Confidentialité et cryptographie en entreprise

Marie Barel

Juriste, spécialiste TIC et sécurité de l'information et des systèmes.
contact : marie.barel@legalis.net

Résumé La cryptographie est à n'en pas douter la solution incontournable lorsqu'on entend assurer la protection des « *assets business* » [1]de l'entreprise. Si donc elle apporte une réponse technique adaptée à la problématique majeure de la confidentialité des données, la cryptographie n'en demeure pas moins strictement encadrée par les législateurs français et étrangers. Ainsi l'objet de notre conférence consistera dans un premier temps à donner une vision claire et synthétique de la réglementation française issue de la loi nr 2004-575 du 21 juin 2004 (ci-après la « LEN ») en cette matière (section 1). Dans un second temps, nous examinerons une problématique soulevée récemment devant les tribunaux concernant l'utilisation de la cryptographie par les salariés dans l'entreprise (section 2).

Ordre juridique concerné : France

[1] Les assets sont l'ensemble des biens, actifs, ressources ayant de la valeur pour l'entreprise et nécessaires à son bon fonctionnement. A côté des assets liés au SI – on parle dans ce cas d'assets système (matériel, logiciels et réseaux ainsi que l'environnement même du SI, tel que les bâtiments), on distingue les assets business qui comprennent en particulier les informations (par exemple la désignation des comptes utilisateurs : couple identifiant-mot de passe) et les processus (comme l'administration des comptes).

1 Synthèse de la législation française réglementant les biens de cryptologie

Après un rappel historique de l'évolution de la réglementation française en cette matière (1.1), nous exposerons le détail du dispositif en vigueur suite à l'adoption de la LEN (1.2).

1.1 De la prohibition au « contrôle étatique et à la liberté concédée » [2] (1939-2004) : grandes étapes de l'évolution du régime juridique applicable aux moyens de chiffrement

La cryptologie, étymologiquement la « science du secret », a longtemps été considérée comme une arme de guerre. Art ancien (du bâton de Jules César aux cabinets noirs et à la machine à chiffrer *Enigma* utilisée par l'Allemagne nazie au temps de la seconde guerre mondiale), la scène cryptographique s'est finalement déplacée, par une évolution encore récente, d'une technique réservée à l'usage strictement militaire vers une commercialisation au bénéfice des acteurs économiques et civils[3]. Cette diffusion de la « cryptographie civile » s'est fortement accélérée ces dernières années avec le développement en particulier de l'informatique[4] puis du commerce électronique, qui a posé comme une nécessité incontournable le principe de confidentialité des données.

Prenant acte de ce nouveau besoin de sécurité soulevé par l'avènement de la société de l'information, le législateur français a du, à plusieurs reprises, adapter la législation qui régit à la fois l'usage et le commerce des « biens de cryptologie »[5]. Ainsi, on peut distinguer quatre grandes étapes de l'évolution de la réglementation en la matière :

Le régime issu du décret-loi de 1939. – A l'origine, les « *équipements de cryptophonie ou de cryptographie* »[6] sont régis par le décret-loi du 18 avril 1939 qui fixe le régime des « matériels de guerre, armes et munitions ». Etant ainsi considérés comme armes de guerre de deuxième catégorie[7], leur usage « à des fins professionnelles ou privées » est par conséquent prohibé sauf dérogation gouvernementale autorisant la « déclassification » de certains matériels commerciaux.

[2] Lire Bertrand Warusfel, Dix ans de réglementation de la cryptologie en France : du contrôle étatique à la libertée concédée - `http://www.droit.univ-paris5.fr/warusfel/articles/reglcrypto\_warusfel.pdf`

[3] Par exemple les premières versions commerciales d'Enigma (« Enigma-D) remontent au début des années 1920.

[4] Lire *La Guerre des Codes secrets : des hiéroglyphes à l'ordinateur*, par David Kahn – InterEditions, 1980 ; aussi : *La Science du Secret*, ouvrage de Jacques Stern paru en 1998 aux éditions Odile Jacob - chapitre II « L'âge technique ».

[5] Nous verrons plus loin, quelle en est la définition en vigueur ...

[6] La définition des procédés techniques de cryptologie concernés fut précisée dans le décret nr 86-250 du 18 février 1986 – celui-ci permit également d'élargir quelque peu les conditions dans lesquelles une dérogation pouvait être attribuée aux moyens de cryptologie à usage commercial ; un arrêté du 2 juillet 1990 précisa quant à lui les conditions de fabrication, de commerce, d'acquisition, de détention et d'utilisation de moyens de cryptologie destinés à des fins professionnelles ou privées sur le territoire national.

[7] Dans la même classe, on trouve par exemple : les « équipements de brouillage, leurres et leurs systèmes de lancement ». Voir : décret nr 73-364 du 12 mars 1973 relatif à l'application du décret-loi du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions – JO du 30 mars 1973 – et modifié par le décret no 93-17 du 6 janvier 1993 – JO du 7 janvier 1993.

Ainsi longtemps domaine réservé des militaires, ce sont les deux étapes du processus européen de l'essor de la concurrence dans le secteur des télécommunications qui vont permettre d'abord un assouplissement puis un compromis favorable à la libéralisation du secteur.

La LRT de 1990. – C'est en décembre 1990 que le régime juridique de la cryptographie connaît un premier tournant (on peut dire, de ce point de vue, qu'il y a un « avant 1990 » et un « après 1990 ») avec l'adoption de la Loi de Réforme des Télécommunications (LRT)[8].

Pour la première fois, le législateur inverse la perspective[9]et crée une distinction entre la cryptographie utilisée pour mettre en œuvre des fonctions d'authentification ou d'intégrité et celle utilisée pour assurer des besoins de confidentialité. Ainsi, elle met en place deux régimes distincts (article 28 de la loi de 1990), respectivement de

1. déclaration préalable, lorsque le moyen ou la prestation ne peut avoir d'autre objet que d'authentifier une communication ou d'assurer l'intégrité du message transmis ; et de :
2. autorisation préalable du Premier ministre, dans les autres cas.[10]

Force est de souligner toutefois que, malgré cette réforme du régime juridique applicable, la loi de 1990 est d'abord prise, suivant la lecture des motifs indiqués par le législateur, « *pour préserver les intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat* ». Dès lors, loin de témoigner d'une quelconque forme de libéralisation, l'esprit du texte décrit bien un modèle qui reste avant tout sécuritaire et où le Service Central de la Sécurité des Systèmes d'Information (SCSSI), en charge du respect de l'application des textes concernés, conduit jusqu'en 1996 (cf. infra, point 3) une politique tendant à endiguer les utilisations civiles et même commerciales des moyens de chiffrement[11] tout en leur simplifiant l'accès aux technologies de signature électronique (qui permettent de sécuriser l'accès aux réseaux informatiques et de renforcer la confiance dans les transactions commerciales et financières générées par le commerce électronique).

Vaine politique sans doute dans un contexte technologique et international où, par l'effet de la mondialisation véhiculée par l'Internet, les moyens de chiffrement se trouvent facilement accessibles (exemple de PGP mis en libre téléchargement par son auteur, Phil Zimmerman, dès 1991) et sont même de plus en plus souvent intégrés par défaut dans les logiciels standards comme dans les navigateurs Web ou les applications de messagerie, ou bien encore le système d'exploitation lui-même (exemple de la version *Entreprise* du nouveau système d'exploitation de Microsoft, Windows *Vista*®, qui comprend un dispositif de chiffrement des données : *BitLockerDriveEncryption*). De même, la France se singularise par un régime toujours très contraignant s'agissant de *l'utilisation*

[8] Loi nr 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications - JO du 30 décembre 1990.

[9] A partir de 1990, la cryptographie n'est plus réservée au seul usage des militaires et les moyens de cryptologie ne sont plus des matériels de guerre, sauf dans le cas particulier de moyens de cryptologie « *qui sont spécialement conçus ou modifiés pour permettre ou faciliter l'utilisation ou la mise en œuvre des armes* » (art. 28, IV de la loi).

[10] Les contrevenants s'exposaient à une amende comprise entre 6 000 F et 500 000 F et/ou à une peine d'emprisonnement allant de un à trois mois, le tout assorti d'une éventuelle confiscation des moyens de cryptologie.

[11] Outre le fait qu'elles constituent un obstacle sérieux aux « interceptions de sécurité » (écoutes administratives) ou décidées par la justice, les partisans de la vision « militaire » de la cryptographie postulent en faveur du maintien d'un contrôle étatique fort en raison des risques d'une utilisation de ces techniques à des fins malveillantes (criminalité organisée) ou pire, terroristes.

des moyens de cryptologie, par rapport à la plupart des autres Etats qui ne connaissent pour leur part que des restrictions à *l'exportation* (à l'exception de quelques rares pays comme la Russie, la Chine, l'Iran ou la Corée du Nord !).

La loi sur les télécommunications de 1996. – C'est donc un premier pas forcé vers la libéralisation que constitue l'adoption de la loi du 26 juillet 1996[12] laquelle met en place un dispositif certes plus libéral mais qui suscita de nombreuses interrogations tenant aussi bien à sa complexité (i) qu'à sa viabilité économique (ii).

(i) Tout d'abord, la nouvelle réglementation, très formaliste, ne compte alors pas moins de six régimes qui s'appliquent suivant les fonctionnalités des moyens ou prestations de cryptologie, la nature des actes et la taille de l'algorithme de chiffrement :

1. régime de liberté : ainsi l'utilisation personnelle de moyens de cryptologie ayant pour seule fonction l'authentification et l'intégrité ou encore la signature de messages est libre (pour plus de précisions, voir le décret du 24 février 1998) ;
2. régime de dispense de formalité préalable (décret n° 98-206 du 23 mars 1998[13], qui sera abrogé et remplacé par le décret nr 99-200 du 17 mars 1999),
3. de déclaration simplifiée,
4. de déclaration préalable,
5. de substitution de la procédure de déclaration à la procédure d'autorisation (décret n° 98-207 du 23 mars 1998, qui sera abrogé et remplacé par le décret nr 99-199 du 17 mars 1999), et
6. d'autorisation préalable : sont visés en particulier tous les moyens ou prestations de cryptologie assurant des fonctions de confidentialité et dont les clés de chiffrement sont supérieures à 40 bits[14] ou bien utilisent des clés non gérées par un tiers de confiance.

(ii) Ensuite, disposition phare de la réglementation de 1996, la mise en place des tiers de confiance (certains préférant la désignation de « tiers de séquestre »)[15] – dont le rôle est de conserver les clés secrètes des utilisateurs mises en œuvre à des fins de confidentialité afin de les remettre à ces mêmes utilisateurs s'ils les demandent, ainsi qu'aux autorités judiciaires ou de sécurité pour satisfaire aux exigences de la loi du 10 juillet 1991 relative au secret des correspondances – contribue à nouveau à isoler la France sur l'échiquier international : comme le souligne un commentateur après la publication des décrets d'application en 1998, « *la France est le premier pays au monde à se doter*

[12] Recherche d'un compromis entre la « *protection des informations et le développement des communications et des transactions sécurisées* » et la préservation des « *intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat.* »

[13] Il s'agit par exemple des équipements ou systèmes suivants : les systèmes d'identification des cartes bancaires, les décodeurs de programmes audiovisuels, les radiotéléphones mobiles, les video laser, les moyens conçus pour protéger les logiciels contre les copies illicites, les équipements de contrôle d'accès (distributeurs de billets, ...), les télérelevés des compteurs de consommation.

[14] La taille de la clé de chiffrement sera augmentée en 1999, sous le gouvernement Jospin, de 40 à 128 bits (voir décret nr 99-200 précité).

[15] Système que les anglo-saxons désignent pour leur part sous le terme de « GAK » pour « *Gouvernment Access to Keys* » ou encore *key escrow*.

d'un tel système (et le seul jusqu'à présent) »[16]. Vivement critiqué[17] aussi tant par l'Autorité de Régulation des Télécommunications (ART)[18] que par le Conseil d'Etat[19], le dispositif retenu a en effet des répercussions économiques qui mettent en jeu la compétitivité des entreprises françaises.

En définitive, la législation de 1996, jugée unanimement trop complexe (en témoigne également les deux années qui furent nécessaires avant de publier ses premiers décrets d'application) est rapidement et à nouveau assouplie (voir les décrets précités, pris en 1999) et le SCSSI, encouragé par les pratiques de ses pairs à l'étranger et l'évolution du contexte législatif international et communautaire[20] qui progresse toujours dans le sens d'une plus grande libéralisation, multiplie par exemple la délivrance de licences générales et l'octroi de qualification « produit *mass market* » qui facilitent pour les entreprises françaises le commerce des biens de cryptologie.

Entérinant ainsi un processus d'ouverture devenu inéluctable, la loi du 21 juin 2004 va notamment achever, dans une dernière étape, le processus de libéralisation de l'usage des moyens de cryptographie[21].

1.2 Vue synoptique du dispositif en vigueur depuis la loi nr 2004-575 du 21 juin 2004 (« LEN »)

Inscrite dans son titre III sur la « Sécurité dans l'économie numérique », le nouveau dispositif réglementant les « moyens et prestations de cryptologie » est adopté dans le cadre de la loi nr 2004-575 du 21 juin 2004, chapitre que nous mettons en annexe du présent article.

Avant-propos : définitions. – Le législateur de 2004 met désormais davantage l'accent sur les moyens de cryptologie plutôt que sur les prestations.
L'article 29 de la LEN stipule : « *On entend par* ***moyen de cryptologie*** *tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide*

[16] Me Valérie Sédaillian, *Décrets sur la cryptographie : la logique sécuritaire de la réglementation française demeure inchangée* - http ://www.iris.sgdg.org/axes/crypto/decrets.html#ref

[17] Un groupe *ad hoc* de cryptographes et de scientifiques de renom international ont publié sur ce sujet un papier décrivant les risques de ces dispositifs : *The risks of key recovery, key escrow and thrusted third party encryption* < `http://www.cdt.org/crypto/risks98/` >

[18] Lire son avis du 8 octobre 1997 (JO du 28 février 1998) dans lequel l'ART souligne « l'absence d'une étude de l'environnement économique de ces organismes et de leur conditions de viabilité », jugeant ainsi que : « cette activité nouvelle de tierce partie de confiance qui n'existe pas dans la plupart des pays avec lesquels la France entretient des relations commerciales doit, pour constituer un véritable métier susceptible de s'exercer dans le secteur concurrentiel, être envisageable dans des conditions de responsabilités clairement déterminées et suppose donc des relations financières équilibrées ».

[19] Voir son rapport publié en juillet 1998 : *Internet et les réseaux numériques.*

[20] Décision du Conseil (EC) N° 1334/2000 du 22 Juin 2000 instituant un régime communautaire de contrôles des exportations de biens et technologies à double usage (JOCE L.159, 30.6.2000) ; décision du Conseil N° 2000/402/CFSP du 22 Juin 2000 abrogeant la décision 94/942/PESC relative à l'action commune concernant le contrôle des exportations de biens à double usage (JOCE L.157, 30.6.2000)

[21] Dès 1999, dans son discours prononcé à Hourtin, le Premier ministre, Lionel Jospin, annonce « *un changement fondamental d'orientation* ». La nouvelle politique devra s'articuler autour de deux axes : « *offrir une liberté complète dans l'utilisation des produits de cryptologie, sous la seule réserve du maintien des contrôles à l'exportation découlant des engagements internationaux de la France* (arrangement de Wassenaar) » et « *supprimer le caractère obligatoire du recours au tierces parties de confiance pour le dépôt des clefs de chiffrement* ».

de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité.

On entend par ***prestation de cryptologie*** *toute opération visant à la mise en œuvre, pour le compte d'autrui, de moyens de cryptologie. »*

De l'usage des moyens de cryptologie. – Comme le met en lumière le tableau en FIG1(p6) ci-dessous, la liberté d'utilisation des moyens de cryptologie devient totale à partir de 2004, tant pour les personnes physiques que pour les personnes morales (entreprises).

La France rallie ainsi, bien que tardivement, les pays qui, comme les Etats-Unis où l'usage de ces moyens est libre depuis l'origine, considèrent la cryptographie comme une composante essentielle de la démocratie et de la protection des libertés publiques et individuelles.

<table>
<tr><th colspan="4">AVANT</th><th>APRES</th></tr>
<tr><td>Authentification,
Intégrité</td><td colspan="3">Confidentialité
Longueur de clé</td><td rowspan="3">LIBRE
(art.30-I LEN)</td></tr>
<tr><td rowspan="2">LIBRE</td><td>40 bits ≤</td><td>128 bits ≤</td><td>> 128 bits</td></tr>
<tr><td>LIBRE</td><td>LIBRE *</td><td>AUTORISEE
/ LIBRE *</td></tr>
</table>

FIG. 1: Réglementation de l'usage des moyens de cryptologie depuis la LEN

** A condition : soit que lesdits matériels ou logiciels aient préalablement fait l'objet d'une déclaration par leur producteur, un fournisseur ou un importateur, soit que lesdits matériels ou logiciels soient exclusivement destinés à l'usage privé d'une personne physique ; sinon, une déclaration d'utilisation personnelle doit être adressée à la DCSSI*

*** A condition que lesdits matériels ou logiciels aient fait l'objet d'une autorisation de fourniture en vue d'une utilisation générale. Sinon, une demande d'autorisation d'utilisation personnelle doit être adressée à la DCSSI.*

**** Lorsque la clé est gérée par un tiers de confiance, l'utilisation de moyens de chiffrement offrant des services de confidentialité reposant sur des clés strictement supérieure à 128 bits est libre. Le tiers de confiance est un organisme agréé par la DCSSI pour gérer les clés des utilisateurs ; il doit remettre les clés aux autorités judiciaires et de sécurité sur requête de leur part.*

Notons d'ores et déjà également que le législateur de 1994 abandonne désormais la distinction entre systèmes cryptographiques (symétrique/asymétrique) ainsi que le concept de longueur de clé, qui était par ailleurs critiqué[22].

[22] Comme le rappelle Claudine Guerrier (in *La cryptologie, entre sécurité et liberté* – publication OSTIC, « L'année des TIC 2004 »), deux écoles s'affrontent sur ce sujet : tandis que certains soulignent la sécurité induite par la longueur des clés (le code généré à l'aide d'une clé de chiffrement de 40 bits serait facile déchiffrer tandis qu'une clé de plusieurs milliers de bits serait quasiment inviolable), d'autres considère à l'inverse que la taille de la clé n'est pas la panacée car les cryptanalystes contournent ou cassent assez facilement les algorithmes eux-mêmes.

De l'importation et la fourniture des moyens de cryptologie. - La lecture des tableaux en FIG2 (p7) et FIG3 (p8) montre ensuite la volonté du législateur non seulement de simplifier mais aussi d'alléger les procédures. Ainsi, en matière de fourniture comme d'importation, seuls les produits de cryptographie mettant en œuvre des fonctionnalités de confidentialité sont encore soumis au régime de déclaration préalable (dont les conditions de souscription sont explicitées dans le décret nr 98-101 du 24 février 1998[23] modifié par le décret nr 2002-688 du 2 mai 2002).

AVANT				**APRES**	
Authentification Intégrité	Confidentialité *Longueur de clé*			Authentification Intégrité	Confidentialité
LIBRE	40 bits ≤	128 bits ≤	> 128 bits	LIBRE	DECLARATION PREALABLE ** (dossier technique + code source des logiciels utilisés)
	L	L*	A		

FIG. 2: Réglementation de l'importation des moyens de cryptologie depuis la LEN
L = régime de liberté ; A = régime d'autorisation
***** *A condition : soit que lesdits matériels ou logiciels aient préalablement fait l'objet d'une déclaration par leur producteur, un fournisseur ou un importateur, soit que lesdits matériels ou logiciels soient exclusivement destinés à l'usage privé d'une personne physique ; sinon, une déclaration d'utilisation personnelle doit être adressée à la DCSSI.*
****** *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 importation peut être dispensée de toute formalité préalable, sont fixées par un décret en Conseil d'Etat. (non publié à ce jour[24]).*

Rappelons toutefois ici que le régime de déclaration préalable n'est pas comparable à une simple formalité de dépôt légal, mais suppose, un (1) mois au moins avant la fourniture, l'importation (ou l'exportation : cf. le tableau en FIG5 (p9)), l'envoi d'un dossier détaillé à la DCSSI (anciennement SCSSI) – dossier dont la forme et le contenu sont fixés dans un arrêté du 17 mars 1999. Ce dossier de déclaration comporte une partie administrative mais aussi une partie technique qui est en réalité à l'identique de celui relevant de la procédure d'autorisation ! La préparation du dossier technique (qui peut nécessiter plusieurs semaines de travail d'un ingénieur spécialisé) doit notamment comporter une description complète des procédés de cryptographie employés, avec description mathématique et simulation dans un langage informatique de haut niveau, et la description complète de la gestion des clés mises en œuvre par le moyen. En définitive, la différence principale entre le régime de la déclaration et le régime de l'autorisation tient seulement au délai donné à la DCSSI pour répondre[25] au déclarant (un mois dans le cas de la déclaration[26] et quatre mois dans celui de l'autorisation).

[23] Voir : `http://www.ssi.gouv.fr/fr/reglementation/regl.html\#crypto`

[25] Contact à la DCSSI en charge de la réglementation de la cryptologie : Bureau des relations industrielles, SGDN / DCSSI - 51, boulevard de Latour-Maubourg 75700 PARIS 07 SP ; téléphone : 01 71 75 82 75, rid.dcssi@sgdn.pm.gouv.fr

[26] Le silence du SCSSI (devenu aujourd'hui « DCSSI ») vaut en effet acceptation conformément à un principe du droit administratif.

AVANT *				**APRES ****	
Authentification Intégrité	Confidentialité *Longueur de clé*			Authentification Intégrité	**Confidentialité**
Déclaration simplifiée	40 bits ≤	128 bits ≤	> 128 bits	LIBRE	DECLARATION PREALABLE (dossier technique + code source des logiciels utilisés)
	D	D	A		

FIG. 3: Réglementation de la fourniture des moyens de cryptologie depuis la LEN
D = régime de déclaration ; A = régime d'autorisation
** Moyens pouvant être exemptés de contrôle quelle que soit la longueur de clé sous certaines conditions (D. nr 99-200 du 17 mars 1999) : cartes à puce personnalisées, équipements de réception de télévision de type grand public, moyens matériels ou logiciels spécialement conçus pour assurer la protection des logiciels contre la copie ou l'usage illicite, moyens de cryptologie utilisés dans les transactions bancaires, radiotéléphones portatifs ou mobiles destinés à l'usage civil, station de base de radiocommunication cellulaires civiles, ...*
*** 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 peut être dispensée de toute formalité préalable, sont fixées par un décret en Conseil d'Etat (non publié à ce jour).*

Du transfert et de l'exportation des moyens de cryptologie. – Notion introduite par le législateur de 1994, la notion de transfert désigne le « passage de frontière » entre deux États membres de la Communauté européenne ; il ne s'agit plus d'exportation/importation stricto sensu puisque les États membres sont dans un marché unique. La qualification d'exportation/ importation s'applique donc lorsqu'est concerné un État tiers à la Communauté européenne.

Authentification	Confidentialité	
Contrôle d'intégrité (art. 30, II LEN)	(Depuis la France) Vers un État membre de l'UE - art. 30, IV LEN	Depuis un État membre de l'UE (vers la France) – Art. 30, III LEN
LIBRE	AUTORISATION	DECLARATION PREALABLE

FIG. 4: Réglementation du transfert des moyens de cryptologie depuis la LEN
Cf. Membre de l'UE [27]

Conformément à l'article 30 de la LEN, le législateur français prévoit en matière de transferts intra-communautaires les mêmes conditions de contrôle que celles applicables en matière d'importation et d'exportation vers des pays tiers (sort en théorie moins favorable que pour l'export vers sept destinations qui peuvent bénéficier d'une licence générale communautaire – cf. tableau en FIG5 (p9)).

Toutefois, il est prévu que « *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*

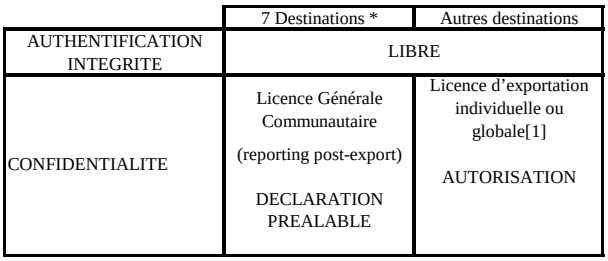

FIG. 5: Réglementation de l'exportation des moyens de cryptologie depuis la LEN
** Australie, Canada, Japon, Nouvelle Zélande, Norvège, Suisse, USA*
Licence d'exportation individuelle ou globale[28]

européenne ou leur exportation peuvent être soit soumis au régime déclaratif (...) soit dispensés de toute formalité préalable. »

En définitive, les exceptions au régime d'autorisation et au régime déclaratif, qui doivent être définies par les différents décrets en Conseil d'Etat visés dans la loi de 2004, vont jouer un rôle d' « arbitre » dans l'appréciation du dispositif actuel en matière de cryptologie : si les exceptions sont nombreuses, le régime de la cryptologie française pourra être considéré comme néo- libéral ; inversement, si les exceptions sont circonscrites, le régime de la cryptologie française sera mixte, libéral quant à l'utilisation, plus sécuritaire quant à la fourniture, le transfert, l'importation et l'exportation.

Nota bene – En dernier lieu, il est important de rappeler quelles sont les sanctions encourues en cas de non respect de la réglementation en matière de contrôle des biens de cryptologie. Ainsi, deux types de sanctions sont susceptibles de s'appliquer : sanctions de type administrative d'une part (interdiction de mise en circulation – cf. article 34 de la LEN) et pénales (cf. article 36 de la LEN) d'autre part :

1. jusqu'à un (1) an d'emprisonnement et 15.000 € d'amende dans le cadre du régime déclaratif ou de l'obligation de communication d'informations ;
2. jusqu'à deux (2) ans d'emprisonnement et 30.000 € d'amende dans le cadre du régime d'autorisation ;
3. peines complémentaires : confiscation, fermeture d'établissement, exclusion des marchés publics, ...

Par ailleurs, notons que l'usage d'un moyen de cryptologie en vue de préparer un crime ou un délit ou pour en faciliter la préparation ou la commission est désormais considéré (cf. article 37 de la LEN) comme une circonstance susceptible d'aggraver la peine encourue pour le délit principal (article 132-79 du code pénal).
-/-

Parvenus en particulier, au terme d'une évolution législative lente et difficile que nous venons de retracer, à la libéralisation complète de l'utilisation des moyens de cryptographie, il est intéressant maintenant de voir comment cette nouvelle liberté est finalement amenée à être à nou-

veau réglementée dans le cadre, non plus d'un contrôle étatique, mais de la surveillance des salariés sur les lieux de travail.

2 Confidentialité des données, vie privée et cryptographie en entreprise : des usages à réglementer !

Problématique. **-** Comme nous venons de l'exposer plus haut, l'usage des moyens de cryptographie est désormais totalement libre, tant pour les personnes physiques qui souhaitent de plus en plus protéger leur vie privée, que pour les personnes morales et notamment les entreprises qui doivent par exemple protéger leur patrimoine informationnel et l'ensemble de ses données vitales ou bien encore répondre de l'obligation de sécurité des données à caractère personnel[29] qu'elle met en œuvre dans de nombreux fichiers et traitements quotidiens.

Pour répondre à l'ensemble de ces finalités dont le facteur commun est celui de l'exigence de confidentialité des données, le recours aux moyens de cryptographie est présenté comme la panacée, cependant que leur usage peut soulever des conflits d'intérêt. Ainsi, dans le cadre de la surveillance des salariés sur le lieu du travail, le chiffrement des données peut devenir un obstacle aux contrôles exercés par l'employeur pour s'assurer par exemple de l'absence de fuite d'informations confidentielles appartenant à l'entreprise ou encore de risques faisant encourir sa responsabilité de commettant[30]. Dès lors, se pose une nouvelle fois la question de savoir comment peuvent s'exercer les droits respectifs de l'entreprise et de ses salariés, notamment au travers de l'usage des moyens de chiffrement sur le lieu et à l'occasion du travail.

Après avoir explicité les décisions essentielles susceptibles de nous guider en la matière (2.1), nous nous attacherons à énoncer les recommandations qui devraient être mises en œuvre dans les chartes pour se conformer aux dernières constructions jurisprudentielles (2.2).

2.1 Etat de la jurisprudence en matière de surveillance sur les lieux de travail : la révision de l'arrêt « Nikon »

C'est en particulier à l'occasion de d'un arrêt de la chambre sociale de la Cour de cassation du 18 octobre 2006, que la jurisprudence « *Nikon* » (2001) – qui avait posé les fondements de la protection de la vie privée du salarié au temps et sur les lieux du travail – a trouvé son parachèvement au travers d'une affaire mettant en cause le licenciement pour faute grave d'un salarié qui a mis en œuvre, sans autorisation, des moyens de chiffrement pour protéger l'ensemble des données présentes sur son ordinateur, ce qui constituait, ainsi que l'a jugé la Cour, une entrave au contrôle et à l'accès aux données professionnelles qui doivent pouvoir être exercés, tout à fait légitimement, par l'employeur.

[29] Conformément à l'article 34 de la loi nr 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi nr 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : « *Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.* »

[30] Sur ce sujet, lire par exemple notre article paru dans la Lettre Technique de l'ingénieur/SSI (janvier 2007) : *Agissements personnels des salariés sur l'Internet, la Cour d'appel statue sur la responsabilité de l'entreprise.*

Une jurisprudence à l'origine très protectrice des salariés. – C'est l'**arrêt « *Nikon* »**[31] qui s'est d'abord imposé comme l'arrêt de référence dans le domaine de la cybersurveillance des salariés, posant les jalons d'une jurisprudence particulièrement protectrice des droits et libertés fondamentales des salariés. Dans cette décision, la Cour de cassation avait jugé, dans un attendu de principe à l'interprétation rigide, que le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée, celle-ci impliquant en particulier le secret des correspondances, puis en avait déduit que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur.

Plus audacieux encore, les juges de la Cour d'appel de Bordeaux, dans un **arrêt « Cegelec »** rendu le 1er juillet 2003[32], ont décidé qu'ont le caractère de messages personnels les messages envoyés et reçus par un salarié sur une adresse électronique générique de l'entreprise dans le cadre de son travail, dès lors qu'ils sont consultables sur son seul poste[33]. Comme le commentait le Forum des droits sur l'Internet, « *une telle reconnaissance, très large, du caractère personnel des messages semble donc condamner tout contrôle de l'employeur sur le courrier électronique des salariés, quant bien même il aurait respecté toutes les formalités nécessaires. Si on peut voir dans cette décision une avancée importante dans le domaine de la reconnaissance d'une vie privée pour le salarié au sein de l'entreprise, il n'est pas sûr qu'elle soit bien opportune ne serait-ce qu'au regard des risques de communication par des salariés indélicats de données confidentielles.* »

Plusieurs décisions postérieures ont finalement permis de relativiser la portée de ces décisions très favorables aux salariés, en opérant un retour à plus juste équilibre des droits et notamment le droit légitime de l'employeur à contrôler l'activité de ses salariés.

Le retour à un compromis plus réaliste : la présomption de caractère professionnel. – Après les prémisses de l'arrêt du 19 mai 2004[34], un premier tempérament aux principes posés par l'arrêt « *Nikon* » est apporté par la décision « Cathnet-Science » du 17 mai 2005[35], décision par laquelle la cour de cassation reconnaît la possibilité pour l'employeur de prendre connaissance de fichiers identifiés par le salarié comme personnels, hors sa présence, si un « ***risque ou***

[31] Arrêt de la chambre sociale de la Cour de cassation en date du 2 octobre 2001 (pourvoi nr 99-42.942). A consulter sur le site de la Cour de cassation : http ://www.courdecassation.fr/jurisprudence_publications_documentation _2/actualite_jurisprudence_21/chambre_sociale_576/arrets _577/br_arret_1159.html

[32] A consulter sur le site du forum des droits sur l'Internet :`http://www.foruminternet.org/telechargement/documents/ca-bor20030701.pdf`

[33] La Cour relève ainsi : « *si la salariée a utilisée pour l'envoi et la réception de ses courriers électroniques l'adresse générique de l'entreprise [l'adresse était du type nomdelasociéte@nomdelasociété.com], il ne s'ensuit pas pour autant que les messages envoyés et les messages reçus en réponse étaient diffusés sur l'ensemble des postes informatiques de l'entreprise. Les messages en question étaient au contraire individualisés et n'étaient émis et reçus que depuis le poste informatique utilisé* » par la salariée.

[34] Cass.crim., 19 mai 2004 : Jean-François L. / Nortel Europe : condamnation pour abus de confiance d'un salarié qui a détourné l'usage de la messagerie électronique et de la connexion Internet mis à sa disposition par l'entreprise, pour gérer – à des fins personnelles et illicites - un site à caractère pornographique et échangiste [http ://www.legalis.net/jurisprudence-decision.php3 ?id_article=1785].

[35] Consultable sur : `http://www.legalis.net/jurisprudence-decision.php3?id\_article=1436`

un évènement particulier » le justifie. Comme le commente très finement Sandrine Rouja[36] en l'absence de définition précise de ces termes (notions néanmoins déjà connus dans le cadre de la jurisprudence en matière de fouille sur le lieu de travail), ce risque ou événement particulier devra, pour affranchir l'employeur de la présence du salarié (ou de son aval[37]), avoir un degré de gravité certain et se rapporter à la sécurité de l'entreprise, et enfin il revêtira en principe un caractère d'urgence...

Par deux arrêts rendus le même jour, en date du 18 octobre 2006, la Cour va encore plus loin et parachève l'édifice jurisprudentiel construit depuis 2001 en posant une **présomption (simple) de caractère professionnel** des documents, fichiers ou dossiers (on y inclura *a fortiori* les courriers électroniques) présents dans le bureau ou stockés sur le disque dur de l'ordinateur du salarié. Ce faisant, elle inverse la charge de la preuve et tout document ou fichier informatique trouvé dans le bureau ou sur le PC mis à disposition du salarié doit être considéré comme professionnel, sauf au salarié à prouver qu'il les a identifiés comme personnels.

Ainsi, dans la première affaire (pourvoi nr 04-47400)[38], la Cour de cassation estime que « *les documents détenus par le salarié dans le bureau de l'entreprise mis à sa disposition sont, sauf lorsqu'il les identifie comme étant personnels, présumés avoir un caractère professionnel, en sorte que l'employeur peut y avoir accès hors sa présence* ». En l'espèce, il s'agit d'un salarié qui a été licencié pour faute lourde après la découverte dans son bureau de documents provenant de son précédent employeur, estimés confidentiels et dont la présence indue était susceptible, selon la lettre de licenciement, d'engager la responsabilité de l'entreprise

Dans la seconde affaire (pourvoi nr 04-48.025) – décision que nous mettons en annexe du présent article –, les juges réitèrent la même règle[39] et en déduisent également, c'est là le second apport des arrêts du 18 octobre 2006, la **garantie d'un libre accès** aux fichiers et dossiers qui sont présumés professionnels. Dès lors,les salariés se voient interdits en particulier (faits de l'espèce) de chiffrer, sans l'autorisation de l'employeur, l'ensemble des données de leur disque dur, l'utilisation de moyens de cryptographie constituant une entrave au contrôle que peut légitimement exercer l'entreprise.

Tandis que certains qualifient ces décisions récentes de « nouveau recul de la Cour de cassation »[40] au détriment de la protection des salariés, nous parlerons plutôt d'une solution empreinte de pragmatisme et qui permet de réguler harmonieusement[41] les rapports d'employeur à salarié dans le cadre de la surveillance sur les lieux de travail. A cet égard, le rôle des chartes de sécurité

[36] *Les justifications de l'ouverture des fichiers personnels du salarié par l'employeur* - Juriscom.net : `http://www.juriscom.net/actu/visu.php?ID=702`

[37] « (...) *ou celui-ci dûment appelé,* (...) ».

[38] Texte de la décision accessible sur : `http://www.davidtate.fr/spip.php?article807`

[39] « *Mais attendu que les dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors sa présence.* »

[40] http ://droitsocialparis10.free.fr/dotclear/index.php ?2006/11/22/15-la-protection-des-salaries-contre-les-intrusions-dans-les-documents-personnels-nouveau-recul-de-la-chambre-sociale-de-la-cour-de-cassation

[41] En ce sens, lire le blog de Me Olivier Iteanu, Raoul Fuentes et Nina Bitoun : *Le juge judiciaire, premier régulateur de l'Internet ?* - `http://blog.iteanu.com/index.php?2007/01/24/5-le-juge-judiciaire-premier-regulateur-de-l-internet`

ou d'utilisation des outils informatiques s'en trouve très clairement renforcé car elles permettent de fixer les « règles du jeu » au sein des entreprises.

2.2 Les chartes, des outils de réglementation à la légitimité renforcée

L'encadrement des moyens informatiques mis à disposition du salarié dans l'entreprise est appréhendé aujourd'hui comme une exigence de sécurité par l'employeur qui va devoir maintenant tirer les enseignements de la nouvelle construction jurisprudentielle retenue par la Cour de cassation dans les arrêts précités.

S'agissant de la présomption de caractère professionnel au bénéfice du PC du salarié. – « *Ne nous y trompons pas* », écrivent Mes Barbry et Dufief[42], les récentes décisions qui ont ravivé le débat de la vie privée du salarié sur son lieu de travail « *ne signifie*(nt) *pas pour l'employeur que tout est*(désormais) *permis* ! ».

Ainsi, les apports de l'arrêt *Nikon*demeurent et les salariés ne peuvent se voir interdire l'usage résiduel des outils informatiques mis à leur disposition à des fins personnelles. De même, l'employeur ne peut prendre connaissance du contenu des fichiers ou messages personnels de son salarié, sauf les tempéraments apportés par la jurisprudence :

1. risque ou évènement particulier (arrêt du 17 mai 2005) ;
2. absence de signe apparent permettant d'identifier le fichier ou dossier comme ayant un caractère personnel (arrêt du 18 octobre 2006).

Dès lors, il résulte de cet apport de la jurisprudence la recommandation pratique qui consiste à obliger les salariés à opérer une « discrimination » positive de leurs fichiers, dossiers ou messages ayant un caractère privé. Sur ce point, notons que la détermination du caractère personnel est simple dès lors que le répertoire, dans son intitulé, ou le nom du ou des fichiers revêtent de manière apparente leur caractère privé (« personnel », « private », « PRV »...). Il en va différemment dès le moment où ce caractère privé ne ressort plus ni de l'intitulé du fichier (ou de l'objet du message), ni du lieu de sauvegarde (répertoire nommé « Personnel », disquette étiquetée « personnel », ou encore sur une clé USB personnelle, ...) ..., mais seulement de leur contenu.

Concernant plus particulièrement les messages électroniques, il apparaît toutefois que la règle de « l'identification positive » est imparfaite car elle ne permet pas de maîtriser correctement les flux entrants. Dès lors, il ressort de la responsabilité du salarié qui veut protéger sa vie privée de renommer le champ Objet des messages concernés ou de les sauvegarder dans un répertoire approprié. Suivant les recommandations du Forum des Droits sur l'Internet, dans son rapport « Relations du travail et Internet » du 17 septembre 2002, un pouvoir de requalification des messages pourrait également être dévolu aux administrateurs systèmes qui, par leur fonction, peuvent avoir accès aux

[42] *Cybersurveillance des salariés : la cour de cassation simplifie le débat* – Le Journal du Net, 7/12/2006 : `http://www.journaldunet.com/juridique/juridique061207.shtml`

messageries et à leur contenu[43]. Enfin, en cas d'absence du salarié, certains[44] recommandent la mise en place d'un message automatique d'absence précisant la personne assurant l'intérim et à contacter dans l'entreprise. Les expéditeurs de correspondances professionnelles sont ainsi invités à rediriger leurs messages, l'entreprise s'abstenant d'entrer dans la messagerie du salarié absent où l'attendent en principe, par l'effet du tri induit par le message d'absence, ses correspondances privées.

S'agissant plus généralement des fichiers informatiques stockés sur le PC du salarié, on rappellera simplement la faculté pour l'employeur de prévoir un espace de « vie privée résiduelle » qui pourra être limité par exemple à la fois en taux d'occupation de la mémoire de stockage et au regard d'un périmètre réseau défini (cas des systèmes classifiés / non classifiés).

En définitive, notons que c'est le principe de proportionnalité qui guidera les juges dans l'appréciation des mesures restrictives de liberté prises par les employeurs, et dont on peut attendre la plus grande vigilance pour autoriser les atteintes à des droits et libertés fondamentales des salariés.

S'agissant de la garantie de libre accès aux fichiers présumés professionnels. – Dans le second arrêt précité du 18 octobre 2006,les juges ont pu décider que « *la cour d'appel, qui a constaté que M. *** avait procédé volontairement au cryptage*[45] *de son poste informatique, sans autorisation de la société faisant ainsi obstacle à la consultation, a pu décider, sans encourir les griefs du moyen, que le comportement du salarié, qui avait déjà fait l'objet d'une mise en garde au sujet des manipulations sur son ordinateur, rendait impossible le maintien des relations contractuelles pendant la durée du préavis et constituait une faute grave* ». Il en résulte, comme nous le mentionnions plus haut, une garantie de libre accès qui doit assurer à l'employeur la possibilité de consulter à tout moment les fichiers ou dossiers présumés professionnels.

Dès lors, l'employeur aura soin de réglementer de façon très précise, en fonction de la politique de classification des documents comme du profil des utilisateurs (exigences spécifiques pour les utilisateurs « nomades »), l'utilisation des fonctions de sécurité applicables aux fichiers de l'entreprise, qu'il s'agisse d'une simple protection par un mot de passe ou de l'application de moyens de chiffrement dont elle aura par ailleurs intérêt à maîtriser l'origine.

L'organisation pourra par exemple décider d'utiliser une version d'un logiciel de chiffrement « approuvée » par la DCSSI[46], excluant par cette politique tous téléchargements par les utilisateurs de moyens « libres » de chiffrement. De plus, si l'obligation de remise des conventions secrètes - initialement prévue dans le projet de loi de la LEN[47] - à l'encontre des « *personnes (physiques comme morales) qui fournissent des moyens de cryptologie visant à assurer une fonction de confidentialité* », n'a pas finalement pas été retenue, il est certain que les entreprises ont intérêt à pouvoir collaborer

[43] Ce qui n'est contraire, conformément à la position de la CNIL exprimée dans son Rapport du 5 février 2002 sur la cybersurveillance, à aucune disposition de la loi Informatique et Libertés du 6 janvier 1978. En ce sens également, l'arrêt de la Cour d'Appel de Paris du 17 décembre 2001 : « *il est dans la fonction des administrateurs de réseaux d'assurer le fonctionnement normal de ceux-ci ainsi que leur sécurité, ce qui entraîne, entre autre, qu'ils aient accès aux messageries et à leur contenu, ne serait-ce que pour les débloquer ou éviter des démarches hostiles* ».

[44] En ce sens, Xavière Caporal, *La réglementation par l'employeur de l'utilisation des moyens informatiques mis à disposition du salarié au sein de l'entreprise* : `http://www.legalbiznext.com/droit/La-reglementation-par-l-employeur`

[45] Anglicisme (malheureux) désignant le chiffrement des données.

[46] Cf. Système Acid Cryptofiler du ministère de la défense utilisé pour le chiffrement de données gouvernementales sensibles

[47] Cf article 26 du projet : http ://www.assemblee-nationale.fr/12/projets/pl0528.asp)

au mieux avec les instances judiciaires en ayant la posture des « poursuivants » et donc, d'organiser les conditions de nature à permettre la remise aux autorités de la version en clair de toutes données chiffrées de l'entreprise (rapprochement avec les dispositions de l'article 37 denier alinéa de la loi du 21 juin 2004).

3 Conclusion. –

Outils essentiels de la sécurité et de la confiance dans les transactions financières et commerciales ainsi que les communications électroniques dans leur ensemble, les techniques de cryptographie jouent un rôle croissant en matière de protection contre la fraude informatique, de sécurité des données ou encore de protection de la confidentialité des correspondances. C'est la reconnaissance de ces besoins de sécurité dans notre société de l'information qui a permis d'aboutir à l'une des dispositions les plus remarquables de la loi pour la confiance dans l'économie numérique : la libéralisation complète de l'utilisation des moyens de cryptologie.

Il n'en demeure pas moins cependant que la mise en œuvre de ces moyens doit demeurer sous la maîtrise des organisations, afin de parer à différents risques de sécurité dont, en particulier, la fuite d'informations confidentielles sous couvert de données « privées » des salariés. En effet, l'employeur n'ayant pas accès au contenu de ces données protégées en vertu du sacro-saint principe de droit au respect de la vie privée et de secret des correspondances, le chiffrement des données personnelles des utilisateurs fait entrave au contrôle qui peut légitimement être mis en œuvre par l'entreprise (ex. analyse par agent logiciel sur la base d'une liste de mots clés susceptible de révéler la présence de données de l'entreprise).

En définitive, les récentes constructions jurisprudentielles en matière de surveillance sur les lieux de travail vont accroître encore la légitimité des « chartes » relatives à l'utilisation des moyens informatiques de l'entreprise. Ces documents servent en effet de plus en plus de référence pour les juges qui fondent sur eux leur appréciation à la fois quant à la détermination de la nature (privé/professionnel) des fichiers ou messages soumis à son examen[48] et aussi quant à la légalité des restrictions à l'exercice d'une vie privée résiduelle par les salariés et des modalités de contrôle prévues au sein de l'entreprise.

[48] Voir par exemple : Conseil de prud'hommes de Nanterre, 15 septembre 2005 (à propos du licenciement pour faute grave d'un salarié qui a communiqué des informations confidentielles à une banque concurrente, les juges relèvent que la mention « PRV » imposée dans la charte de l'entreprise pour signaler les messages à caractère privé ne figure pas sur les courriers électroniques produits à titre de preuve et dès lors, considèrent que le secret de la correspondance privée n'a pas été violé par l'employeur qui a accédé au contenu de ces messages)- `http://forum-internet.org/texte/documents/jurisprudence/lire.phtml?id=980`

4 Annexes

[1] Loi nr 2004-575 du 21 juin 2004, Titre III, chapitre 1er « Moyens et prestations de cryptologie »
[2] Cass.Soc., 18 octobre 2006 – Jérémy L.F. / Techni-soft : vie privée – salarié – licenciement – cryptographie

4.1 Annexe 1 : LOI nr 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

Publié au Journal officiel de la République française nr 143 du 22 juin 2004, page 1168.

[...]

TITRE III DE LA SÉCURITÉ DANS L'ÉCONOMIE NUMÉRIQUE
CHAPITRE Ier Moyens et prestations de cryptologie

Article 29

On entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité.

On entend par prestation de cryptologie toute opération visant à la mise en œuvre, pour le compte d'autrui, de moyens de cryptologie.

Section 1
Utilisation, fourniture, transfert, importation et exportation de moyens de cryptologie

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 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.

Section 2 Fourniture de prestations de cryptologie

Article 31

I. - La fourniture de prestations de cryptologie doit être déclarée auprès du Premier ministre. Un décret en Conseil d'Etat définit les conditions dans lesquelles est effectuée cette déclaration et peut prévoir des exceptions à cette obligation pour les prestations dont les caractéristiques techniques ou les conditions de fourniture sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, cette fourniture peut être dispensée de toute formalité préalable.

II. - Les personnes exerçant cette activité sont assujetties au secret professionnel, dans les conditions prévues aux articles 226-13 et 226-14 du code pénal.

Article 32

Sauf à démontrer qu'elles n'ont commis aucune faute intentionnelle ou négligence, les personnes fournissant des prestations de cryptologie à des fins de confidentialité sont responsables au titre de ces prestations, nonobstant toute stipulation contractuelle contraire, du préjudice causé aux personnes leur confiant la gestion de leurs conventions secrètes en cas d'atteinte à l'intégrité, à la confidentialité ou à la disponibilité des données transformées à l'aide de ces conventions.

Article 33

Sauf à démontrer qu'ils n'ont commis aucune faute intentionnelle ou négligence, les prestataires de services de certification électronique sont responsables du préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats présentés par eux comme qualifiés dans chacun des cas suivants :

1° Les informations contenues dans le certificat, à la date de sa délivrance, étaient inexactes ;

2° Les données prescrites pour que le certificat puisse être regardé comme qualifié étaient incomplètes ;

3° La délivrance du certificat n'a pas donné lieu à la vérification que le signataire détient la convention privée correspondant à la convention publique de ce certificat ;

4° Les prestataires n'ont pas, le cas échéant, fait procéder à l'enregistrement de la révocation du certificat et tenu cette information à la disposition des tiers.

Les prestataires ne sont pas responsables du préjudice causé par un usage du certificat dépassant les limites fixées à son utilisation ou à la valeur des transactions pour lesquelles il peut être utilisé, à condition que ces limites figurent dans le certificat et soient accessibles aux utilisateurs.

Ils doivent justifier d'une garantie financière suffisante, spécialement affectée au paiement des sommes qu'ils pourraient devoir aux personnes s'étant fiées raisonnablement aux certificats qualifiés qu'ils délivrent, ou d'une assurance garantissant les conséquences pécuniaires de leur responsabilité civile professionnelle.

Section 3 Sanctions administratives

Article 34

Lorsqu'un fournisseur de moyens de cryptologie, même à titre gratuit, ne respecte pas les obligations auxquelles il est assujetti en application de l'article 30, le Premier ministre peut, après avoir mis l'intéressé à même de présenter ses observations, prononcer l'interdiction de mise en circulation du moyen de cryptologie concerné.

L'interdiction de mise en circulation est applicable sur l'ensemble du territoire national. Elle emporte en outre pour le fournisseur l'obligation de procéder au retrait :

1° Auprès des diffuseurs commerciaux, des moyens de cryptologie dont la mise en circulation a été interdite ;

2° Des matériels constituant des moyens de cryptologie dont la mise en circulation a été interdite et qui ont été acquis à titre onéreux, directement ou par l'intermédiaire de diffuseurs commerciaux.

Le moyen de cryptologie concerné pourra être remis en circulation dès que les obligations antérieurement non respectées auront été satisfaites, dans les conditions prévues à l'article 30.

Section 4 Dispositions de droit pénal

Article 35

I. - Sans préjudice de l'application du code des douanes :

1° Le fait de ne pas satisfaire à l'obligation de déclaration prévue à l'article 30 en cas de fourniture, de transfert, d'importation ou d'exportation d'un moyen de cryptologie ou à l'obligation de communication au Premier ministre prévue par ce même article est puni d'un an d'emprisonnement et de 15 000 € d'amende ;

2° Le fait d'exporter un moyen de cryptologie ou de procéder à son transfert vers un Etat membre de la Communauté européenne sans avoir préalablement obtenu l'autorisation mentionnée à l'article 30 ou en dehors des conditions de cette autorisation, lorsqu'une telle autorisation est exigée, est puni de deux ans d'emprisonnement et de 30 000 € d'amende.

II. - Le fait de vendre ou de louer un moyen de cryptologie ayant fait l'objet d'une interdiction administrative de mise en circulation en application de l'article 34 est puni de deux ans d'emprisonnement et de 30 000 e d'amende.

III. - Le fait de fournir des prestations de cryptologie visant à assurer des fonctions de confidentialité sans avoir satisfait à l'obligation de déclaration prévue à l'article 31 est puni de deux ans d'emprisonnement et de 30 000 e d'amende.

IV. - Les personnes physiques coupables de l'une des infractions prévues au présent article encourent également les peines complémentaires suivantes :

1° L'interdiction, suivant les modalités prévues par les articles 131-19 et 131-20 du code pénal, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés, et d'utiliser des cartes de paiement ;

2° La confiscation, suivant les modalités prévues par l'article 131-21 du code pénal, de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;

3° L'interdiction, suivant les modalités prévues par l'article 131-27 du code pénal et pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise ;

4° La fermeture, dans les conditions prévues par l'article 131-33 du code pénal et pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

5° L'exclusion, dans les conditions prévues par l'article 131-34 du code pénal et pour une durée de cinq ans au plus, des marchés publics.

V. - Les personnes morales sont responsables pénalement, dans les conditions prévues par l'article 121-2 du code pénal, des infractions prévues au présent article. Les peines encourues par les personnes morales sont :

1° L'amende, suivant les modalités prévues par l'article 131-38 du code pénal ;

2° Les peines mentionnées à l'article 131-39 du code pénal.

VI. - L'article L. 39-1 du code des postes et télécommunications est complété par un 4° ainsi rédigé :

« 4° De commercialiser ou de procéder à l'installation d'appareils conçus pour rendre inopérants les téléphones mobiles de tous types, tant pour l'émission que pour la réception, en dehors des cas prévus à l'article L. 33-3. »

Article 36

Outre les officiers et agents de police judiciaire agissant conformément aux dispositions du code de procédure pénale et, dans leur domaine de compétence, les agents des douanes agissant conformément aux dispositions du code des douanes, les agents habilités à cet effet par le Premier ministre et assermentés dans des conditions fixées par décret en Conseil d'Etat peuvent rechercher et constater par procès-verbal les infractions aux dispositions des articles 30, 31 et 34 de la présente loi et des textes pris pour leur application.

Les agents habilités par le Premier ministre mentionnés à l'alinéa précédent peuvent accéder aux moyens de transport, terrains ou locaux à usage professionnel, à l'exclusion des parties de ceux-ci affectées au domicile privé, en vue de rechercher et de constater les infractions, demander la communication de tous les documents professionnels et en prendre copie, recueillir, sur convocation ou sur place, les renseignements et justifications. Les agents ne peuvent accéder à ces locaux que pendant leurs heures d'ouverture lorsqu'ils sont ouverts au public et, dans les autres cas, qu'entre 8 heures et 20 heures.

Le procureur de la République est préalablement informé des opérations envisagées en vue de la recherche des infractions. Il peut s'opposer à ces opérations. Les procès-verbaux lui sont transmis dans les cinq jours suivant leur établissement. Une copie en est également remise à l'intéressé.

Les agents habilités peuvent, dans les mêmes lieux et les mêmes conditions de temps, procéder à la saisie des moyens de cryptologie mentionnés à l'article 29 sur autorisation judiciaire donnée par ordonnance du président du tribunal de grande instance ou d'un magistrat du siège délégué par lui, préalablement saisi par le procureur de la République. La demande doit comporter tous les éléments d'information de nature à justifier la saisie. Celle-ci s'effectue sous l'autorité et le contrôle du juge qui l'a autorisée.

Les matériels et logiciels saisis sont immédiatement inventoriés. L'inventaire est annexé au procès-verbal dressé sur les lieux. Les originaux du procès-verbal et de l'inventaire sont transmis, dans les cinq jours suivant leur établissement, au juge qui a ordonné la saisie. Ils sont versés au dossier de la procédure.

Le président du tribunal de grande instance ou le magistrat du siège délégué par lui peut à tout moment, d'office ou sur la demande de l'intéressé, ordonner mainlevée de la saisie.

Est puni de six mois d'emprisonnement et de 7 500 € d'amende le fait de faire obstacle au déroulement des enquêtes prévues au présent article ou de refuser de fournir les informations ou documents y afférant.

Article 37

Après l'article 132-78 du code pénal, il est inséré un article 132-79 ainsi rédigé :

« Art. 132-79. - Lorsqu'un moyen de cryptologie au sens de l'article 29 de la loi nr 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique a été utilisé pour préparer ou commettre un crime ou un délit, ou pour en faciliter la préparation ou la commission, le maximum de la peine privative de liberté encourue est relevé ainsi qu'il suit :

« 1° Il est porté à la réclusion criminelle à perpétuité lorsque l'infraction est punie de trente ans de réclusion criminelle ;

« 2° Il est porté à trente ans de réclusion criminelle lorsque l'infraction est punie de vingt ans de réclusion criminelle ;

« 3° Il est porté à vingt ans de réclusion criminelle lorsque l'infraction est punie de quinze ans de réclusion criminelle ;

« 4° Il est porté à quinze ans de réclusion criminelle lorsque l'infraction est punie de dix ans d'emprisonnement ;

« 5° Il est porté à dix ans d'emprisonnement lorsque l'infraction est punie de sept ans d'emprisonnement ;

« 6° Il est porté à sept ans d'emprisonnement lorsque l'infraction est punie de cinq ans d'emprisonnement ;

« 7° Il est porté au double lorsque l'infraction est punie de trois ans d'emprisonnement au plus.

« Les dispositions du présent article ne sont toutefois pas applicables à l'auteur ou au complice de l'infraction qui, à la demande des autorités judiciaires ou administratives, leur a remis la version en clair des messages chiffrés ainsi que les conventions secrètes nécessaires au déchiffrement. »

Section 5 Saisine des moyens de l'Etat pour la mise au clair de données chiffrées

Article 38

Après le premier alinéa de l'article 230-1 du code de procédure pénale, il est inséré un alinéa ainsi rédigé :

« Si la personne ainsi désignée est une personne morale, son représentant légal soumet à l'agrément du procureur de la République ou de la juridiction saisie de l'affaire le nom de la ou des personnes physiques qui, au sein de celle-ci et en son nom, effectueront les opérations techniques mentionnées au premier alinéa. Sauf si elles sont inscrites sur une liste prévue à l'article 157, les personnes ainsi désignées prêtent, par écrit, le serment prévu au premier alinéa de l'article 160. »

Section 6 Dispositions diverses

Article 39

Les dispositions du présent chapitre ne font pas obstacle à l'application du décret du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions, à ceux des moyens de cryptologie qui sont spécialement conçus ou modifiés pour porter, utiliser ou mettre en œuvre les armes, soutenir ou mettre en œuvre les forces armées, ainsi qu'à ceux spécialement conçus ou modifiés pour le compte du ministère de la défense en vue de protéger les secrets de la défense nationale.

Article 40

I. - L'article 28 de la loi nr 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications est abrogé à compter de l'entrée en vigueur du présent chapitre.

II. - Les autorisations et déclarations de fourniture, d'importation et d'exportation de moyens de cryptologie délivrées ou effectuées conformément aux dispositions de l'article 28 de la loi nr 90-1170 du 29 décembre 1990 précitée et de ses textes d'application conservent leurs effets jusqu'à l'expiration du terme prévu par celles-ci. Les agréments délivrés aux organismes chargés de gérer pour le compte d'autrui des conventions secrètes de moyens de cryptologie permettant d'assurer des fonctions de confidentialité valent, pour ces moyens, déclaration au sens de l'article 31.

4.2 Annexe 2 : COUR DE CASSATION, Chambre sociale, arrêt du 18 octobre 2006[N° de pourvoi :04-48.025]-Jérémy L.F./ Techni-soft

La Cour de cassation, chambre sociale, a rendu l'arrêt suivant : Attendu que Jérémy L.F. a été engagé le 2 octobre 2000 par la société Techni-Soft en qualité d'attaché technico-commercial, par contrat à durée déterminée de six mois qui s'est poursuivi en un contrat à durée indéterminée ; que le 28 février 2002, il a été licencié pour faute grave ayant notamment consisté à empêcher l'accès à ses dossiers commerciaux sur son poste informatique de travail ; que contestant son licenciement et revendiquant le statut de VRP, il a saisi la juridiction prud'homale le 12 avril 2002 ;

Sur le premier moyen

Attendu que le salarié fait grief à l'arrêt attaqué (Rennes, 21 octobre 2004) d'avoir dit son licenciement fondé sur une faute grave, en violation de l'article L 122-14-3 du code du travail ;

Mais attendu que les dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors sa présence ; que la cour d'appel, qui a constaté que Jérémy L.F. avait procédé volontairement au cryptage de son poste informatique, sans autorisation de la société faisant ainsi obstacle à la consultation, a pu décider, sans encourir les griefs du moyen, que le comportement du salarié, qui avait déjà fait l'objet d'une mise en garde au sujet des manipulations sur son ordinateur, rendait impossible le maintien des relations contractuelles pendant la durée du préavis et constituait une faute grave ; que le moyen n'est pas fondé ;

Sur le second moyen :

Attendu que le salarié fait grief à l'arrêt de ne pas lui avoir reconnu la qualité de VRP, pour les motifs exposés au moyen, tirés d'une violation de l'article L 751-2 du code du travail ;

Mais attendu que la cour d'appel, se fondant sur les éléments de fait et de preuve versés aux débats qu'elle a souverainement appréciés, en a déduit que le salarié ne travaillait pas sur un secteur géographique déterminé, ne prenait pas des ordres, exerçait en partie des tâches administratives et n'avait pas développé une clientèle personnelle ; qu'elle a exactement décidé qu'il ne remplissait pas l'ensemble des conditions lui permettant de bénéficier du statut de VRP ;

DECISION

Par ces motifs,

. Rejette le pourvoi ;

. Condamne Jérémy L.F. aux dépens ;

. Vu l'article 700 du NCPC, rejette la demande de Jérémy L.F.

La Cour : M. Sargos (président), M. Texier (conseiller rapporteur), M. Chagny (conseiller doyen),

Avocat général : M. Duplat

Avocat : Me Odent