radioprotection, p. 36.

<sup>13</sup> Arrêté du 30 décembre 2004 relatif à la carte individuelle de suivi médical et aux informations individuelles de dosimétrie des travailleurs exposés aux rayonnements ionisants.

leur emploi<sup>14</sup>. Ainsi, tandis que les informations dosimétriques servent à la gestion de l'emploi des salariés par la dose, sans ces informations protégées par le secret médical, il est difficile d'assurer le suivi par la dose des personnes susceptibles d'être exposées.

2 – Les contours du secret en matière industrielle et commerciale sont plus difficiles à tracer pour deux raisons. En raison d'abord de la multiplicité des objets couverts à propos desquels on peut tout de même se référer à une typologie de la CADA. Il s'agit 1/ de procédés - données relatives aux techniques de fabrication, aux propriétés de matériels, par exemple la puissance d'une antenne de radio-émission ; 2/ des informations économiques et financières - déclarations de produits mis sur le marché ; 3/ des données sur les stratégies commerciales - procédés d'extraction de matières premières, coûts. En raison surtout du régime juridique de la possession applicable à tous les éléments et objets de secret, qu'ils soient corporels (locaux, outils, stocks, hardware) ou immatériels (savoir-faire technique et renseignements non divulgués au sens de l'article 39-2 de l'accord sur les ADPIC). Le fait de se les réserver et le pouvoir discrétionnaire de ne pas révéler, ainsi le choix de ne pas breveter, les précautions et dispositifs concrets de sécurisation prévalent sur le titre et les preuves de la propriété.

L'objet du secret industriel et commercial, proprement indéfini par la loi, répond à des fins d'appropriation et de protection de biens matériels et immatériels contre l'usurpation ou la publication. Il s'entend de manière subjective, extensive et pragmatique. Tout ce dont un commerçant industriel fabricant, promoteur, distributeur, investisseur, « se réserve » physiquement et contractuellement la maîtrise et qu'il décide de ne pas révéler ou divulguer peut être considéré comme secret et confidentiel. La teneur, l'effectivité et la portée du secret industriel et commercial procèdent de la volonté des opérateurs économiques, de l'intérêt de l'entreprise et du pouvoir des dirigeants de ne pas dévoiler - au public en général ou à des tiers dans des relations d'affaires - des éléments de toute nature, physique, tels des locaux et sites d'exploitation, installations et appareils, stocks, équipements et aménagements, et incorporelle, qu'il s'agisse de procédés techniques, informations financières et méthodes commerciales, listes de prospects, contrats et comptes-rendus, données ou projections chiffrées.

S'agissant de biens incorporels, d'informations et connaissances, de fichiers numérisés, du savoir-faire et des résultats non appropriés - i.e. non constitués en biens intellectuels par un titre de propriété industrielle ou un droit d'auteur acquis sans formalité, la possession, dans sa double composante – *corpus*, maîtrise concrète et *animus domini*, volonté d'appropriation, est caractéristique du secret industriel ou commercial. L'emprise de fait résulte à la fois d'une organisation concrète, de barrières et contrôles d'accès aux installations techniques, aux systèmes d'information et aux supports documentaires par des codes et moyens de cryptage. Dans l'entreprise, la réservation d'informations est le principe, leur publication l'exception. La non mise à disposition du public a une fonction conservatoire et elle présente un intérêt stratégique. Car, au-delà de l'utilité immédiate de la protection de fait consistant à les garder secrets, le détenteur de « renseignements non divulgués »<sup>15</sup> se réserve le choix de leur affectation future et les potentialités de développement économique. Il en organise le maintien secret et la mise à profit par des contrats de transfert de technologie et des clauses de confidentialité.

---

<sup>14</sup> E. Filhol, La centrale, éd. P.O.L., 2010 : « Précision documentaire et poésie de l'écriture pour un premier roman charnel et glaçant sur les intérimaires de l'industrie nucléaire », Télérama radio, L'actualité du poche, 19 octobre 2011.

<sup>15</sup> Selon l'article 39.2 de l'accord sur les ADPIC annexé au Traité de Marrakech (1994) qui impose aux États membres de l'OMC de les protéger, il s'agit de renseignements secrets ou non aisément accessibles, ayant une valeur commerciale parce qu'ils sont secrets et ayant fait l'objet, de la part de la personne qui en a licitement le contrôle, de dispositions raisonnables (...) destinées à les garder secrets. Trois éléments sont caractéristiques : la non publication, la valeur économique et la volonté d'exclusivité.

V. Infra, II, Encadrement juridique du secret industriel et des affaires – Actualité législative.

## II/ Encadrement juridique du secret industriel et des affaires – Actualité législative

Les règles de protection de l'information réservée par des entreprises, qu'elle soit objectivement cachée ou relativement couverte par des clauses de secret, diffèrent selon la nature des atteintes : en matière pénale, en renfort de dispositions peu appropriées aux violations de secrets d'entreprises, une récente proposition de loi réprimant l'atteinte au « secret des affaires » instaurerait une classification « d'informations à caractère économique protégées », sur le modèle du régime du secret-défense ; au civil, le non-respect de conventions de confidentialité dont les excès des effets sont bornés par la jurisprudence française et européenne est, en droit, très difficilement « réparable » et, en fait, irrémédiable.

En droit français, aucun dispositif spécifique ne protège des secrets d'entreprise excepté l'article du code du travail qui punit la violation d'un secret de fabrication par un salarié ou un dirigeant<sup>16</sup>. Ce texte qui ne concerne que les processus de fabrication<sup>17</sup> et ne vise pas les tiers extérieurs à l'entreprise, qu'il s'agisse du public, de clients ou concurrents, est inadapté et en pratique très peu appliqué. Les sociétés victimes d'indiscrétions et d'atteintes fondent leurs poursuites pénales sur les incriminations d'abus de confiance<sup>18</sup> et de violation de secrets professionnels ou de fraude informatique, voire d'espionnage comme dans l'affaire Michelin<sup>19</sup>. En l'espèce, la qualification des actes de livraison d'informations à une puissance étrangère et d'espionnage<sup>20</sup> résultait de celle de la protection des renseignements en cause au titre de secrets de la défense nationale.

Le droit de l'OMC fait obligation aux Etats membres d'élaborer une protection du secret des affaires. L'accord sur les ADPIC<sup>21</sup> leur impose de protéger les renseignements non divulgués en « assurant une protection effective contre la concurrence déloyale », étant précisé à l'article 39.2 de cet accord qu'il s'agit de renseignements secrets ou non aisément accessibles, ayant une valeur commerciale parce qu'ils sont secrets et ayant fait l'objet, de la part de la personne qui en a licitement le contrôle, de dispositions raisonnables (...) destinées à les garder secrets. Trois éléments sont caractéristiques : la non publication, la valeur économique et la volonté d'exclusivité.

La notion de « secret des affaires » est directement liée à la protection de l'intérêt légitime de

---

<sup>16</sup> Code de la propriété intellectuelle, article L 621-1 : « Les peines frappant la violation des secrets de fabrication sont prévues à l'article L. 1227-1 du code du travail ci-après reproduit :

" Le fait pour un directeur ou un salarié de révéler ou de tenter de révéler un secret de fabrication est puni d'un emprisonnement de deux ans et d'une amende de 30 000 euros.

La juridiction peut également prononcer, à titre de peine complémentaire, pour une durée de cinq ans au plus, l'interdiction des droits civiques, civils et de famille prévue par l'article 131-26 du code pénal. "

<sup>17</sup> Entendu comme « tout procédé de fabrication offrant un intérêt pratique ou commercial mis en œuvre par un industriel et gardé secret à l'égard de ses concurrents, Cass. Crim. 29 mars 1935.

<sup>18</sup> Code pénal, Art. 314-1 : *L'abus de confiance est le fait par une personne de détourner, au préjudice d'autrui, des fonds, des valeurs ou un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les rendre, de les représenter ou d'en faire un usage déterminé.*

*L'abus de confiance est puni de trois ans d'emprisonnement et de 375000 euros d'amende.*

<sup>19</sup> Un ancien ingénieur de l'entreprise tente de vendre à son concurrent japonais Bridgestone des secrets d'affaires stratégiques dans un « fichier pouvant conférer à son détenteur cinq ans d'avance technologique » ; les « actifs intellectuels et technologiques qu'il s'était appropriés au sein de la Manufacture de pneumatiques » sont qualifiés de « patrimoine informationnel ». Le 21 juin 2010, le TGI de Clermont-Ferrand le condamne pour simple abus de confiance. En l'espèce, l'espionnage n'est pas retenu. Est-ce que l'atteinte à des données confidentielles concernant des secrets de fabrication et de stratégie copiées sur un disque dur externe, modifiées et actualisées « intéressait ou menaçait la nation » ? Quelle interprétation est faite du critère de susceptibilité d'atteinte à des intérêts fondamentaux de la Nation fondant la classification en secret défense ? Quelle qualification en est donnée à une information stratégique ? (V. Infra, IV et V).

<sup>20</sup> Code pénal, Art. 411-6 : *Le fait de recueillir ou de rassembler, en vue de les livrer à une puissance étrangère, à une entreprise ou organisation étrangère ou sous contrôle étranger ou à leurs agents, des renseignements, procédés, objets, documents, données informatisées ou fichiers dont l'exploitation, la divulgation ou la réunion est de nature à porter atteinte aux intérêts fondamentaux de la nation est puni de dix ans d'emprisonnement et de 150 000 euros d'amende.*

<sup>21</sup> Accord sur les droits de propriété intellectuelle intéressant le commerce annexé au Traité de Marrakech de 1994.



l'entreprise et reconnue comme telle par le droit communautaire et, en droit français, par le code de commerce et les règles procédurales devant l'Autorité de la concurrence<sup>22</sup> dont le rapporteur général peut refuser la consultation ou la communication de pièces mettant en jeu ce secret<sup>23</sup>. Pour autant, il n'existe pas de définition du secret industriel et commercial dans la législation ou la réglementation française<sup>24</sup>. Faisant suite à plusieurs initiatives<sup>25</sup> du député B. Carayon<sup>26</sup>, la proposition de loi adoptée le 23 janvier 2012<sup>27</sup> complète le code pénal par un paragraphe « De l'atteinte au secret des affaires des entreprises » très largement défini<sup>28</sup> et spécialement réprimé<sup>29</sup>. Ce sont des « informations (...), quel que soit leur support, les procédés, objets, documents, données ou fichiers, de nature commerciale, industrielle, financière, scientifique, technique ou stratégique, ne présentant pas un caractère public, dont la divulgation non autorisée serait de nature à compromettre gravement les intérêts de cette entreprise en portant atteinte à son potentiel scientifique et technique, à ses positions stratégiques, à ses intérêts commerciaux ou financiers ou à sa capacité concurrentielle, et qui ont, en conséquence, fait l'objet de mesures de protection spécifiques destinées à informer de leur caractère confidentiel et à garantir celui-ci ». Dans cette définition, on trouve, autrement formulés, deux des critères caractérisant les renseignements non divulgués dans l'accord sur les ADPIC, auxquels les États membres de l'OMC doivent – comme pour les données communiquées aux pouvoirs publics - assurer une protection effective contre la concurrence déloyale : à savoir, le caractère secret - non généralement connu de personnes appartenant aux milieux qui s'occupent normalement du genre de renseignements en question ou ne leur sont pas aisément accessibles -, et la valeur commerciale qui en résulte. Le troisième critère - des dispositions raisonnables prises par la personne qui en a le contrôle, destinées à les garder secrets - revêt une tout autre portée dans la proposition relative à des « mesures de protection

---

<sup>22</sup> Sur les relations entre transparence, concurrence et secret industriel et commercial, Intervention de Marie-Dominique Hagelsteen, présidente de la section des Travaux publics en Conseil d'État, Les 30 ans de la loi du 17 juillet 1978, Conférence-débat du 2 juillet 1978..

<sup>23</sup> Article L463-4 : *Sauf dans les cas où la communication ou la consultation de ces documents est nécessaire à l'exercice des droits de la défense d'une partie mise en cause, le rapporteur général de l'Autorité de la concurrence peut refuser à une partie la communication ou la consultation de pièces ou de certains éléments contenus dans ces pièces mettant en jeu le secret des affaires d'autres personnes. Dans ce cas, une version non confidentielle et un résumé des pièces ou éléments en cause lui sont accessibles.*

<sup>24</sup> HCTISN, Rapport transparence et secrets, p. 35. Les difficultés induites par l'absence de définition du secret industriel et commercial :

Si certains ne manqueront pas de souligner l'intérêt qui peut être attaché à l'absence de définition réglementaire, s'agissant de notions évolutives, car cela permet de faire varier les interprétations en fonction des circonstances, cette absence de définition reste source d'incertitudes et d'applications pas toujours homogènes ou cohérentes.

En outre, certaines informations au sein des entreprises ne sont pas jugées suffisamment protégées dans le sens où il n'existe pas toujours d'infraction qui permette de réprimer leur divulgation. Le gouvernement prépare d'ailleurs un projet de loi qui créerait une nouvelle catégorie d'informations protégées au titre d'un « secret des affaires ».

<sup>25</sup> Proposition de loi AN n°1754, 17 juin 2009, pour la performance de la sécurité intérieure ; une précédente proposition de loi AN n° 1611, déposée le 13 mai 2004, était restée sans suite. Elle visait « *des informations ne constituant pas des connaissances générales pouvant être facilement et distinctement constatées par le public, susceptibles d'être sources, directement ou indirectement, d'une valeur économique pour l'entreprise et pour la protection desquelles leur détenteur légitime a pris des mesures* ».

<sup>26</sup> « Le député qui s'affiche comme le spécialiste de l'intelligence économique », [www.larevueparlementaire.fr](http://www.larevueparlementaire.fr)

<sup>27</sup> Inspirée de l'« Economic Espionage Act », dit « Cohen Act » américain de 1996 (18 USC § 1831-1839) sur la préservation des secrets d'affaires, le texte a fait l'objet d'observations critiques : Ch. Le Stanc, Une protection pénale du secret des affaires ?, Prop. Ind. Octobre 2009, p. 1.

<sup>28</sup> Code pénal, Art. 226-15-1. – *Constituent des informations protégées relevant du secret des affaires d'une entreprise, quel que soit leur support, les procédés, objets, documents, données ou fichiers, de nature commerciale, industrielle, financière, scientifique, technique ou stratégique, ne présentant pas un caractère public, dont la divulgation non autorisée serait de nature à compromettre gravement les intérêts de cette entreprise en portant atteinte à son potentiel scientifique et technique, à ses positions stratégiques, à ses intérêts commerciaux ou financiers ou à sa capacité concurrentielle, et qui ont, en conséquence, fait l'objet de mesures de protection spécifiques destinées à informer de leur caractère confidentiel et à garantir celui-ci.*

*Ces mesures de protection spécifiques, prises après une information préalable du personnel par le représentant légal de l'entreprise ou par toute personne qu'il aura préalablement désignée par écrit et destinées à garantir la confidentialité des informations, sont déterminées par décret en Conseil d'État.*

<sup>29</sup> « Art. 226-15-2. – *Le fait de révéler à une personne non autorisée à en avoir connaissance, sans autorisation de l'entreprise ou de son représentant, une information protégée relevant du secret des affaires de l'entreprise, pour toute personne qui en est dépositaire ou qui a eu connaissance de cette information et des mesures de protection qui l'entourent, est puni d'une peine d'un an d'emprisonnement et de 15 000 euros d'amende.*



spécifiques destinées à informer de leur caractère confidentiel et à garantir celui-ci », lesquelles mesures restant à déterminer par décret en Conseil d'État. L'exposé des motifs annonce : « on retrouve là une rédaction assez analogue à celle qui, par son caractère englobant, définit avec efficacité le secret de la défense nationale et se fonde sur trois éléments constitutifs : un objet assez large ; l'absence de publicité autour de ces informations ; l'existence de mesures prises par leur détenteur afin d'en préserver le caractère confidentiel ».

Il est ainsi clairement fait référence aux mesures de classification du secret-défense et le nouveau dispositif prétend à une même exhaustivité<sup>30</sup>. Et, à l'instar du formalisme qui caractérise le régime du secret défense avec l'apposition de la marque d'un type de classement<sup>31</sup>, il est prévu un marquage par un cachet « confidentiel entreprise ». Un procédé d'estampillage permettrait ainsi aux entreprises de classer « secret des affaires » n'importe quel support, fichier et dossier. Et, en l'absence de toute définition objective du secret des affaires, il faut considérer que la teneur des informations couvertes relèverait d'un arbitraire, au demeurant assez peu différent de la possession qu'exercent en fait aujourd'hui les entreprises de leurs données et résultats pour s'en réserver la maîtrise et l'exclusivité. A ceci près que la révélation non autorisée d'une information relevant d'un tel secret serait punie d'un an d'emprisonnement et de 15 000€ d'amende.

A ce jour, il n'existe donc pas de disposition spécifique en vigueur pour le secret des affaires qui est beaucoup plus large que le savoir-faire industriel et la technologie innovante de l'entreprise. Et, de par sa nature privative, le secret industriel et commercial est objectivement indéterminé. Il peut s'agir d'une note interne sur l'état d'une infrastructure ou de ses projets stratégiques - de fusion, cession ou reprise d'une activité ou de la mise sur le marché d'un produit -, aussi de fichiers, contrats, méthodes de gestion. Comment garantir et se prévaloir du secret pour tous ces éléments ? La maîtrise de l'information et des résultats qui dépend de l'organisation concrète de l'inaccessibilité, autrement dit du secret, résulte par ailleurs de l'aménagement conventionnel de la confidentialité pour en assurer la sauvegarde. Or les clauses de confidentialité créent une indisponibilité d'origine contractuelle d'éléments d'information telle que, pour limiter la portée excessive des obligations de ne pas divulguer, les tribunaux les soumettent à un contrôle de proportionnalité de l'engagement souscrit avec les intérêts en cause et peuvent les juger nulles.

En dépit du caractère indéfini des éléments et informations dont une entreprise se réserve la maîtrise et l'exclusivité, la détermination de ce qui est secret s'impose néanmoins à l'égard des salariés et vis-à-vis de tiers. Le secret industriel et commercial est relativement circonscrit dans les conventions qui engagent, d'une part, en interne, le personnel, d'autre part des prestataires et partenaires extérieurs à l'entreprise. Les premiers et les seconds sont tenus à une obligation de confidentialité dont l'objet, la teneur du secret, est aussi difficile à appréhender dans les contrats de travail, notamment par des clauses de non-concurrence, qu'à stipuler dans les relations et les contrats d'affaires<sup>32</sup>. Des clauses générales et spécifiques visent expressément une durée d'interdiction, des conditions et circonstances d'utilisation. Mais à trop couvrir par l'obligation de secret ou à tout ranger dans le champ du confidentiel, le risque est en effet de ne rien vraiment protéger ou, au contraire, à trop préciser les éléments relevant du secret, l'écueil est de ne pas en

---

<sup>30</sup> Ces deux dispositifs se fondent sur des dispositions suffisamment exhaustives dans leur formulation pour saisir, dans toute sa complexité, le concept d'« information à caractère économique protégée » et éviter toute interprétation *a contrario*. Au demeurant, ces dispositions se présentent comme suffisamment précises pour permettre la protection des informations à caractère économique protégées grâce à une mise en œuvre effective des sanctions dont celle-ci dépend en précisant l'objet et les supports de ce type de données et d'informations.

<sup>31</sup> La classification des documents a été étendue à des « lieux auxquels il ne peut être accédé sans que, en raison des installations ou des activités qu'ils abritent, cet accès donne par lui-même connaissance d'un secret » par l'article 75 de l'arrêté du 23 juillet 2010 portant approbation de l'instruction générale interministérielle sur la protection du secret de la défense nationale.

<sup>32</sup> Du latin, *scernere*, écarter, le secret connu d'un nombre limité de personnes est caché des autres, du public. Et le terme affaires sous-tend la valeur et la recherche du gain dans des échanges commerciaux.

identifier les aspects déterminants ni les facteurs d'évolution ou de modification. Le secret ainsi convenu et circonscrit a une portée limitée et une efficacité contingente<sup>33</sup>.

Dans l'entreprise, certaines catégories d'informations spécialement protégées par la loi n'en sont pas moins soumises à des obligations de confidentialité – les données à caractère personnel et les secrets protégés par des dispositions d'ordre public. Ainsi, des données transmises à un établissement financier sont couvertes par le secret bancaire de même que toutes celles confiées à un professionnel tenu au secret, commissaire aux comptes, avocat, notaire, expert-comptable.

---

<sup>33</sup> CA Paris, 27 novembre 2009, SA Sylvius c. SAS Philips Fr. Voir infra, L'encadrement jurisprudentiel du secret. Sur le contrat comme « outil visant à organiser des obligations dites de confidentialité ou de secret, lire Latreille A., Réflexion critique sur la confidentialité dans le contrat, Petites affiches 7 août 2006, N° 156, p. 4.

### III/ Légitimité et opposabilité de secrets d'entreprise dans les dispositifs de transparence en matière nucléaire – Limitations de la portée des clauses de confidentialité en droit commun

Le secret qui interdit l'accès à l'information va à l'encontre des obligations de transparence et de communication qui pèsent sur les entreprises à des fins de contrôle et de surveillance, qu'il s'agisse de sécurité, de réglementation boursière, de règles de concurrence et de transparence des marchés et des concentrations économiques<sup>34</sup> ou de la lutte contre le blanchiment d'argent. Les secrets opposés au public par leur détenteur font échec à la liberté d'accéder à des documents administratifs et aux obligations légales de publication. La question de la confrontation des préoccupations de confidentialité avec l'objectif participatif et les devoirs d'information du public en matière environnementale, en particulier dans le cadre de la loi TSN<sup>35</sup>, a été examinée dans la communication *Transparence et secrets privés* lors du Colloque du CREDESPO, Transparence et environnement - Réflexions théoriques et casuistique du nucléaire français, qui s'est tenu à Dijon le 22 mars 2012.

Avant d'en résumer les principaux éléments, citons, pour « planter le décor », quelques-uns des propos d'experts qui ont participé en 2005 aux débats sur l'EPR et sur les déchets nucléaires<sup>36</sup>, de Corinne Lepage et d'un témoin intervenant à la Conférence des 30 ans de la loi du 17 juillet 1978<sup>37</sup>.

*« Secret commercial ou industriel, secret financier, secret médical... sans oublier le secret défense, le plus "méchant" de tous ! L'accès à certains dossiers s'avère aujourd'hui encore difficile. D'autant qu'il peut arriver que nous ne connaissions même pas l'existence d'un dossier. Et dans ce dernier cas, comment demander à le consulter ? (...) La transparence produit une sensation biaisée. En donnant des informations sur le moindre incident dans les installations nucléaires, on peut laisser croire que le nucléaire souffre d'une mauvaise gestion. C'est pourquoi certains acteurs estiment que la diffusion d'informations peut susciter des craintes. L'IRSN a adopté une position claire : il est préférable d'informer la population, même sur des sujets sensibles comme les accidents nucléaires, plutôt que de laisser planer une suspicion de dissimulation, voire de mensonge. Aujourd'hui de nombreuses informations sont disponibles. Toutefois, l'idée que le nucléaire est opaque est encore fortement ancrée dans les esprits. En dehors d'événements radiologiques très médiatisés, on observe peu de réactions du public pour ces informations »<sup>38</sup>.*

*« La question du secret industriel, dans le domaine santé/environnement, revêt une importance toute particulière. En effet, vus l'organisation actuelle de la recherche et les moyens dont disposent effectivement la recherche publique et la recherche privée, il est tout à fait clair que l'essentiel de la connaissance la plus fine est dans le secteur privé ; elle n'est plus dans le secteur public. D'où la question très précise de savoir quelle possibilité d'accès est réservée aux études dans le domaine de la santé et de l'environnement, lorsque ces études appartiennent à des entreprises privées. Ce problème s'est concrètement posé dans le domaine des organismes génétiquement modifiés, pour lequel la directive 2001-18, de manière dérogatoire dans son article 25, exclut l'application du secret industriel en ce domaine. La commission d'accès aux documents administratifs a appliqué cette disposition pour reconnaître un droit à l'information, qui s'est heurté au refus de*

---

<sup>34</sup> CE 13 févr. 2006, Société Fiducial Informatique, G. P. 31 août 206, N° 243, p. 19 : « Les investigations auxquelles se livre le Conseil de la concurrence pour apprécier la portée économique d'une concentration impliquent qu'il prenne connaissance d'informations couvertes par le secret des affaires ».

<sup>35</sup> Loi n° 2006-686 du 13 juin 2006 relative à la transparence et à la sécurité en matière nucléaire.

<sup>36</sup> Marguerite Boutelet, Note sur les parcours professionnels et politiques des experts participant aux débats publics sur l'EPR et sur les déchets nucléaires, V. Infra, en fin du texte « Transparence et secrets privés », Annexe IV, p.22.

<sup>37</sup> CADA, Les 30 ans de la loi du 17 juillet 1978, Conférence-débat du 2 juillet 2008,

<sup>38</sup> Didier Champion, directeur de l'environnement et de l'intervention de l'IRSN et Monique Sené, vice-présidente de l'Association nationale des commissions locales d'information, ANCLI. IRSN, Magazine Repères n°3, Septembre 2009.

*l'administration de communiquer les documents*<sup>39</sup> ».

« En ce qui concerne le secret professionnel, un point délicat est soulevé dans le jugement du Conseil d'Etat du 21 mai 2008<sup>40</sup> : plusieurs communes demandent la communication des copies de déclaration de taxes générales sur les activités polluantes. Mais, en l'absence de « dérogation législative expresse », le secret professionnel des agents des douanes fait obstacle à la communication des déclarations à des tiers. Et le juge de lui-même ne se reporte pas au code de l'environnement qui ne retient pas l'obstacle du secret professionnel »<sup>41</sup>.

Les secrets privés ont cependant perdu tout caractère absolu face aux impératifs participatifs et aux obligations d'information : les entreprises ne peuvent opposer le secret industriel et commercial à l'administration et/ou au public qu'à des conditions légales précises (1). D'autre part, les tribunaux en contrôlent les effets en limitant la portée des clauses de confidentialité (2).

1 - Limitant la transparence environnementale, les secrets privés sont envisagés comme des motifs légaux de refus de communiquer dans les dispositifs d'accès aux documents administratifs et d'information en matière environnementale et nucléaire. Restreignant les droits du public, ils sont tout de même encadrés. En droit commun administratif, le droit d'accès des citoyens aux documents s'exerce sous réserve de la protection des secrets visés à l'article 6 de la loi du 17 juillet 1978 et sous l'autorité de la CADA qui est également compétente en matière d'accès à l'information relative à l'environnement et en matière nucléaire.

La CADA a érigé une doctrine<sup>42</sup> au travers de nombreux avis et dans les travaux publiés à l'occasion des 30 ans de la loi du 17 juillet 2008<sup>43</sup>. Dans le cadre des demandes d'accès aux documents relatifs à des marchés publics, les documents d'ordre privé confiés à l'administration pour l'instruction de

---

<sup>39</sup> Corinne LEPAGE, Le régime de communication des informations relatives à l'environnement : bilan critique et perspectives d'évolution, CADA, Les 30 ans de la loi du 17 juillet 1978, Conférence-débat du 2 juillet 2008.

<sup>40</sup> Ministre du budget contre Communauté d'Aurillac, n° 306.138.

<sup>41</sup> Témoignage d'une personne responsable de l'accès aux documents administratifs, Le secret en matière industrielle et commerciale, CADA, Les 30 ans de la loi du 17 juillet 1978, Conférence-débat du 2 juillet 2008.

<sup>42</sup> La question de la portée du secret industriel et commercial et de son opposabilité à toute personne exerçant le droit d'accès à des documents administratifs en application de la loi du 17 juillet 1978 se pose dès lors que l'administration est dépositaire d'informations non divulguées et relevant comme telles du secret d'entreprises et des affaires.

Dans son **rapport d'activité pour 2008, (Première partie, Questions de droit abordées en 2008, Analyse des décisions, p 31)**, c'est notamment à propos des documents administratifs liés aux contrats de commande publique que la CADA a élaboré une doctrine visant à établir l'équilibre entre l'obligation de transparence et de communication de toutes les informations détenues par une personne publique - ou une personne privée délégataire en charge de la gestion d'un service public - et les dérogations tenant à la protection, entre autres secrets de tiers visés à l'article 6 de la loi de 1978, des informations couvertes par le **secret en matière industrielle et commerciale**.

La commission indique les catégories de données et informations couvertes par le secret en matière industrielle et commerciale des candidats à la passation d'un contrat de commande publique, non communicables aux tiers et devant donc être occultées préalablement à la communication des documents liés à un marché.

Une fiche thématique sur *Les documents couverts par le secret en matière industrielle et commerciale* précisant que la notion recouvre trois catégories de données indique que « la communication des documents contenant des informations dont la divulgation pourrait porter atteinte au secret industriel et commercial est réservée aux seuls intéressés ».

Toutefois, il semble que cette « doctrine » n'ait pas cours en matière environnementale, dans « le cas des installations nucléaires de base et des installations classées pour la protection de l'environnement ». En effet, lorsque l'accès s'exerce dans le cadre des dispositions « du chapitre tendant à protéger la santé humaine et l'environnement contre les risques qui peuvent résulter des substances et préparations chimiques » issues de l'ordonnance n° 2009-229 du 26 février 2009 prise pour l'application de l'article 12 de la loi n° 2008-757 du 1er août 2008 relative à la responsabilité environnementale et à diverses dispositions d'adaptation au droit communautaire dans le domaine de l'environnement, il n'appartient pas à l'administration de soustraire à la communication et donc de déterminer quelles sont les données et informations secrètes.

<sup>43</sup> Les 30 ans de la loi du 17 juillet 1978, Conférence-débat du 2 juillet 2008.

dossiers de réponses à des appels d'offres deviennent des documents administratifs communicables à toute personne qui en fait la demande après occultation des mentions couvertes par le secret industriel et commercial<sup>44</sup>. Comme le sont, en matière environnementale et nucléaire, les dossiers et les pièces de demandes d'autorisations d'installations classées<sup>45</sup> ou d'émissions de rejets. Mettant en balance les intérêts respectivement attachés à la communication et au refus motivé par le secret industriel et commercial, la Commission a par exemple considéré que les comptes-rendus de visites sanitaires réalisées par les agents sanitaires apicoles comprenaient bien des informations relatives à l'environnement mais que la divulgation des pratiques des ruchers et des appréciations portées sur celles-ci par l'administration ne présentent pas un intérêt suffisant pour justifier leur communication et constituaient des mentions dont la communication porterait atteinte aux secrets protégés par l'article 6-II de la loi du 17 juillet 1978<sup>46</sup>. On voit par cet exemple comment elle exerce son arbitrage pour concilier les contraintes des entreprises et le respect du principe de transparence.

Concernant le contrôle de produits et les substances chimiques, la procédure de l'article L. 521-7 du code de l'environnement oblige l'entreprise à revendiquer le secret industriel et commercial sur des données précises et à en justifier<sup>47</sup>. Il incombe en premier lieu à la personne ayant transmis à l'autorité administrative des informations, d'une part, d'indiquer celles de ces informations qu'elle considère comme commercialement sensibles, dont la diffusion pourrait lui porter préjudice ; d'autre part, de fournir à l'appui de sa demande des justifications à l'autorité qui en apprécie le bien-fondé. En second lieu, dans le cas où l'autorité administrative a reconnu les informations « revendiquées » comme relevant effectivement du secret industriel et commercial, elle prend toutes dispositions utiles pour que ces informations ne soient accessibles qu'aux personnes habilitées – celles qu'elle a désignées et qui sont astreintes au secret professionnel. Et la loi du 13 juin 2006 relative à la transparence et à la sécurité en matière nucléaire dont l'article 19 institue un droit d'accès à divers documents et rapports, limité et mis en échec par les secrets opposés par l'exploitant d'une INB, impose pareillement que le refus de communication soit justifié.

2 - En droit commun, dans les relations qu'elles entretiennent à l'extérieur et en interne avec leur personnel, les entreprises soumettent leurs partenaires contractuels et leurs salariés à des clauses et chartes de confidentialité qui créent non seulement des obligations de ne pas divulguer mais aussi – à l'instar de clauses d'inaliénabilité – une réelle indisponibilité des informations généralement très

---

<sup>44</sup> À l'exclusion des pièces que s'est procurées l'Autorité de la concurrence par le biais de saisies judiciaires, les documents produits ou reçus par cette autorité administrative dans le cadre des affaires qu'elle examine constituent en principe des documents administratifs qui, une fois qu'ils ont perdu leur caractère préparatoire (soit à compter de l'intervention de la décision), et sous réserve qu'ils soient achevés et que leur divulgation ne porte pas atteinte au bon déroulement d'une procédure juridictionnelle en cours ou d'opérations préliminaires à celle-ci, sont communicables à toute personne qui en fait la demande, après occultation des mentions couvertes par le secret en matière commerciale et industrielle ou mettant en cause la protection de la vie privée, en application des dispositions combinées des articles 2 et 6 de la loi du 17 juillet 1978. Ainsi le résumé d'une opération de reprise ou de cession d'une société ne contenant ni informations confidentielles ni secret d'affaires est communicable à toute personne en faisant la demande, en application de l'article 2 de cette loi. En revanche les autres éléments du dossier de notification de la reprise ou de cession et ses annexes relèvent, soit du secret des informations économiques et financières, soit du secret des stratégies commerciales, protégés par le II de l'article 6 de ladite loi, et ne sont donc pas communicables (avis 20101787 du 3 juin 2010).

<sup>45</sup> Code de l'environnement, article 515-8.

<sup>46</sup> Les comptes rendus de visites sanitaires apicoles réalisés par les agents sanitaires apicoles, qui portent sur l'état sanitaire des colonies d'abeilles dans le département, contiennent des informations relatives à l'environnement, au sens des articles L. 124-1 et suivants du code de l'environnement. Toutefois, les mentions dont la communication porterait atteinte aux secrets protégés par le II de l'article 6 de la loi du 17 juillet 1978, notamment du fait de la divulgation des pratiques des ruchers et des appréciations portées sur celles-ci par l'administration, ne présentent pas un intérêt suffisant pour justifier leur communication (avis 20104558 du 2 décembre 2010).

<sup>47</sup> V. *Infra*, Texte de l'article L.521-7 du code de l'environnement et analyse du dispositif, M. Barré-Pépin, L'opposabilité des secrets privés en matière environnementale.

largement couvertes par ces engagements. En pratique, les obligations de secret et de discrétion résultent de clauses de non-concurrence et de stipulations signalant des documents, données et renseignements confidentiels comme tels au moment de leur transmission et précisant qui est qualifié pour transmettre et recevoir des informations confidentielles. En raison de la portée indéfinie ou illimitée – quant à la teneur des secrets stipulés et/ou à la durée, les clauses impliquant la non-révélation d'informations sont soumises à un contrôle de proportionnalité de l'engagement souscrit avec les intérêts en cause. Et les exemples de décisions de nullité ou d'inopposabilité de telles clauses et chartes de confidentialité se multiplient.

Le secret des affaires n'est pas absolu. Il ne peut pas s'imposer à des co-contractants de manière arbitraire, par l'effet de clauses de confidentialité injustifiées ou illimitées. Il ne peut leur être opposé que s'il est légitime et licite. En ce qui concerne les clauses de non-concurrence, la doctrine de la divulgation inévitable de ses connaissances et d'un savoir-faire par un ancien salarié tempère son obligation de ne pas en faire usage. Et la jurisprudence judiciaire relative aux obligations de secret et de confidentialité dessine un régime comparable au dispositif du code civil relatif aux clauses d'inaliénabilité dans les libéralités<sup>48</sup>. Pour être valides, ces clauses qui dérogent au principe de la libre disposition des biens et privent le propriétaire légataire ou donataire de l'attribut essentiel de son droit doivent être limitées dans le temps et justifiées par un intérêt légitime. S'agissant de biens immatériels tels qu'une information ou un savoir-faire, les libertés d'entreprendre et d'expression sont également en jeu.

Dans un arrêt rendu par la Chambre sociale le 8 décembre 2009<sup>49</sup>, la Cour de cassation apprécie de la sorte la licéité d'un dispositif d'alerte que la société aurait par ailleurs dû déclarer à la CNIL. À propos d'un code de conduite des affaires élaboré en 2004 puis en 2007 par la société Dassault systèmes<sup>50</sup> organisant un dispositif d'alerte et définissant les règles applicables dans le groupe à la diffusion des « informations confidentielles » et des informations à « usage interne » dont les salariés pouvaient avoir connaissance dans le cadre de leur contrat de travail, il est jugé que « les informations à usage interne dont la divulgation était soumise à autorisation préalable par le code de conduite ne faisant pas l'objet d'une définition précise, il était impossible de vérifier que cette restriction à la liberté d'expression était justifiée par la nature de la tâche à accomplir et proportionnées au but recherché et d'autre part que l'exercice du droit d'expression directe et collective des salariés pouvait impliquer l'utilisation de certaines de ces informations ».

---

<sup>48</sup> Article 900-1 alinéa 1<sup>er</sup> : *Les clauses d'inaliénabilité affectant un bien donné ou légué ne sont valables que si elles sont temporaires et justifiées par un intérêt sérieux et légitime. Même dans ce cas, le donataire ou le légataire peut être judiciairement autorisé à disposer du bien si l'intérêt qui avait justifié la clause a disparu ou s'il advient qu'un intérêt plus important l'exige.*

<sup>49</sup> (N° 08-17191), D. 2010, p. 548, I. Desbrats : Les chartes éthiques et codes de conduites : des normes privées sous surveillance judiciaire renforcée.

<sup>50</sup> À la suite et sur le modèle de la loi fédérale américaine «Sarbanes-Oxley Act» de 2002 sur la réforme de la comptabilité des sociétés cotées et la protection des investisseurs imposant de nouvelles règles de transparence financière.

#### **IV/ Souveraineté, principe de territorialité du brevet et stratégies de secret industriel ou dépôt – Régime de la brevetabilité - publicité officielle des titres après mise au secret des inventions déposées et exercice d'un droit de regard par l'autorité militaire.**

Pour tous les opérateurs, les organismes de recherche publique tels que le CEA ou leurs filiales de valorisation et les sociétés privées, il existe une option résultant de choix et contraintes stratégiques, bien souvent aussi de l'histoire ou d'une culture d'entreprise, entre déposer une demande de brevet pour une invention et en garder le secret<sup>51</sup>. Le brevet impose le respect de formalités et il est assorti d'une publicité qui le rend opposable aux tiers. C'est un titre officiel de propriété industrielle conférant un monopole d'exploitation territorial et temporaire<sup>52</sup> qui fait entrer de manière définitive et universelle la connaissance technique dans l'état de la science. Le secret en revanche exige l'organisation concrète et conventionnelle du silence. Il procure une protection de fait par l'ignorance, voire la dissimulation et la désinformation. Il permet de conserver une avancée technologique en attendant de décider de l'exploiter ou de la transmettre mais il peut aussi inciter à l'espionnage, à des fraudes et vols, et il fait risquer que des concurrents brevètent et protègent légalement une invention déjà existante.

Le titre de brevet est un instrument de communication assurant la diffusion des inventions. À cet égard, l'option en faveur du brevet d'un produit ou procédé innovant est antinomique du secret car elle implique la description de l'invention couverte par un titre officiel et sa publication par l'INPI ou un autre office national, ou pour un dépôt international, l'OEB (Office européen de brevet à Munich) ou l'OMPI (Office mondial à Genève). La documentation technique, juridique et commerciale que les instituts nationaux et internationaux de propriété industrielle ont pour mission de mettre à la disposition du public est le principal outil de veille technologique à l'échelle mondiale. L'intelligence économique - dont il est question de réglementer l'exercice à titre privé et principal<sup>53</sup> - a au contraire pour objet la recherche et le traitement d'informations non disponibles.

Le choix de déposer une demande de brevet à l'office du ou des pays où l'exclusivité est recherchée en contrepartie de la publication de l'invention vaut allégerance pour l'octroi, aux conditions fixées par les lois nationales, du titre conférant un droit exclusif d'exploitation d'une portée limitée aux territoires des Etats visés<sup>54</sup>. La souveraineté de l'État français se manifeste notamment par la mise au secret temporaire et prorogable<sup>55</sup> dont fait l'objet toute invention pour laquelle une demande de

---

<sup>51</sup> Dans la maîtrise de résultats de la recherche et des innovations technologiques, l'appropriation sert à acquérir une chose et à jouir des droits qu'implique sa possession. Dans le cas du savoir scientifique et technique, la possession est fragile tandis que l'appropriation permet d'orienter son développement, de récupérer et d'utiliser ses résultats pour satisfaire des besoins propres. Or la divulgation des informations scientifiques et techniques nuit à la maîtrise de leur destination ou de leurs applications. Parmi les différents outils utilisés pour empêcher ou officialiser cette divulgation, les titres de propriété industrielle sont des instruments essentiels d'appropriation des résultats du travail scientifique et technique, c'est-à-dire des créations de l'industrie.

<sup>52</sup> Au terme de la durée légale de vingt ans, l'innovation est dans le domaine public : elle peut être librement exploitée, sans autorisation du titulaire du monopole de brevet qui peut auparavant la céder ou en concéder des utilisations.

<sup>53</sup> « Consistant à rechercher et traiter des informations non directement accessibles au public et susceptibles d'avoir une incidence significative pour l'évolution des affaires », l'intelligence économique est définie par l'article 33-1 du projet LOPSI présenté en conseil des Ministres le 27 mai 2009 (V. Annexe, page 9) qui en réglemente l'activité, (Obs. S. Lavric, D. 2009, Act. Lég. 404 ; Thibault du Manoir de Juaye, Intelligence économique et secret des affaires : le point des juristes, Cah. Dr. Entr., sept-oct. 2008, p. 29).

<sup>54</sup> Le titre de brevet confère dans le pays où il est octroyé, l'usage exclusif, la fabrication et la commercialisation du produit ou procédé correspondant à l'invention décrite et revendiquée, ainsi que le droit d'en concéder l'exploitation.

<sup>55</sup> Selon l'article L. 612-8 du code de la propriété intellectuelle, l'autorité militaire a un droit de regard sur les inventions déposées ; l'article L. 612-9 pose une interdiction générale de divulguer et exploiter quelle qu'invention que ce soit en l'absence d'autorisation et les demandes de brevets sont mises au secret pendant un délai de 5 mois au terme duquel elle est accordée de plein droit sauf prorogation par le Ministre de la Défense pour un an renouvelable (Art. L. 612-10),



brevet est déposée à l'INPI. Toute prétention au brevet d'une invention comprenant sa description et des revendications est portée à la connaissance de l'autorité militaire et soumise au contrôle préalable du Ministre chargé de la Défense qui, habilité à prendre connaissance des demandes auprès de l'INPI, à titre confidentiel, peut la maintenir au secret et la classer secret défense<sup>56</sup>. Les détenteurs d'une innovation sont donc tenus au secret de la défense nationale quand ils déposent des demandes brevets. Ainsi, paradoxalement, au moment où un opérateur privé ou public fait le choix de ne pas garder secret le nouveau produit ou procédé qu'il détient et de publier des résultats innovants pour s'en faire délivrer le titre d'exclusivité, la technologie revendiquée tombe sous le coup d'une interdiction générale et provisoire de divulgation et d'exploitation. L'inventeur empêché d'exploitation commerciale et de mise à disposition du public de l'invention peut théoriquement prétendre à une indemnisation de son préjudice. L'invention peut alors faire l'objet d'un changement de destination en cas d'expropriation pour les besoins de la défense nationale<sup>57</sup>. La pratique de la procédure de classification des inventions permet d'appréhender la place du secret dans les domaines scientifiques et techniques<sup>58</sup>.

Au cours d'un entretien conduit en avril 2011 au siège d'un important groupe industriel de chimie français, une personne travaillant au Département de propriété industrielle<sup>59</sup>, mandataire européen, a fait part de son expérience à la Direction Générale de l'Armement où, embauchée avec l'habilitation secret défense, elle a commencé sa carrière, et des conditions dans lesquelles sont sélectionnés les brevets en vue de leur soumission à des comités d'experts du Ministère de la Défense en vue d'une éventuelle classification. Affectée pendant trois ans et demi à la DRETE (Direction Recherche et Études technologiques), une des neuf directions spécialisées, la plus « en amont », son rôle consiste à « mettre les inventions au secret » en travaillant dans une tour sécurisée. Après sélection des dossiers de demande de brevets par l'INPI où deux pièces sont affectées au ministère de la Défense, elle les présélectionne en vue de la classification « secret défense » par les scientifiques du contingent, l'objectif étant d'empêcher que des informations sensibles ne sortent de France<sup>60</sup>. Une centaine d'experts interviennent dans un des neuf services spécialisés, dont la DRETE<sup>61</sup>. Comme les autres délégués des Directions, elle retient les dossiers à l'aide des mots-clés pour lesquels ils ont des consignes, avant que cinq ou six experts ne les réexaminent et ne les classifient. « Dès qu'on voyait des mots comme CEA, on sélectionnait ». Au bilan, 5 % environ des demandes sont sélectionnées et 1 à 2 % sont classifiées à différents niveaux : les experts se rendent dans les locaux de l'INPI, où une pièce est affectée au Ministère de la Défense. Personne ne peut y entrer, sauf les délégués chargés de

---

auquel cas le demandeur peut demander à être indemnisé de son préjudice ; à défaut d'accord amiable, l'indemnité est fixée par le Tribunal de Grande Instance.

L'administration peut exproprier à tout moment pour les besoins de défense nationale (Art. L.613-20) ou obtenir une licence d'office (Art. L. 613-19).

<sup>56</sup> Code de la propriété intellectuelle, Article L. 612-8.

<sup>57</sup> Selon les propos recueillis lors de l'entretien présenté ci-après, « il n'y a jamais de demande d'indemnisation, alors que le code de la propriété intellectuelle en prévoit la possibilité ».

<sup>58</sup> Blandine Laperche observe que la majorité des demandes de brevet maintenues au secret concernent des réalisations industrielles dans le domaine des armements et fréquemment financées par le Ministère de la Défense. Ainsi, les inventions d'origine française mises au secret appartiennent en 1979 pour 74% au CEA, pour 20% à l'État français par le biais de ses agents inventeurs, pour 5% à des industriels et pour 1% à des inventeurs indépendants.

V. « Les inventions, la science et la guerre : la place du secret », Innovations 1/2005 (N° 21), p. 109-143.

<sup>59</sup> Corinne Delprat, chimiste de formation, diplômée du CEIPI (Strasbourg) en Brevets d'Invention, a son premier poste à la DGA (Direction Générale de l'Armement) où elle doit "sélectionner" les demandes de brevet à soumettre à des experts pour leur éventuelle classification SD.

<sup>60</sup> Des peines de 10 à 15 ans de détention criminelle et de 150 000 à 225 000 € sont encourues pour livraison ou permission d'accès à une puissance étrangère ou organisation sous contrôle étranger de renseignements ou documents dont l'exploitation est de nature à porter atteinte aux intérêts fondamentaux de la nation (Code pénal, articles 411-6 et 7).

<sup>61</sup> Informatique, Télécommunications, Optique, Chimie, Biologie, Armes Terrestres, Missiles Espace, Chantiers Navals et Mission Atome où, commente-t-elle, « un vieux monsieur, salarié du CEA, (était) un peu juge et partie ! ».

repérer les éléments intéressants. « Ils ont tendance à ‘ratisser large’ ».

Selon la responsable du Département de Propriété industrielle de la même société, physicienne dans la spécialité Atomique et Nucléaire longtemps chercheur au CEA dans le Département de protection contre les rayonnements puis gestionnaire des brevets et de contrats dans le domaine nucléaire à la société BREVATOME<sup>62</sup>, il faut distinguer le secret défense afin d’éviter la communication d’information et la sortie de données sensibles à l’étranger et le droit de préemption pour l’Armée, avec les licences obligatoires. On reformule et on redessine. Par exemple, « il ne faut pas qu’il y ait d’élément en forme d’ogive, alors on fait une forme de diabolo ! ». Elle précise cependant que les experts des directions opérationnelles interviennent avec rigueur. « Le classement conforte la sécurité ». Les ingénieurs de l’armement – les X – se connaissent tous et travaillent à huis clos pour la préemption. Evoquant la stratégie de classification, elle précise que, pour sa part au CEA, l’objectif étant d’éviter une préemption, « on faisait tout pour que ce ne soit pas classifié. Par exemple, s’agissant de demandes de brevet sur des drones, le mot était écarté en accord avec le CEA. Il fallait faire une gymnastique et sur un sujet comme le Cadmium Mercure, c’était une torture... ».

« On classe à juste titre - les choses sensibles - les éléments dont l’armée peut avoir besoin ou pourra avoir besoin - les dépôts attachés à un marché public de recherche du Ministère de la Défense. Après trois ans, on faisait tout pour déclassifier ; si on déclassifiait dans les trois semaines on publiait et l’invention entrait « dans l’état de la science ». Sinon, c’était plusieurs années après : ce qui était sensible ne l’était alors plus nécessairement. La responsable du Département de propriété industrielle illustre son propos avec des expériences de retrait de brevet sur des longueurs d’ondes sensibles, suivi d’un nouveau dépôt de demande pour un redéveloppement. Elle évoque le cas des collaborations CEA/Thomson : le CEA préfère protéger puis discute avec Thomson la question de l’exploitation. Il faut une autorisation du Ministère de la Défense pour donner licence de brevets CEA à Thomson, société pourtant classifiée qui fabriquait pour les Etats-majors. « Au CEA, on fait toujours de la recherche pour la Défense Nationale (de sorte que), les retours sur investissement, c’est ‘peanuts’ ! Il y a une entrave à l’exploitation, d’où le risque de ne plus faire de recherche à même d’intéresser la défense nationale ».

L’interlocutrice s’exprime sur les **stratégies de secret et de brevet du groupe**, en matière de nanotechnologies innovantes. En pratique, « des personnes viennent voir la société avec un papier ou un dossier. Il faut faire une présentation et procéder à la description de leur invention. On ne brevète que si on a des chances d’exploiter ». Et le secret n’est ici que territorial : « dans l’hypothèse de la construction d’une usine ailleurs, en Chine ou en Inde, donc avec d’autres matériaux et d’autres fournisseurs, impliquant l’obligation de dire ce qu’on allait faire, il devient nécessaire de breveter, de laisser publier et de faire une extension (à l’étranger). On publie pour être libre d’exploiter ; c’est une garantie, une sorte de label que ce n’est pas secret-défense ». Elle évoque ensuite le cas de la protection des procédés : pendant très longtemps, on ne les protégeait pas par des brevets et ils n’étaient mis en œuvre que par celui qui en avait eu l’idée. Ce qui pose certains problèmes, comme celui de la contrefaçon : il y a dépôt de plainte, mais avec renversement de la charge de la preuve. Car il faut aussi avoir les moyens de détection de la contrefaçon de procédés ; en France, depuis 1996, avec le renversement de la charge de la preuve, c’est au défendeur de montrer qu’il n’utilise pas le procédé en cause. En pratique, comme on a une meilleure connaissance de l’état de la science qu’eux, on procède à des actions en invalidation des brevets des tiers devant les offices et auprès des

---

<sup>62</sup> D’abord chez L’Oréal puis en Cabinet libéral, elle intervient pour le CEA, avec l’habilitation secret-défense après enquête familiale, renouvelée lors de son mariage ; elle effectue des stages à Saclay ; travaille sur des dossiers confidentiels (entre autres, de détecteurs de radars) chez Brevatome, filiale du CEA créée pour gérer la propriété industrielle, les contrats et les brevets, regroupant Framatone, Rhône-Poulenc, EDF et d’autres industriels autour de la « gestion nucléaire ».

tribunaux ; ou à des oppositions ; aux Etats-Unis, ce doit être en réplique à des menaces.... ».

« Il n’y a pas alternative mais coexistence entre informations secrètes et brevets ». « Qu’il s’agisse de mesures test sur des matières premières, polymères ou produits réfrigérants – ces nouveaux produits vendus aux équipementiers pour la climatisation des automobiles -, on fait très attention à ce qu’on publie : il y a les choses obligatoires et celles qui peuvent se retourner contre nous. Car tout le business peut s’arrêter. Dans la publicité vers les clients et dans les déclarations sur nos sites et aux administrations, une grande attention est portée à la présentation de nos informations ». « Dans les documents de presse sur un réfrigérant, par exemple, on a recours à un brevet allemand mais on évite d’en mentionner certaines utilisations ; l’industriel qui attaque est en train de monter une usine en Chine sur laquelle on a des informations. Les documents de presse peuvent être utilisés par un concurrent. Beaucoup de secret(s) industriel(s) donne(nt) lieu à des informations orales ». « Par ailleurs, de nombreux contrats sont passés, mais dont on ne peut pas toujours en assurer le respect. Enfin il est fait état du problème du respect du secret par des anciens ingénieurs : un collaborateur étranger peut aisément faire une synthèse, ce qu’un français ne peut pas faire au Japon où il est procédé à une division, un fractionnement, entre le début et la fin d’un processus. Cela relève de la culture d’entreprise ».

L’entretien a montré les **recoupements** - et l’articulation qui est faite - du secret industriel et du secret défense en Recherche & Développement - dans les stratégies de traitement des demandes, de gestion et de défense de brevets. « Rien ne sort de chez nous sans être lu et relu ». « La violation du secret défense donne lieu à des sanctions pénales ; pour le secret industriel, il n’y a rien : il n’y a pas d’autre procédure que celle que l’industriel met en place. Il est possible cependant de recourir aux clauses du droit du travail et à la mise en jeu de la responsabilité civile de l’employé. Dans l’affaire Renault<sup>63</sup>, il y a eu une descente de la DGA chez Martine Planche, directeur de l’INPI ». On peut conclure que, « de la part de la DGA, il s’agit de surveiller largement des données sensibles qui évoluent avec la technique, alors que pour Brevatome ou Brevallex, il y a de la part de l’industriel une stratégie d’esquive du risque de classification ».

---

<sup>63</sup> L’affaire Renault a défrayé la presse en 2011. Trois cadres du Technocentre de développement des nouveaux véhicules du groupe de Guyencourt avaient été licenciés « pour des faits très graves nuisant à l’intérêt de l’entreprise et qui menaçaient des actifs stratégiques ». Le constructeur s’estimant victime de divulgations d’informations sur les coûts et l’architecture de la voiture électrique, une plainte contre X visant « la fourniture d’éléments intéressant le secret économique français à une puissance étrangère » avait été portée près du Parquet de Paris « pour des faits constitutifs d’espionnage industriel, de corruption, d’abus de confiance, de vol et recel, commis en bande organisée ». Officiellement saisie de l’enquête, la DCRI (Direction centrale du renseignement intérieur) les a innocentés. A l’origine des accusations d’espionnage, le responsable de la sécurité de Renault, un ancien militaire, qui aurait été en contact avec une mystérieuse source, rémunérée à hauteur de plusieurs centaines de milliers d’euros, a finalement été mis en examen et incarcéré pour escroquerie touchant le constructeur.

## **V/ Technologie et dualité d'applications militaire/civile - Intelligence économique, Patrimoine et Potentiel Scientifique et Technique (PST), objet commun du secret défense et du secret industriel**

L'analogie entre secret militaire et secret industriel tient à l'identité de contexte conflictuel des deux types de secret et de leurs objectifs respectifs, la guerre et la compétition économique avec armes de guerre, supériorité et atouts concurrentiels, stratégies offensives et de défense. Il y a aussi un rapprochement, voire une confusion d'objets dans le domaine de la recherche et du développement technologique où une part croissante de la recherche civile nationale est potentiellement une recherche de guerre. Tout au cours de l'histoire, science et guerre se sont mutuellement stimulées. Ce sont les besoins de guerre qui ont favorisé le développement de la science, en finançant les scientifiques et en fournissant des problèmes concrets à résoudre. L'utilisation du savoir n'est pas immédiatement marchande ; l'invention est d'abord et avant tout strictement militaire<sup>64</sup>. Et l'innovation technologique, qu'elle fasse l'objet d'un titre officiel de propriété industrielle ou d'une réservation de fait par le secret, est à la fois un atout concurrentiel, un avantage dans la compétition économique, et, en particulier dans le domaine nucléaire, un facteur de risques tels que l'exposition et la contamination à la radioactivité<sup>65</sup> ainsi qu'un enjeu stratégique dont les pouvoirs publics doivent assurer un suivi et le contrôle.

Les technologies duales peuvent faire l'objet d'usages et d'applications tant militaires – guerre, moyens de destruction et/ou de dissuasion - que civiles - y compris armements et toutes autres. Les secteurs industriels concernés sont l'espace, l'électronique, l'informatique, l'aéronautique et le nucléaire ; également, la cartographie, les données océanographiques<sup>66</sup> ; et les télécommunications marquées par la récente libéralisation du régime de la cryptologie auparavant restreinte à des usages militaires et diplomatiques, littéralement science du secret et technique de chiffrement des messages<sup>67</sup>.

---

<sup>64</sup> « Le pouvoir politique, pour gagner les guerres, a toujours eu recours aux connaissances scientifiques et/ou techniques disponibles et cherché à les appliquer à son objectif. Mais pour surprendre l'adversaire, dans une démarche offensive ou défensive, la divulgation des connaissances ou des informations scientifiques et techniques doit être empêchée. Le secret, défini comme un ensemble de connaissances, d'informations qui doivent être réservées à quelques uns et que le détenteur ne doit pas révéler, est alors le médiateur des relations entre la science et la guerre ». Blandine Laperche, « Les inventions, la science et la guerre : la place du secret, Innovations 1/2005 (n° 21), p. 109-143.

<sup>65</sup> « Les catastrophes artificielles sont filles du progrès » - navire et naufrage, train et déraillement, avion et crash, atome et Tchernobyl, catastrophe génétique ; les accidents sont « inventés avec la substance du progrès technique ».

<sup>66</sup> Sur les technologies duales, v. François Lefaudeux, 10 janvier 2008, Nucléaire civil et militaire, Livre blanc Défense et sécurité nucléaire 2008, Ch. VI, L'industrie et la recherche où il est fait mention de sept secteurs de priorités technologiques et industrielles à objectifs stratégiques de sécurité nationale.

<sup>67</sup> Loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, Article 30 :

*I. - L'utilisation des moyens de cryptologie est libre.*

*II. - La fourniture, le transfert depuis ou vers un Etat membre de la Communauté européenne, l'importation et l'exportation des moyens de cryptologie assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont libres.*

*III. - La fourniture, le transfert depuis un Etat membre de la Communauté européenne ou l'importation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont soumis à une déclaration préalable auprès du Premier ministre, sauf dans les cas prévus au b du présent III. Le fournisseur ou la personne procédant au transfert ou à l'importation tiennent à la disposition du Premier ministre une description des caractéristiques techniques de ce moyen de cryptologie, ainsi que le code source des logiciels utilisés. Un décret en Conseil d'Etat fixe :*

*a) Les conditions dans lesquelles sont souscrites ces déclarations, les conditions et les délais dans lesquels le Premier ministre peut demander communication des caractéristiques du moyen, ainsi que la nature de ces caractéristiques ;*

*b) Les catégories de moyens dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, leur fourniture, leur transfert depuis un Etat membre de la Communauté européenne ou leur importation peuvent être dispensés de toute formalité préalable.*

*IV. - Le transfert vers un Etat membre de la Communauté européenne et l'exportation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont soumis à autorisation du Premier ministre, sauf dans les cas prévus au b du présent IV. Un décret en Conseil d'Etat fixe :*

*a) Les conditions dans lesquelles sont souscrites les demandes d'autorisation ainsi que les délais dans lesquels le Premier*

En ce qui concerne le nucléaire, « les questions nucléaires d'aujourd'hui découlent peu ou prou de ce double usage qui a été fait de l'énergie nucléaire depuis qu'elle a reçu une application militaire et économique<sup>68</sup> ». La recherche et la technologie nucléaires sont initiées, orientées et conduites par le CEA, Commissariat à l'énergie atomique et aux énergies alternatives, pour être développées dans des industries de défense et des industries civiles, notamment de production d'énergie – les centrales, INB – et de santé publique – radiothérapie.

Dès lors que et partout où sont en jeu la sécurité intérieure ou extérieure de l'Etat et des intérêts fondamentaux de la nation, le secret industriel et commercial relève aussi du secret-défense avec lequel il se confond alors. Les questions nucléaires revêtent un caractère stratégique pour la France comme pour chaque grand pays qui procède méthodiquement à des réévaluations de « posture nucléaire », militaire ou civile, politique ou industrielle, légale ou morale. Les activités industrielles, scientifiques et économiques du secteur entrent dans la nomenclature des informations et technologies sensibles concernant la sécurité nationale, qu'il s'agisse d'armement, d'énergie, de composants et matériaux, du tissu industriel du secteur et bien entendu des installations nucléaires, INB (installations nucléaires de base) soumises au classement ICPE<sup>69</sup> et à autorisation au titre de la protection de l'environnement de la prévention des risques<sup>70</sup> et INBS (installations nucléaires de base secrètes) régies par le code de la défense.

Dans les domaines scientifique, technique et économique, les ministres responsables ont le devoir de définir, à l'usage des citoyens, ce qui doit être protégé. Les « hauts fonctionnaires défense et de sécurité » (HFDS) des ministères sont responsables de la sécurité défense des sites et installations industriels. Sous leur autorité et celle des fonctionnaires de défense et de sécurité (FDS) correspondants du secteur para administratif ou privé, ce devoir incombe aux entreprises publiques ou privées, détentrices à un titre ou à un autre de secrets de la défense nationale. Plus largement, la mission de protection du FDS<sup>71</sup> concerne des intérêts fondamentaux pour la Nation, qui touchent à la sauvegarde du patrimoine scientifique et économique, et à la défense et la sécurité publique, dans le périmètre d'activité d'un établissement. Dans la pratique, cela se traduit ainsi par une activité de veille, de sensibilisation, d'information, d'expertise, voire de contrôle.

Un entretien du 5 mai 2011 avec Gilles Bertrand<sup>72</sup>, Directeur du Laboratoire Interdisciplinaire Carnot de Bourgogne – ICB (UMR 5205) - sur le secret défense et secret industriel dans les coopérations de recherche avec le CEA Valduc montre comment les règles propres aux deux types de secret s'appliquent aux chercheurs du laboratoire universitaire et quelles sont les pratiques de confidentialité au CEA de Valduc et dans d'autres centres CEA. L'ICB collabore avec différents CEA et plusieurs équipes<sup>73</sup> sur des sujets très divers, tant pour la Direction des Applications Militaires (DAM) du

---

*ministre statue sur ces demandes ;*

*b) Les catégories de moyens dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, leur transfert vers un Etat membre de la Communauté européenne ou leur exportation peuvent être soit soumis au régime déclaratif et aux obligations d'information prévus au III, soit dispensés de toute formalité préalable.*

<sup>68</sup> Jean Dufourcq, Les Cahiers de la Revue Défense Nationale, N° Hors Série sept. 2010 ( [www.defnat.com](http://www.defnat.com) )

<sup>69</sup> Installations Classées pour la Protection de l'Environnement, (Article R. 511-9 du Code de l'environnement - version consolidée mars 2011).

<sup>70</sup> Articles L. 511-1 à 1 et suivants du code de l'environnement.

<sup>71</sup> La responsabilité de cette protection relève du directeur général et de la ligne managériale (directeurs d'entité). Le FSD est là pour les aider à faire face à ces responsabilités et à conduire les actions appropriées.

<sup>72</sup> Professeur de chimie-physique, Président de l'Université de Bourgogne (1988-1993).

<sup>73</sup> Le LaBoMaP (EA 3634, Laboratoire bourguignon des matériaux et procédés), l'IMB (UMR CNRS 5584, Institut de Mathématiques de Bourgogne) et l'ICMUB (UMR CNRS 5260, Institut de Chimie Moléculaire de Bourgogne). D'autre part, l'ICB appartient à la Fédération de Recherche – Structure fédérative 2604 Mathématiques, Matière et Matériaux - M3 – avec le CEA Valduc qui en est membre.

Valduc que pour les départements civils (de Grenoble et Marcoule) avec lesquels sont passés des contrats d'assistance et des contrats d'études. Il s'agit de travaux d'intérêt scientifique général et de collaborations de nature industrielle. Et il en va de même avec la Direction Générale de l'Armement (DGA). Les recherches de l'ICB portent sur des sujets proposés par le CEA Valduc, la DGA et les entreprises et elles font généralement l'objet de publications conjointes. Il n'y a pratiquement pas de brevets déposés par l'ICB.

Le secret défense (SD) s'impose exceptionnellement et formellement à des chercheurs de l'ICB pour certains travaux dont le Directeur n'a pas à connaître. Seuls trois ou quatre membres de l'ICB habilités SD sont directement concernés parmi lesquels le conseiller scientifique de la culture au Valduc. De nombreux sujets de thèses et d'études revêtent un caractère sensible à raison de leurs évidentes applications militaires potentielles dont l'ICB n'a pas connaissance mais que des spécialistes peuvent apprécier en « lisant entre les lignes » des sujets<sup>74</sup>. En revanche, tous les sujets et tous les contrats industriels relèvent de l'Intelligence économique<sup>75</sup>. Et l'ICB fait l'objet d'un contrôle rigoureux et les interventions de la Direction Centrale du Renseignement Intérieur (DCRI) y sont fréquentes. Et le Haut fonctionnaire de défense et sécurité (H.F.D.S.) intervient à raison de risques d'atteinte au patrimoine scientifique et technique (PST) dans les échanges internationaux. Ainsi le F.D.S. du CNRS a prononcé des rejets de candidatures à l'ICB pour des étudiants iraniens.

En amont du patrimoine industriel des entreprises partenaires et commanditaires couvert par des mesures concrètes de maintien au secret et des conventions ou clauses de confidentialité, la recherche scientifique publique et son développement technologique « constituent » d'abord le patrimoine scientifique et technique (P.S.T.) de la nation dont la protection est fondamentale pour la sécurité et la défense de l'État<sup>76</sup>. Selon le Ministère de l'Enseignement Supérieur et de la Recherche (MESR) qui en définit la teneur<sup>77</sup>, la protection du patrimoine scientifique et technique, quand bien même elle ne relève pas de la réglementation du secret défense, n'en dépend pas moins de l'Esprit de Défense et Sécurité<sup>78</sup>. Et l'ICB est un laboratoire classifié (E.R.R.) - Établissement à Régime Restrictif - à des fins de protection du patrimoine scientifique et technique. L'accès y est effectivement limité et l'entrée dans les locaux de l'ICB contrôlé par un système électronique de cartes magnétiques et d'interphone. La sécurité informatique y est très importante : selon le Directeur G. Bertrand, le Système de Sécurité de l'Information (SSI) est à l'origine de lourdeurs, de tensions internes entre les chercheurs ou de difficultés avec l'administration universitaire. La classification<sup>79</sup> des laboratoires publics<sup>80</sup> en trois

---

<sup>74</sup> Tels que « Études de corrosion en brouillard salin » - concernant à l'évidence des applications militaires, au milieu et aux engins sous-marins ; ou les applications TRICIUM dans le cadre du projet « Laser-Mégajoule » de Bordeaux.

<sup>75</sup> Pour autant, Gilles Bertrand dit avoir toujours été favorable à une « recherche ouverte », tant pour les thèses que dans les conventions partagées, affirmant clairement la nécessité pour les chercheurs de l'ICB de publier les résultats de leur travaux et pour les doctorants de ne pas être entravés dans leurs candidatures et leurs projets par des exigences de confidentialité.

<sup>76</sup> V. Infra Annexe II – La recherche publique et la protection du PST dans les échanges internationaux.

<sup>77</sup> « Le patrimoine scientifique et technique (P.S.T.) englobe nombre d'informations de toute nature, qui prises individuellement, ne présentent pas nécessairement de caractère secret mais dont l'ensemble constitue dans des domaines déterminés de l'activité scientifique et technique de notre pays des secteurs sensibles pour lesquels il faut envisager des règles de protection adaptées ». V. Protection du patrimoine scientifique et technique et intelligence économique, page du site du MESR : reproduite en Annexe III ci-après.

<sup>78</sup> V. Infra, Annexe II in fine - Esprit de défense et de sécurité.

<sup>79</sup> Au sens de l'instruction générale interministérielle 486/SGDN relative à la protection du patrimoine scientifique et technique français dans les échanges internationaux et dont résulte la classification des laboratoires de recherche publics.

<sup>80</sup> La recherche publique est réalisée, en France, par les organismes de recherche et les universités.

De grands organismes, généralistes ou spécialisés, à forte visibilité internationale, contribuent à la Recherche en France. Ils comprennent, en dehors de quelques fondations et instituts particuliers (Pasteur, Curie) :

- des établissements publics à caractère scientifique et technologique (E.P.S.T.) dont les personnels ont le statut de fonctionnaires : le C.N.R.S. pour la science fondamentale, l'Inserm pour la santé, l'INRA pour l'agronomie en sont quelques exemples ;

catégories comprend : les E.R.R., ainsi définis « établissements dont l'activité justifie l'existence d'un régime d'accès réglementé et dont l'application peut concerner tout ou partie de l'établissement - il s'agit d'établissements effectuant des travaux de recherche, de développement, de fabrication ou de maintenance, et dont la divulgation sans contrôle à des étrangers serait contraire aux intérêts fondamentaux de la Nation » ; les E.A.S. (établissement à accès surveillé) et les E.R.O. (établissements à régime ordinaire). La liste des E.R.R et des E.A.S. est arrêtée par le SGDN et la liste des E.R.R est elle-même classifiée secret-défense. Visant à moderniser les outils de protection du potentiel scientifique et technique contre les risques de captation et de détournement, le décret du 2 novembre 2011 définit désormais une **catégorie particulière de zones protégées, les zones à régime restrictif**<sup>81</sup>.

Le secret industriel et le secret défense (SD) sont soumis à des règles fondamentalement différentes. Ils obéissent à des logiques et des pratiques différenciées. L'exemple de l'ICB montre pourtant comment les questions de confidentialité et les préoccupations de défense du patrimoine – aujourd'hui potentiel - scientifique et technique (PST) se cumulent et se confondent. La « protection de notre capacité à nous défendre » et « la protection de notre compétitivité économique » sont les enjeux communs de la protection des résultats scientifiques et techniques de la recherche publique française. Significativement, les dispositifs ne protègent plus le patrimoine mais le potentiel scientifique et technique de la nation. Spécialement dans les relations avec l'étranger, les aspects de défense et sécurité et ceux de propriété et secret industriels sont également des objectifs de la protection d'intérêts fondamentaux de la nation. L'intelligence économique<sup>82</sup> ressortit de chacune de ces logiques et la Direction centrale du renseignement intérieur (DCRI) du Ministère de l'Intérieur est logiquement conviée dans les affaires d'espionnage industriel et de renseignement économique. Des dispositions relatives aux « Atteintes aux intérêts fondamentaux de la nation » et à l'espionnage introduites dans le code pénal en 1995 permettent théoriquement d'alourdir les peines et les amendes des personnes qui portent atteinte à l'intérêt d'entreprises nationales clés. Les auteurs de faits d'espionnage par « livraison à une entreprise étrangère de renseignements dont l'exploitation et la divulgation sont de nature à porter atteinte aux intérêts fondamentaux de la Nation » encourent quinze ans de détention criminelle et 225 000 euros d'amende<sup>83</sup>. Comme dans l'affaire Michelin<sup>84</sup> où la frilosité du système judiciaire a d'ailleurs été critiquée<sup>85</sup>.

- 
- des établissements publics à caractère industriel et commercial (EPIC) dont les personnels ont le statut de salariés de droit privé, comme le C.E.A. pour l'atome ou le CNES pour l'espace.

<sup>81</sup> Décret N° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique, V. Annexe III.

<sup>82</sup> V. Supra, note 52.

<sup>83</sup> Article 411-6 et suivants, Annexe I - Code pénal, Extraits.

<sup>84</sup> L'ingénieur Marwan Arbache, ancien salarié de la manufacture - qui avait offert en juillet 2007 des informations confidentielles à Bridgestone et était poursuivi pour avoir tenté de vendre un nouveau procédé de fabrication de pneus de poids lourds visant à allonger leur longévité au groupe japonais - est condamné par le Tribunal Correctionnel de Clermont-Ferrand le 21 juin 2010 pour abus de confiance à deux ans de prison avec sursis et à 5 000 euros d'amende (ainsi qu'à 10 000 euros de dommages et intérêts à l'entreprise Michelin). Il est en revanche relaxé des poursuites pour espionnage en l'absence de preuve que les informations proposées « présentaient un caractère à ce point stratégiques », étant jugé que « le seul fait du classement du centre de recherches en établissement à régime restrictif n'induit pas nécessairement que des éléments du potentiel économique de la France, au titre de l'article 410-1 du code pénal, soient concernés ». Les faits ont été déqualifiés en « collecte irrégulière de documents ».

<sup>85</sup> Les difficultés de la justice française à traiter les affaires de renseignement économique, [www.Knowers.org](http://www.Knowers.org), 23 juin 2010. Cette modération de la justice s'inscrit dans une tradition récurrente. Que ce soit dans les procès portant sur des affaires d'espionnage classique, ou des affaires de vols de secret industriel, les juges des tribunaux correctionnels ont toujours fait preuve d'une certaine mansuétude. Contrairement à des pays comme les États-Unis où les auteurs de tels faits sont souvent lourdement condamnés.



## **Annexe I - Articles (extraits) du Code pénal réprimant les atteintes au secret industriel :**

### **LIVRE IV : Des crimes et délits contre la nation, l'Etat et la paix publique**

#### **TITRE Ier : Des atteintes aux intérêts fondamentaux de la nation**

**Article 410-1** : *Les intérêts fondamentaux de la nation s'entendent au sens du présent titre 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.*

#### **CHAPITRE Ier : De la trahison et de l'espionnage ([Article 411-1](#))**

Section 1 : De la livraison de tout ou partie du territoire national, de forces armées ou de matériel à une puissance étrangère ([Articles 411-2 à 411-3](#))

Section 2 : Des intelligences avec une puissance étrangère ([Articles 411-4 à 411-5](#))

#### **Section 3 : De la livraison d'informations à une puissance étrangère**

**Article 411-6** : *Le fait de livrer ou de rendre accessibles à une puissance étrangère, à une entreprise ou organisation étrangère ou sous contrôle étranger ou à leurs agents des renseignements, procédés, objets, documents, données informatisées ou fichiers dont l'exploitation, la divulgation ou la réunion est de nature à porter atteinte aux intérêts fondamentaux de la nation est puni de quinze ans de détention criminelle et de 225000 euros d'amende.*

**Article 411-7** : *Le fait de recueillir ou de rassembler, en vue de les livrer à une puissance étrangère, à une entreprise ou organisation étrangère ou sous contrôle étranger ou à leurs agents, des renseignements, procédés, objets, documents, données informatisées ou fichiers dont l'exploitation, la divulgation ou la réunion est de nature à porter atteinte aux intérêts fondamentaux de la nation est puni de dix ans d'emprisonnement et de 150 000 euros d'amende.*

**Article 411-8** : *Le fait d'exercer, pour le compte d'une puissance étrangère, d'une entreprise ou organisation étrangère ou sous contrôle étranger ou de leurs agents, une activité ayant pour but l'obtention ou la livraison de dispositifs, renseignements, procédés, objets, documents, données informatisées ou fichiers dont l'exploitation, la divulgation ou la réunion est de nature à porter atteinte aux intérêts fondamentaux de la nation est puni de dix ans d'emprisonnement et de 150000 euros d'amende.*

Section 4 : Du sabotage ([Article 411-9](#))

#### **Section 5 : De la fourniture de fausses informations**

**Article 411-10** : *Le fait de fournir, en vue de servir les intérêts d'une puissance étrangère, d'une entreprise ou organisation étrangère ou sous contrôle étranger, aux autorités civiles ou militaires de la France des informations fausses de nature à les induire en erreur et à porter atteinte aux intérêts fondamentaux de la nation est puni de sept ans d'emprisonnement et de 100000 euros d'amende.*

Section 6 : De la provocation aux crimes prévus au présent chapitre ([Article 411-11](#))

#### **CHAPITRE II : Des autres atteintes aux institutions de la République ou à l'intégrité du territoire national**

Section 1 : De l'attentat et du complot ([Articles 412-1 à 412-2](#))

Section 2 : Du mouvement insurrectionnel ([Articles 412-3 à 412-6](#))

Section 3 : De l'usurpation de commandement, de la levée de forces armées et de la provocation à s'armer illégalement ([Articles 412-7 à 412-8](#))

### **CHAPITRE III : Des autres atteintes à la défense nationale**

Section 1 : Des atteintes à la sécurité des forces armées et aux zones protégées intéressant la défense nationale ([Articles 413-1 à 413-8](#))

#### **Section 2 : Des atteintes au secret de la défense nationale**

**Article 413-9 :** *Présentent un caractère de secret de la défense nationale au sens de la présente section les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers intéressant la défense nationale qui ont fait l'objet de mesures de classification destinées à restreindre leur diffusion ou leur accès.*

*Peuvent faire l'objet de telles mesures les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers dont la divulgation ou auxquels l'accès est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale.*

*Les niveaux de classification des procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers présentant un caractère de secret de la défense nationale et les autorités chargées de définir les modalités selon lesquelles est organisée leur protection sont déterminés par décret en Conseil d'Etat.*

**Article 413-10 :** *Est puni de sept ans d'emprisonnement et de 100 000 euros d'amende le fait, par toute personne dépositaire, soit par état ou profession, soit en raison d'une fonction ou d'une mission temporaire ou permanente, d'un procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier qui a un caractère de secret de la défense nationale, soit de le détruire, détourner, soustraire ou de le reproduire, soit d'en donner l'accès à une personne non qualifiée ou de le porter à la connaissance du public ou d'une personne non qualifiée.*

*Est puni des mêmes peines le fait, par la personne dépositaire, d'avoir laissé accéder à, détruire, détourner, soustraire, reproduire ou divulguer le procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier visé à l'alinéa précédent.*

*Lorsque la personne dépositaire a agi par imprudence ou négligence, l'infraction est punie de trois ans d'emprisonnement et de 45 000 euros d'amende.*

**Article 413-11 :** *Est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende le fait, par toute personne non visée à [l'article 413-10](#) de :*

*1° S'assurer la possession, accéder à, ou prendre connaissance d'un procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier qui présente le caractère d'un secret de la défense nationale ;*

*2° Détruire, soustraire ou reproduire, de quelque manière que ce soit, un tel procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier ;*

*3° Porter à la connaissance du public ou d'une personne non qualifiée un tel procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier.*

**Article 413-12 :** *La tentative des délits prévus au premier alinéa de l'article 413-10 et à l'article 413-11 est punie des mêmes peines.*

#### **Section 3 : Des atteintes aux services spécialisés de renseignement**

**Article 413-13 :** *La révélation de toute information qui pourrait conduire, directement ou indirectement, à la découverte de l'usage, en application de l'article L. 2371-1 du code de la défense, d'une identité d'emprunt ou d'une fausse qualité, de l'identité réelle d'un agent des services spécialisés de renseignement mentionnés à l'article 6 nonies de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires ou de son appartenance à l'un de ces services est punie de cinq ans d'emprisonnement et de 75 000 € d'amende. Lorsque cette révélation a causé une atteinte à l'intégrité physique ou psychique à l'encontre de ces personnes ou de leur conjoint ou partenaire lié par un pacte civil de solidarité ou de leurs descendants ou ascendants directs, les peines sont portées à sept ans d'emprisonnement et à 100 000 € d'amende. Lorsque cette révélation a causé la mort de ces personnes ou de leur conjoint ou partenaire lié par un pacte civil de solidarité ou de leurs descendants ou ascendants directs, les peines sont portées à dix ans d'emprisonnement et à 150 000 € d'amende, sans préjudice, le cas échéant, de l'application du chapitre Ier du titre II du livre II. La révélation, commise par imprudence ou par négligence, par une personne dépositaire soit par état ou profession, soit en raison d'une fonction ou d'une mission temporaire ou permanente, de l'information mentionnée au premier alinéa est punie de trois ans d'emprisonnement et de 45 000 € d'amende. Le présent article est applicable à la révélation de toute information qui pourrait conduire, directement ou indirectement, à l'identification réelle ou supposée d'une personne comme source ou collaborateur d'un service spécialisé de renseignement.*

## Annexe II - La recherche publique et la protection du patrimoine scientifique et technique (PST) dans les échanges internationaux<sup>86</sup> [www.enseignementsup-recherche.gouv.fr](http://www.enseignementsup-recherche.gouv.fr)

Les échanges internationaux peuvent revêtir plusieurs formes :

- une coopération scientifique et technique qui est un engagement souscrit conjointement par une autorité ou un établissement français avec un organisme soit étranger, soit international ;
- des séjours de toute durée, effectués en délégation ou à titre individuel dans les organismes et les entreprises du secteur public ou privé ;
- des transferts de technologies impliqués par ces coopérations, séjours et visites ;
- l'accès de chercheurs étrangers non titularisés, à des centres français de recherche scientifique ou des entreprises pour y exercer une activité ;
- l'activité des français à l'étranger à l'occasion de missions d'ordre économique, scientifique et technologique.

Une des missions du *service du H.F.D.S.*<sup>87</sup> est d'assurer une protection efficace de notre patrimoine national, scientifique et technique, en réunissant les garanties optimales compatibles avec le bon fonctionnement des échanges internationaux. *Cette protection est fondamentale pour la sécurité et la défense de l'Etat et les échanges internationaux sont eux aussi absolument nécessaires pour le rayonnement de la France.*

**Les enjeux** - Ils sont nombreux et essentiels.

Premièrement, pour la protection et la sécurité des Français et plus largement de l'Etat :

- la lutte contre la prolifération des armes de destruction massive et de leurs vecteurs (menaces Nucléaire Radiologique Biologique et Chimique et balistique) ;
- la lutte contre le terrorisme ;
- *la protection de notre capacité à nous défendre.*

Deuxièmement, pour la protection de l'homme en tant qu'être humain :

- le respect de la bioéthique.

Troisièmement, pour la protection de l'emploi, des connaissances et de la propriété intellectuelle :

- *la protection de notre compétitivité économique ;*
- la protection des établissements d'enseignement supérieur et de recherche et de leurs personnels.

**La réglementation** - Le cadre juridique dans lequel s'inscrivent les missions de protection du patrimoine scientifique et technique peut être défini à différents niveaux de réglementation internationale, nationale, interministériel et ministériel.

Au plan international, cela se traduit par l'application des traités et conventions internationales telles que les résolutions du conseil de sécurité de l'O.N.U. ou la position commune 2008/652 P.E.S.C. du conseil de sécurité européenne contre les pays proliférants.

Au niveau national, ministériel et interministériel, c'est la mise en œuvre des instructions interministérielles et des circulaires ministérielles relatives à la lutte contre la prolifération, au contrôle des coopérations internationales, au contrôle des visiteurs et stagiaires dans les établissements à régime restrictif (E.R.R.) et aux recommandations pour les Français en mission à l'étranger, ainsi que l'application des articles D.123-15 à D.123-22 du code de l'éducation en matière de coopération d'enseignement supérieur internationale.

**La mise en œuvre - Au niveau interministériel**

Le service participe aux groupes de travail relatifs aux politiques "pays" pilotés par le secrétariat général de la défense et de la sécurité nationale ou par le ministère des affaires étrangères et européennes.

Il participe également à d'autres travaux interministériels, notamment ceux concernant la lutte contre la prolifération ou l'organisation nécessaire pour faire face à une inspection par mise en demeure en France en application de la convention du 13 janvier 1993 sur l'interdiction de la mise au point, de la fabrication, du stockage et de l'emploi des armes chimiques et sur leur destruction.

---

<sup>86</sup> Nous soulignons en italique

<sup>87</sup> Le service du haut fonctionnaire de défense et de sécurité est placé auprès des ministres de l'Education nationale et de l'Enseignement Supérieur et de la Recherche.

La sécurité doit être adaptée aux menaces et aux enjeux pour qu'elle soit source d'efficacité et de sérénité plutôt que d'être une contrainte. Le retour d'expérience montre que les menaces sont bien réelles tant sur nos savoirs-faire, nos systèmes d'information, nos grands équipements, nos agents...

**Au niveau ministériel, M.E.S.R. et M.E.N.** *Le service du H.F.D.S. instruit des milliers de demandes d'accords de coopération internationale, et de demandes de visites et de stages dans les organismes de recherche et les établissements d'enseignement supérieur.*

Les coopérations internationales peuvent impliquer des établissements d'enseignement supérieur entre eux ou des organismes de recherche entre eux ou bien encore diverses combinaisons possibles d'acteurs parmi des structures privées de recherche, des écoles d'ingénieurs, des universités, des organismes de recherche sous tutelle du M.E.S.R. ou bien encore des laboratoires à statut international.

Les demandes de visites et de stages instruites concernent les laboratoires E.R.R.

Au-delà de la diversité apparente de ces demandes multiples, la méthodologie d'instruction, eu égard aux enjeux de la mission de protection du patrimoine scientifique et technique, est, dans les grandes lignes, unique, assurant par là-même une équité dans le traitement des dossiers. Ceux-ci sont étudiés avec une grille de lecture qui analyse le respect des réglementations internationales et des engagements de la France, *les aspects de défense et de sécurité, l'équilibre de la coopération et la prise en compte des questions de propriété intellectuelle.*

Par ailleurs le service du H.F.D.S. est impliqué dans les projets de recrutement de personnels étrangers hors Union européenne.

### **L'intelligence économique « défensive » et « active »**

*Les actions de protection du patrimoine scientifique et technique dans les échanges internationaux sont des actions d'intelligence économique "défensive".*

Le service participe également à l'intelligence économique "active" dans le cadre des groupes de travail interministériels placés sous l'autorité du délégué interministériel à l'intelligence économique.

### **Esprit de défense et de sécurité**

L'esprit de défense et de sécurité n'est pas spontané. Il n'est pas non plus réservé aux militaires. Il repose sur la formation d'un esprit civique et citoyen qui doit être abordée dès l'école et poursuivi dans l'enseignement supérieur.

### **Qu'est-ce que l'esprit de défense et de sécurité ?**

Comme le précise le livre blanc sur la défense et la sécurité nationale : " L'adhésion de la nation est la condition de l'efficacité de l'appareil de défense et de sécurité et de légitimité des efforts qui lui sont consacrés ". Le Livre blanc souligne la nécessité d'investir dans la recherche de haut niveau et les formations supérieures ; c'est le moyen de contribuer à une bonne compréhension de l'appareil de défense et de sécurité par la société.

Quatre axes d'action doivent être privilégiés : la recherche scientifique et technologique, la recherche universitaire en sciences sociales, la formation permanente, la recherche stratégique.

Sans dramatiser les risques encourus, préparer la nation à l'éventualité d'une crise grave, prendre conscience que notre pays peut être la cible d'évènements bouleversant la vie quotidienne des citoyens (tremblements de terre, inondations, actes terroristes..) sont des conditions déterminantes de la capacité de la population à réduire les risques et à faire face aux évènements résiduels.

Le protocole d'accord signé le 31 janvier 2007 entre les ministres de la défense et de l'enseignement supérieur et de la recherche a pour objectif de développer une culture de défense et de sécurité et de renforcer la coopération entre les grandes écoles militaires et les établissements d'enseignement supérieur et de recherche. Il prévoit aussi une coopération pour l'insertion et l'emploi et le développement de la connaissance.

### **Comment se former à l'esprit de défense et de sécurité ?**

Les formations à l'esprit de défense et à la sécurité sont multiples et présentes à tous les niveaux. Afin de faciliter la mise en œuvre des programmes scolaires, des formations à la défense et à la sécurité sont proposées par les instituts de formation des maîtres. Elles sont aussi dispensées dans les universités et instituts universitaires de technologie, soit dans des masters spécialisés ou lors de séminaires et colloques. Ces formations comportent bien souvent un volet défense économique.

Elles sont également proposées aux étudiants et enseignants par l'Institut des Hautes études de la défense nationale (I.H.E.D.N.), l'Institut national des hautes études de la sécurité et de la justice (I.N.H.E.S.J.) et par le Haut comité de la défense civile (H.C.D.C.).

Les enseignants chercheurs, auditeurs de l'I.H.E.D.N., sont invités à soutenir l'action des trinômes académiques pour développer la culture de défense et de sécurité dans l'enseignement secondaire.

### **Annexe III – Dispositions relatives à la protection du potentiel scientifique de la nation et au contrôle de l'accès à des zones à régime restrictif**

**Code pénal, Article 413-7 :** *Est puni de six mois d'emprisonnement et de 7500 euros d'amende le fait, dans les services, établissements ou entreprises, publics ou privés, intéressant la défense nationale, de s'introduire, sans autorisation, à l'intérieur des locaux et terrains clos dans lesquels la libre circulation est interdite et qui sont délimités pour assurer la protection des installations, du matériel ou du secret des recherches, études ou fabrications.*

*Un décret en Conseil d'Etat détermine, d'une part, les conditions dans lesquelles il est procédé à la délimitation des locaux et terrains visés à l'alinéa précédent et, d'autre part, les conditions dans lesquelles les autorisations d'y pénétrer peuvent être délivrées.*

#### **Décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation (J.O. du 4/11/2011)**

**Publics concernés :** *organismes et laboratoires de recherche, universités, grandes écoles, entreprises.*

**Objet :** *protéger le potentiel scientifique et technique de la nation contre des risques de captation ou de détournement.*

**Notice :** *le présent décret vise à moderniser les outils de protection du potentiel scientifique et technique de la nation. Il est pris en application de l'article 413-7 du code pénal et institue une catégorie particulière de zones protégées, les zones à régime restrictif. Il définit les modalités de concertation entre les chefs de service, établissements ou entreprises et les pouvoirs publics.*

Art. 1er. – La section 1 du chapitre III du titre Ier du livre IV de la partie réglementaire du code pénal est complétée par un article ainsi rédigé :

« **Art. R. 413-5-1. – I.** – *Sont dites "zones à régime restrictif" celles des zones, mentionnées à l'article R. 413-1, dont le besoin de protection tient à l'impératif qui s'attache à empêcher que des éléments essentiels du potentiel scientifique ou technique de la nation :*

« *1° Fassent l'objet d'une captation de nature à affaiblir ses moyens de défense, à compromettre sa sécurité ou à porter préjudice à ses autres intérêts fondamentaux ;*

« *2° Ou soient détournés à des fins de terrorisme, de prolifération d'armes de destruction massive et de leurs vecteurs ou de contribution à l'accroissement d'arsenaux militaires.*

« *Les zones à régime restrictif peuvent inclure, dans leur périmètre, des locaux dont la protection renforcée est justifiée par l'entreposage de produits ou par l'exécution d'activités comportant des risques particuliers au regard des impératifs mentionnés aux trois premiers alinéas.*

« **II.** – *Par dérogation aux deux premiers alinéas de l'article R. 413-5, l'accès à une zone à régime restrictif pour y effectuer un stage, y préparer un doctorat, y participer à une activité de recherche, y suivre une formation, y effectuer une prestation de service ou y exercer une activité professionnelle est soumis à l'autorisation du chef du service, d'établissement ou d'entreprise, après avis favorable du ministre chargé d'en exercer la tutelle ou, à défaut de ministre de tutelle, du ministre qui a déterminé le besoin de protection en application de l'article R. 413-2.*

*«La demande d'avis est adressée par le chef de service, d'établissement ou d'entreprise au ministre mentionné au précédent alinéa. Le silence gardé par le ministre au cours des deux mois suivant la réception de la demande vaut avis favorable.*

« *Le refus d'autorisation d'accès n'est pas motivé.*

« **III.** – *Toute personne bénéficiant d'une habilitation au titre de la protection du secret de la défense nationale est réputée avoir obtenu l'avis ministériel favorable mentionné au II.*

« *Les prestataires extérieurs de services relevant de catégories précisées par arrêté du Premier ministre et exerçant leur activité habituelle dans une zone à régime restrictif sont réputés avoir obtenu l'avis ministériel favorable mentionné au II pour accéder, dans les conditions prévues par un contrat de prestation de service, à la zone à régime restrictif.*

« **IV.** – *Dans tous les cas, le chef du service, de l'établissement ou de l'entreprise informe le ministre mentionné au premier alinéa du II de sa décision relative à l'autorisation d'accès. »*

Art. 2. – I. – La protection du potentiel scientifique et technique de la nation est assurée par concertation entre les pouvoirs publics et les chefs des services, établissements ou entreprises dans lesquels :

1° Ont été délimitées une ou plusieurs zones à régime restrictif, en application de l'article R. 413-5-1 du code pénal ;

2° Ou qui abritent une activité exposée aux risques définis au I du même article.