LES ENJEUX DU DROIT DE L'INTELLIGENCE ÉCONOMIQUE POUR LES ENTREPRISES

Olivier de MAISON ROUGE

Avocat, Docteur en droit

Si l'intelligence économique se définit couramment comme étant « *la maîtrise et la protection de l'information stratégique pertinente pour tout acteur économique* »[1], en revanche aucun texte d'origine légale n'est venu régir son contenu, ni même le contour de la matière.

Rappelons néanmoins l'initiative malheureuse, au détour de la loi dite « LOPPSI 2 » du 14 mars 2011, en vue d'encadrer l'activité privée d'intelligence économique qui aurait définie comme « consistant dans la recherche et le traitement d'informations sur l'environnement économique, social, commercial, industriel ou financier d'une ou plusieurs personnes physiques ou morales, destinées soit à leur permettre de se protéger des risques pouvant menacer leur activité économique, leur patrimoine, leurs actifs immatériels ou leur réputation, soit à favoriser leur activité en influant sur l'évolution des affaires ou les décisions de personnes publiques ou privées ». Cette disposition a toutefois été invalidée pour imprécision par le Conseil Constitutionnel[2]. Cela ne signifie pas pour autant, comme l'a souligné Bertrand Warusfel[3] que nous soyons face à un vide juridique sur le sujet.

Pour sa part, « l'intelligence juridique » – qui constitue notre propos – peut se définir, quant à elle, comme étant une démarche polymorphe et transversale d'ingénierie juridique au profit de la stratégie économique de l'entreprise. S'il s'agit d'une matière émergente, encore résiduelle et trop souvent marginale, elle a néanmoins d'ores et déjà gagné ses lettres de noblesse en étant officiellement instituée comme étant une « composante essentielle de l'intelligence économique »[4].

En la matière, la réflexion s'est pour une large partie fixée autour de la conception du patrimoine immatériel de l'entreprise, dans la mesure où il constitue le cœur nucléaire de l'intelligence économique et juridique. Bien que le droit n'ait pas encore donné corps à ce bien immatériel, il en connaît les composantes essentielles dans la mesure où une entreprise se valorise désormais non seulement sur ses stocks et son matériel d'exploitation mais aussi sur ses actifs immatériels, tels que la R&D,

---

[1] www.intelligence-economique.gouv.fr

[2] Conseil constitutionnel, décision n° 2011-625 DC du 10 mars 2011

[3] Warusfel B., « Intelligence économique et pratiques juridiques », in *Revue de l'Intelligence économique*, octobre 1999, n° 5, p.6.

[4] Convention entre la Délégation Interministérielle à l'Intelligence Economique et le Conseil National des Barreaux, du 18 avril 2012.

les fichiers clients ou fournisseurs, les données commerciales stratégiques, les taux de marge, les recettes, les savoir-faire, un organigramme ... même si ces biens sont difficilement quantifiables dès lors qu'il sont souvent couverts par la confidentialité et ne reflètent parfois qu'un potentiel. Un tel patrimoine incorporel est toujours déterminant dans la mesure où il confère à son titulaire un avantage substantiel et décisif sur ses concurrents.

Il nous appartient en conséquence de donner corps juridiquement à ce patrimoine informationnel (**I**) pour ensuite donner une réponse appropriée dans le cadre de sa défense (**II**).

I. Approche du droit de l'intelligence économique

A. Dimension de l'intelligence économique

L'intelligence économique est désormais devenue une réelle préoccupation et un véritable complément efficient dans la prise de décision des dirigeants d'entreprise. Elle participe à la détermination de tout acteur économique pour lui permettre de comprendre et d'anticiper les mutations qui affectent un marché mondial désormais animé par une concurrence exacerbée.

Ce faisant, le positionnement affirmé est d'obtenir l'information grâce à des outils légaux et opérants pour l'exploiter en temps opportun, d'une part et de protéger les données stratégiques détenues par toute structure, d'autre part. C'est pourquoi l'intelligence économique s'appuie *in fine* sur une démarche pluridisciplinaire conduisant à analyser les informations en associant des compétences techniques et des spécialités multiples aussi bien d'ordre économique, commercial, juridique et financière, cette énonciation n'étant pas limitative.

Il est convenu et généralement admis que la matière s'articule autour de trois axes majeurs que sont :

1. La **veille stratégique**, c'est-à-dire la collecte et le récolement des informations économiques stratégiques, à partir de sources ouvertes, en vue de leur interprétation, de leur analyse. Il est souvent affirmé que l'information utile est essentiellement « ouverte », 90 % des données stratégiques sont accessibles sur Internet, dans la presse ou les publications spécialisées, et peuvent également être recueillies dans un cadre légal, éthique et déontologique (colloques, salons, manifestations...).

2. **L'influence**, c'est-à-dire la faculté à orienter positivement les décisions et les textes d'origine légale ou règlementaire ou à déstabiliser un concurrent par le biais d'une communication négative, voire hostile.

3. **La protection économique**, à entendre comme étant la sécurisation, par tous moyens technique et juridique, et la valorisation du patrimoine informationnel qui en constitue le noyau dur.

B. Tentative de définition du patrimoine informationnel de l'entreprise

1. La théorie du patrimoine informationnel de l'entreprise

Si, jusqu'à présent, le Droit connaît et a parfaitement intégré en son sein la notion de patrimoine, il n'en est pas de même concernant l'information elle-même. Et pourtant, cette question centrale et préalable est trop souvent ignorée par les acteurs de l'intelligence économique eux-mêmes.

En effet, le patrimoine informationnel tel que nous l'utilisons dans notre propos est exclusivement composé de biens et de droits incorporels. Cela ne signifie par pour autant que tous les biens et droits immatériels entrent dans ce périmètre. Le droit au bail, les contrats et abonnements, les ondes, l'électricité... pour ne prendre que quelques exemples courants, ne sont pas rattachables à notre objet car, s'ils sont effectivement incorporels, ils ne concourent pas à la composition du patrimoine informationnel car ils ne revêtent pas la notion d'information économique.

Il n'existe à l'heure actuelle pas plus de texte légal en droit positif français définissant précisément le périmètre de la conception pour le moins innovante de patrimoine informationnel qui est une autre universalité de fait, comme jadis pour le fonds de commerce pour en revenir à notre propos introductif de la présente partie.

À cet égard, il nous est d'ores et déjà possible d'affirmer qu'il peut être perçu comme un patrimoine *sui generis*, construit au fur et à mesure par la pratique des affaires, constituant incontestablement une universalité de fait. Alors que le fonds de commerce comprend des biens meubles corporels, pour sa part, le patrimoine informationnel serait exclusivement constitué de biens meubles incorporels.

Ainsi que cela sera démontré ci-dessous, comprenant tant des droits de propriété intellectuelle et/ou industrielle, tels que marques, dessins et modèles et brevets que des biens informationnels et techniques relevant du secret des affaires (compositions organiques, codes source, listing clients, taux de remise commerciale...), une telle entité très diffuse n'a de valeur que pour celui qui a en l'usage pour ses besoins stratégiques propres.

Or, cette nouvelle universalité, si tant est que le patrimoine informationnel soit reconnu comme telle, pourrait donc être assimilée à un bien meuble incorporel, à l'instar du fonds de commerce, mais serait essentiellement composée de secrets d'affaires et de droit de propriété intellectuelle, pris dans un sens large.

Si les auteurs se mettent d'accord pour lui reconnaître une valeur économique, il reste que le droit se refuse obstinément à qualifier les biens informationnels.

2. Consistance du patrimoine informationnel :

En résumé, sans pour autant en faire une vérité juridique absolue, il est possible de schématiser et de conceptualiser la consistance du patrimoine informationnel de la manière suivante :

LES DROITS DE PROPRIÉTÉ INTELLECTUELLE	LES SECRETS D'AFFAIRES
Nature des biens : o marques, o dessins et modèles, o brevets, o certificats d'obtention végétale, o bases de données, … Source : Code de la Propriété intellectuelle **=> COMPOSANTES DU PATRIMOINE INFORMATIONNEL RÉVÉLÉ**	**Nature des biens** : Toute connaissance spécifique tenue secrète, sur tout support, ayant une valeur économique, et protégée, telle que : o informations, données confidentielles, connaissances propres o recette, process, méthodes, o taux de marge, éléments commerciaux et financiers, o savoir-faire, o secrets de fabrication … Source : article 39.2 Traité ADPIC **=> COMPOSANTES DU PATRIMOINE INFORMATIONNEL NON DIVULGUÉ**
→ REPOSENT SUR LA DIVULGATION Par une procédure de dépôt, enregistrement, publication ; Ils confèrent des droits privatifs (monopole d'exploitation), pour une durée limitée dans le temps.	**→ TENUS SECRETS, COUVERTS PAR LA CONFIDENTIALITÉ** Protégés par des moyens de fait à combiner avec des moyens de droit ; leur protection est exclusivement assurée par le secret (pouvoir de fait de son titulaire).

C. Le périmètre du secret des affaires

1. Une absence de définition

Comme cela a été relevé à juste titre par Pol-Droit, « sans le secret des affaires, c'en serait fini de l'industrie, des services, de l'économie »[5]. Il en est ainsi par exemple des célébrissimes secrets de composition des recettes du Coca-Cola ou du Nutella, toujours imitées, mais jamais égalées, permettant à leur titulaire de préserver leur modèle économique.

Or, le secret étant par nature un élément reposant essentiellement sur des comportements factuels, il constitue donc, à l'instar du patrimoine informationnel, ce que nous désignons volontairement par un « objet juridique non identifié ». Cela ne signifie pas pour autant qu'il n'intéresse pas la science juridique. Disons plutôt que c'est le secret, de par sa nature et son essence, qui serait tenté de s'affranchir du droit, dans la mesure où les moyens de protection de fait prévalent sur la sécurité juridique.

À l'exclusion des droits privatifs dûment identifiés, les secrets d'affaires peuvent également revêtir un aspect purement informationnel ou tout autre bien de toute nature, non protégeable. Nous pouvons en conclure, qu'à défaut de protéger par tous moyens de fait ce patrimoine informationnel, notamment par la

[5] Pol-Droit R., « Dangereuse transparence », *Les Échos*, 26 oct. 2011.

confidentialité, le droit ne confère sur cet ensemble de biens immatériels aucun droit de propriété. Cela revient à dire, qu'à l'instar de la clientèle, les biens informationnels n'appartiennent à personne, et donc à tout le monde.

Cette approche serait cependant trop réductrice.

2. Une norme juridique internationale

En effet, en matière de droit commercial, comme en matière de droit de la propriété intellectuelle, les instances internationales ont d'ores et déjà largement appréhendé une telle conception et énoncé ses fondements juridiques.

Ainsi, la propriété intellectuelle fut un des sujets abordés dans le cadre de l'*Uruguay Round* en 1986 au travers des échanges du GATT. À l'issue de ces négociations, il fut établi, puis ultérieurement ratifié par les pays signataires, un accord relatif aux Aspects des Droits de Propriété Intellectuelle liés au Commerce (ou « ADPIC »), lequel était annexé à la Convention de Marrakech en date du 14 avril 1994, instituant l'Organisation Mondiale du Commerce (OMC), dont les règles prévalent aujourd'hui dans le cadre de cette globalisation des échanges parmi les pays membres.

À cet égard, l'article 39.2 de l'accord ADPIC stipule que :

> « Les personnes physiques et morales auront la possibilité d'empêcher que des renseignements licitement sous leur contrôle ne soient divulgués à des tiers ou acquis ou utilisés par eux sans leur consentement et d'une manière contraire aux usages commerciaux honnêtes, sous réserve que ces renseignements :
>
> (a) soient secrets en ce sens que, dans leur globalité ou dans la configuration et l'assemblage exact de leurs éléments, ils ne sont pas généralement connus de personnes appartenant aux milieux qui s'occupent normalement du genre de renseignements en question ou ne leur sont pas aisément accessibles ;
>
> (b) aient une valeur commerciale parce qu'ils sont secrets ; et
>
> (c) aient fait l'objet, de la part de la personne qui en a licitement le contrôle, de dispositions raisonnables compte tenu des circonstances destinées à les garder secrets. »

Ainsi, l'OMC retient qu'appartiennent à la catégorie des secrets d'affaires : des renseignements secrets, commercialement valorisables, et protégés.

II. Défense du patrimoine immatériel de l'entreprise

Toute atteinte au patrimoine informationnel peut avoir des conséquences dévastatrices et bien souvent irréversibles. Il convient donc d'apporter les ripostes judiciaires adaptées. À défaut de texte spécifique – à l'instar du *Cohen Act* en droit

américain[6]- la victime dispose des voies de recours de droit de commun exposées ci-après (**C**), sans toutefois exclure au préalable les actions de sensibilisation (**A**) et les règles de confidentialité (**B**).

A. Protection en amont du patrimoine immatériel : prévention et sûreté interne

Dans la mesure où le patrimoine informationnel est censé procurer à son titulaire un avantage concurrentiel déterminant, toute divulgation d'une donnée stratégique confidentielle peut se révéler particulièrement destructrice, sinon irrémédiable.

Le droit permet donc de mettre en place un mode de protection combiné et rationnellement adapté à l'organisation structurelle de l'entreprise pour remédier à sa vulnérabilité. Tous les pans du droit devant être mobilisés pour assurer la sécurité de ce patrimoine immatériel *sui generis*, l'approche sera donc empirique et pluridisciplinaire.

1. Prévenir dans le respect du droit social

En premier lieu, dans un souci de sensibilisation du personnel, l'employeur veillera à instaurer une charte de bon usage des outils informatiques s'appliquant à tous les salariés et permet de solenniser les principes défensifs.

Articulation générale de la charte informatique :

Préambule	Rappeler les objectifs poursuivis par l'employeur.
Statut de la charte	Additif au règlement intérieur, adoptée selon les mêmes règles – affichage obligatoire.
Objet	Régir l'utilisation des ressources numériques, Internet, Intranet et messagerie. Rappel du cadre légal et de la responsabilité du salarié.
Sanctions encourues	Enonciation des sanctions applicables en cas de non-respect de la charte.
Règles générales d'utilisation	Proscrire l'installation de logiciels extérieurs. Limiter à l'usage professionnel. Interdiction de modifier la configuration. Interdiction de copies.
Règles de sécurité	Définition de codes d'accès personnalisés. Mesures de sauvegarde.
Ordinateurs portables	Responsabiliser et sensibiliser compte tenu des vols de supports contenant des données sensibles.
Usage de la messagerie et d'Internet	Limiter au cadre professionnel. Interdiction de certaines pratiques et de visites de sites (respect des lois et bonnes mœurs, des droits d'auteur ...).
Contrôles	Énonciation des procédures.

[6] La loi fédérale américaine adoptée en 1996, également dénommée *Economic Espionage Act* réprime pénalement deux types d'actes d'espionnage économique :
- ceux exercés pour le compte d'un gouvernement étranger, d'une organisation étrangère ou d'un agent étranger (section 1831) ;
- ceux accomplis par un tiers non autorisé dès lors que ces actes sont effectués en connaissance de cause et au mépris du droit du titulaire légitime (section 1832).

En second lieu, si l'article L. 1222-1 du Code du travail énonce que « le contrat de travail est exécuté de bonne foi », ce principe général de loyauté à l'égard de l'employeur ne s'avère pas toujours suffisant. La convention devra donc intégrer une clause de non-concurrence valide c'est-à-dire limitée dans le temps et l'espace, proportionnelle aux intérêts protégés eu égard au niveau de qualification du salarié. Depuis la jurisprudence sociale de la Cour de cassation du 10 juillet 2002, cette obligation de ne pas faire doit recevoir une contrepartie financière de la part de l'employeur.

Le contrat de travail devra également comprendre des clauses de secret spécifiques, et d'autres énonçant par exemple les outils informatiques qui sont confiés à l'employé avec les dispositions relatives à leur utilisation (login, mot de passe ...) et à leur conservation.

2. Les règles applicables à la surveillance des salariés

Concernant la surveillance des salariés, outre une information à la CNIL[7] toujours nécessaire[8], l'article L. 1222-4 du Code du travail dispose qu'» aucune information concernant personnellement le salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance ». L'employeur doit non seulement en informer préalablement son personnel, mais aussi justifier des objectifs poursuivis par ce procédé.

En revanche, l'examen de la traçabilité numérique échappe à ces dispositions. En effet, il s'agit d'une mesure de contrôle *a posteriori*, comme l'exploration de l'historique de l'ordinateur[9] ; l'employeur peut ainsi accéder aux outils informatiques du salarié, à l'exclusion des seules données estampillées « personnel », comme cela a été dégagé par une jurisprudence depuis lors constante[10]. En effet, les e-mails et fichiers ainsi marqués ne peuvent être ouverts sans commettre le délit de violation du secret de la correspondance, quand bien même l'employeur aurait interdit l'usage à des fins personnelles de la boîte de l'entreprise[11]. Pour ce faire, il faudra une ordonnance aux fins de constat d'huissier qui autorise celui-ci à procéder aux investigations, en présence du salarié[12].

A contrario, tous les autres dossiers peuvent être librement visités, sans porter atteinte au principe ci-dessus, tout ce qui n'est pas identifié comme « personnel », étant présumé comme « professionnel »[13].

---

[7] Guide pour les employeurs et les salariés, CNIL, 2008.
[8] Dossier « La protection des données dans l'entreprise », *Cahiers de Droit de l'Entreprise*, 2010-2.
[9] CA Dijon, 2 déc. 2009, RG 09/002646 ; Soc., 18 juil. 2000, n° 98-43485.
[10] Soc., 21 oct. 2009, n°07-43877, où un salarié a été condamné pour avoir constitué une entreprise concurrente à celle de son employeur. La preuve de cette activité déloyale a été retrouvée dans un fichier dédié sur l'ordinateur mis à disposition par l'entreprise lésée. Egal. : Soc., 15 déc. 2009, n° 07-44264.
[11] Soc., 2 oct. 2001, n° 99-42942 ; Soc., 12 oct. 2004, n° 02-40392.
[12] Soc., 23 mai 2007, n° 05-17818 ; Soc., 10 juin 2008, n° 06-19229.
[13] *Guide pour les employeurs et les salariés*, CNIL, 2008 ; Soc., 30 mai 2007, n° 05-43102.

Les ressources juridiques sont donc légion en vue de sécuriser les secrets d'affaires de l'entreprise, et le juriste appelé à réfléchir à cette problématique devra toujours faire preuve d'ingénierie.

B. Instaurer des règles de confidentialité à l'égard des tiers

1. Éléments de technique contractuelle

En droit commercial, il est nécessaire de veiller à l'insertion de clauses spécifiques dans les contrats dès lors que ces conventions procèdent à un transfert de données immatérielles ou de connaissances techniques, tels que les contrats de franchise, les licences de toute nature, les conventions de coopération, mais aussi les prestations associées et notamment en matière d'infogérance, d'externalisation, ou encore par le biais du *cloud computing* émergeant et ce d'autant que, selon une étude en date du 2 mars 2009 publiée par Grant Thornton, 58 % des chefs d'entreprise estiment que les services d'externalisation participent aux économies de fonctionnement[14].

Les clauses les plus couramment usitées sont :

Désignation des clauses	**Objectif poursuivi**
Clause de confidentialité ou de secret	Assurer la confidentialité des informations échangées : définition du périmètre de confidentialité et du but poursuivi, désignation des informations à tenir secrètes, mention des personnes habilitées à détenir les informations, moyens mis en œuvre pour assurer le secret, relations avec les tiers, durée, le sort des informations à l'issue et leur restitution…
Clause de non-concurrence	Obligation de ne pas réaliser la même activité et/ou de ne pas démarcher les clients du partenaire, directement ou indirectement…
Clause de non-débauchage	Éviter le recrutement d'un homme clef par le partenaire commercial.
Clause pénale	Sanction financière prévue par le contrat en cas d'infraction en dehors de tous dommages et intérêts pour réparer le préjudice. Effet dissuasif dont le montant peut être révisé par un juge.
Clause d'assiduité aux négociations	Pour une meilleure efficacité du partenariat engagé, permet également de mieux veiller à la diffusion des informations et d'en contrôler les étapes.
Clause bonne foi et de loyauté	Un socle de la relation contractuelle.
Clause de résultat et de préemption de droits de propriété intellectuelle	Afin de s'assurer de la propriété des résultats à l'issue de travaux de R&D.
Clause de sollicitation et clause de contrôle	Permet de contrôler la traçabilité des informations échangées et de procéder à des audits
Clause d'alerte	Afin de prévenir les risques.

[14] Cité par L. Chafiol-Chaumont et Virginie Olivier, « Les points-clés d'un contrat d'externalisation souple et évolutif », *Cahiers de Droit de l'Entreprise*, 2009-6, p. 68.

2. Les applications du droit de l'immatériel

En droit économique, outre la protection des droits intellectuels tels que les marques, dessins et modèles et brevets, mais aussi de bases de données, logiciels, obtentions végétales..., en termes de recherche et développement il est nécessaire de recourir à des conventions particulières précisant le périmètre de confidentialité, la propriété des droits en découlant et leur protection ainsi que leur utilisation par chaque partie.

En droit des nouvelles technologies (TIC), il conviendra par exemple, de mettre en place une convention adaptée avec les partenaires extérieurs pour la conservation sécurisée des donnés externalisées. On pourra utilement se référer aux clauses ci-dessus. D'autres mesures consistent à compartimenter les informations stratégiques pour éviter que l'on puisse reconstituer l'intégralité des secrets d'affaires.

C. La défense en aval des secrets d'affaires : les voies de recours pénal contre les actes d'ingérence et de malveillance

1. Un droit pénal spécial inapproprié

Le législateur a créé un droit pénal spécial dont l'efficacité en matière de lutte contre l'espionnage économique reste discutée et suscite les critiques suivantes :

- la loi sur les intrusions informatiques ne vise que les attaques extérieures avérées.
- la législation sur le droit d'auteur et le droit des producteurs qui ne permet pas de protéger efficacement l'accès et l'utilisation des bases de données.
- la législation sur les brevets n'englobe pas les secrets d'affaires.
- le secret professionnel ne s'applique qu'à un nombre limité de personnes.
- la loi Informatique et Libertés ne protège que les informations personnelles.

À titre d'exemple, dans l'affaire Michelin[15], un employé avait compilé des renseignements stratégiques et avait tenté de les revendre à plusieurs concurrents. Dans son jugement du 21 juin 2010, le Tribunal correctionnel de Clermont-Ferrand a condamné, pour abus de confiance, l'ex-salarié à 5.000 € d'amende et deux ans de prison avec sursis. Le tribunal a non seulement exclu la livraison d'informations à une entreprise étrangère, mais aussi la violation des secrets de fabrication.

Concernant précisément cette dernière notion, l'article L. 1227-1 du Code du travail, réprime « Le fait pour un directeur ou un salarié, de révéler ou de tenter de révéler un secret de fabrication ». Cette rédaction ne donnant pas la définition du secret de fabrication, il faut s'en remettre à la jurisprudence qui, dès 1935, a entendu ainsi le qualifier comme étant « tout procédé de fabrication, offrant un intérêt

[15] Trib. corr. Clermont-Ferrand, 21 juin 2010.

pratique ou commercial, mis en œuvre par un industriel et gardé secret à l'égard de ses concurrents »[16].

Cet article pose donc trois conditions cumulatives :

(i) ce texte ne s'applique qu'à un secret de fabrication industrielle, à l'exclusion de tout autre secret d'affaires ;
(ii) l'auteur de l'infraction doit nécessairement être un salarié ou un ancien salarié ;
(iii) l'acte incriminé est une divulgation ou une tentative de divulgation et non la simple possession des secrets.

Compte tenu de l'ensemble de ces impératifs restrictifs, un tel dispositif reste délicat à mettre en application. Il fut ainsi écarté dans l'affaire Michelin.

Ce cas d'espèce démontre de toute évidence que ce droit pénal spécial n'est pas toujours efficient. Par voie de conséquence, en raison d'un spectre d'application plus large, le droit pénal général, qui demeure le tronc commun des peines et délits, s'avère être la voie de recours la plus efficace.

2. Un droit pénal général imparfait

Un autre exemple récent permet d'illustrer ce propos, il s'agit de l'équipementier Valeo[17]. Une étudiante chinoise y avait effectué un stage en 2005, pendant lequel elle avait exporté des données confidentielles retrouvées sur six ordinateurs d'une capacité exceptionnelle. Le 18 décembre 2007, le Tribunal correctionnel de Versailles l'a condamnée à 7.000 € d'amende et un an d'emprisonnement – dont deux mois fermes – sur le fondement de l'abus de confiance, écartant la qualification d'intrusion informatique.

Tel que défini par l'article 314-1 du Code pénal « L'abus de confiance (...) consiste dans le détournement ou la dissipation, frauduleusement commis, de choses remises au délinquant, à charge pour lui de les rendre ou représenter ou d'en faire un emploi déterminé »[18].

Le délit est donc constitué, non par une ruse trompeuse, mais par le détournement d'une chose précédemment attribuée pour un usage déterminé en tout cas contraire à ce pourquoi elle a été remise. Il doit y avoir préalablement le transfert volontaire d'une chose ; en ce sens, l'abus de confiance diffère du vol pour lequel la victime n'a pas entendu se déposséder d'un bien, encore moins au profit d'un individu déterminé. C'est pourquoi on parle en général de relation contractuelle comme fait générateur de la remise de la chose, même verbale.

Dans les exemples cités ci-dessus, s'il s'avère qu'il y avait bien à l'origine un lien contractuel entre les parties, il résidait une difficulté dans la mesure où le bien

[16] Crim., 29 mars 1935, Bull. crim., p. 350.
[17] Trib. corr. Versailles, 18 déc. 2007.
[18] In Merle R. et Vitu A, *Droit pénal spécial*, t. 2, Cujas, 1982, n° 2365.

remis n'était pas un élément corporel, mais une information détenue au titre d'une activité professionnelle accomplie au sein de l'entreprise. Or, la jurisprudence ne sanctionnait auparavant que le détournement de biens corporels, à l'exclusion d'information de toute nature, sauf si elle figurait sur un support matériel, comme pour le vol. Ainsi, un détournement de contrats commerciaux avait été reconnu comme un abus de confiance parce que le délit était constitué par la remise des éléments sur papier, l'infraction pénale ne couvrant pas « les stipulations juridiques qui en constituent la substance juridique »[19].

Mais plus récemment, la Cour d'appel de Paris a considéré que l'envoi par un salarié de fichiers par e-mail à destination de son nouvel employeur était constitutif d'un détournement de documents au sens du texte pénal[20]. C'est donc dans le prolongement de cette dernière décision que les juges de Versailles et de Clermont-Ferrand ont qualifié les actes répréhensibles d'abus de confiance, et ont par conséquent renforcé ce motif de poursuite qu'est l'abus de confiance, quand bien même le détournement ne devrait porter que sur des secrets d'affaires, de nature incorporelle.

Le vol, qui est littéralement stipulé comme étant la *soustraction frauduleuse du bien d'autrui*, s'interprète comme la disparition du bien dans le patrimoine de la victime et son transfert dans l'actif du voleur. Or, dans le cas d'une copie numérique, le fichier d'origine demeure dans l'actif de la victime. Par ailleurs, la jurisprudence exige que l'on dispose d'un support matériel, faute de reconnaître le vol de biens immatériels *stricto sensu*. Après s'être longtemps refusé à reconnaître le vol de données informatiques, la jurisprudence a opéré un revirement en 2003, énonçant que « le fait d'avoir en sa possession (...) après avoir démissionné de son emploi pour rejoindre une entreprise concurrente, le contenu informationnel d'une disquette support du logiciel [X], sans pouvoir justifier d'une autorisation de reproduction et d'usage du légitime propriétaire, qui au contraire soutient que ce programme source lui a été dérobé, caractérise suffisamment la soustraction frauduleuse de la chose d'autrui et la volonté de s'approprier les informations gravées sur le support matériel »[21]. Cette décision demeure néanmoins isolée, même si elle semble avoir été depuis lors confirmée dans un autre arrêt d'espèce de la Chambre criminelle[22].

De même, et plus récemment encore, cette même chambre a énoncé que : « la reproduction de documents est susceptible de recevoir la qualification de vol au même titre que leur appréhension, de sorte que l'effet justificatif attaché à l'exercice des droits de la défense s'applique aussi bien aux documents originaux qu'à leur reproduction... », cela dans le cadre d'une affaire qui n'est pas un cas de concurrence déloyale ou « d'espionnage économique », mais celui d'un ex-salarié ayant introduit un recours prud'homal au soutien de documents collectés au sein de l'entreprise[23].

---

[19] Cass. Crim., 9 mars 1987, n°85-17.484, *JCP G* 1988, II, n° 20913, obs. Devèze J.
[20] CA Paris, 9e ch., 25 févr. 2005, Juris-Data n° 281748.
[21] Crim., 9 sept. 2003, pourvoi n° 02-87098.
[22] Crim., 4 mars 2008, *D.* 2008, p. 2213.
[23] Crim., 21 juin 2011, pourvoi n° 10-87.671. Arrêt n° 3813.

S'agissant de l'affaire *ROSE*[24], dont les faits sont semblables à ceux de l'affaire Michelin, la juridiction pénale a estimé que : « attendu que le rapport d'expertise du disque dur et des clés USB retrouvées en perquisition au domicile de Madame [ROSE] a établi que le fichier « c list 0908.xls » correspondant aux données des clients des d'informations, aux fins d'actualisation des fichiers antérieurs sont constitutifs de soustraction frauduleuse sociétés X et X² a été créé le 16 janvier 2009, soit le jour du départ de la société ; que sous couvert de fournir des données actualisées à Monsieur XX elle a transféré ces données sur une clé USB ; que le transfert ».

Si la sanction s'est révélée minime, en regard de l'atteinte portée à son patrimoine informationnel, il n'en demeure pas moins que cette décision se veut novatrice, ou à tout le moins audacieuse, dans la mesure où le vol d'informations incorporelles s'est trouvé constitué pour une affaire « d'espionnage économique »[25].

Si l'on peut se féliciter d'une telle qualification juridique, il faut toutefois garder à l'esprit qu'un jugement de première instance ne fait pas jurisprudence, même s'il s'inscrit dans une tendance qui semble désormais s'affirmer devant les tribunaux répressifs.

Or, en matière pénale, il est convenu que *nulla poena sine lege, nulla poena sine crimine, nullum crimen sine poena legali*[26]. Sans texte, aucune entreprise victime n'est à l'abri d'un revirement de jurisprudence, les décisions ci-dessus n'étant que justes mais néanmoins précaires interprétations de dispositions pénales de portée générale.

À cet égard, la proposition de loi Urvoas relative à la *protection des secrets d'affaires*, enregistrée à la présidence de l'assemblée nationale le 16 juillet 2014, si elle avait le mérite d'insérer une définition des secrets d'affaires, qui fait cruellement défaut dans le droit positif français, faisait néanmoins doublon avec les fondements de l'abus de confiance, tout en éludant l'appropriation frauduleuse qu'il conviendrait de rapprocher du vol d'information. Or, c'est en cela que le droit français est lacunaire, et qu'il conviendra de remédier dans un avenir que l'on espère proche.

[24] Trib. corr. Clermont-Ferrand, 26 sept. 2011.
[25] de Maison Rouge O., « L'Affaire Rose. Première condamnation de l'espionnage économique par le biais du vol de données immatérielles », *Bulletin du Droit des Secrets d'Affaires*, n°00, mars 2012.
[26] Souvent raccourci en *nullum crimen, nulla poena sine lege*.