# DROIT PENAL NUMERIQUE

# 1) La fraude informatique

## Chapitre III : Des atteintes aux systèmes de traitement automatisé de données

**Article 323-1** Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4

Le fait **d'accéder ou de se maintenir, frauduleusement**, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la **suppression ou la modification de données** contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un **système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat**, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende.

### Article 323-2

Le fait **d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données** est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende.

### Article 323-3

Le fait **d'introduire frauduleusement des données dans un système de traitement automatisé**, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en **œuvre par l'Etat**, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende.

### Article 323-3-1

**Le fait, sans motif légitime**, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

### Article 323-4

La **participation à un groupement formé** ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

### Article 323-4-1

Lorsque les infractions prévues aux articles 323-1 à 323-3-1 ont été commises **en bande organisée** et à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à dix ans d'emprisonnement et à 300 000 € d'amende.

## Article 323-5

Les personnes physiques coupables des délits prévus au présent chapitre encourent également **les peines complémentaires suivantes :**

1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;

2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;

3° La confiscation 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 ;

4° La fermeture, 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, pour une durée de cinq ans au plus, des marchés publics ;

6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;

7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35.

## Article 323-6

Les **personnes morales déclarées responsables pénalement**, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

## Article 323-7

**La tentative des délits** prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.

## Article 323-8

**Le présent chapitre n'est pas applicable aux mesures mises en œuvre, par les agents habilités des services de l'Etat** désignés par arrêté du Premier ministre parmi les services spécialisés de renseignement mentionnés à l'article L. 811-2 du code de la sécurité intérieure, pour assurer hors du territoire national la protection des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du même code.

- L’accès frauduleux

- Le maintien frauduleux

- Les intrusions avec dommages

- L’article 323-3-1

✓ La tentative

✓ STAD de l’Etat

## 2) Les infractions commises à l'aide de l'outil informatique

### Article 313-1

**L'escroquerie** est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manoeuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge.

L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende.

### Article 314-1

**L'abus de confiance** est le fait par une personne de détourner, au préjudice d'autrui, des fonds, des valeurs ou un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les rendre, de les représenter ou d'en faire un usage déterminé.

L'abus de confiance est puni de trois ans d'emprisonnement et de 375 000 euros d'amende.

### Article 311-1

**Le vol** est la soustraction frauduleuse de la chose d'autrui.

### Article L335-2

Toute édition d'écrits, de composition musicale, de dessin, de peinture ou de toute autre production, imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est **une contrefaçon et toute contrefaçon est un délit.**

La contrefaçon en France d'ouvrages publiés en France ou à l'étranger est punie de trois ans d'emprisonnement et de 300 000 euros d'amende.

Seront punis des mêmes peines le débit, l'exportation, l'importation, le transbordement ou la détention aux fins précitées des ouvrages contrefaisants.

Lorsque les délits prévus par le présent article ont été commis en bande organisée, les peines sont portées à sept ans d'emprisonnement et à 750 000 euros d'amende.

### Article 226-4-1

- Créé par LOI n°2011-267 du 14 mars 2011 - art. 2

**Le fait d'usurper l'identité** d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende.

Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.

## Garance Mathias (Avocate) : "Dans les tests d'intrusion, tout doit être cadré par écrit"

**JDNSolutions. Jusqu'où les tests d'intrusion et les pentesteurs peuvent-ils aller ?**
**Garance Mathias.** Tout dépend de l'accord signé entre l'auditeur et l'audité. Celui-ci doit être précis et exhaustif. Il doit par exemple mentionner clairement les adresses IP concernées et les heures pendant lesquelles les tests vont être réalisés, entre autres.
Il faut un document juridique complet autorisant les accès. Certains points peuvent figurer dans l'appel d'offres, mais les détails peuvent ensuite faire l'objet d'une réunion avec l'auditeur retenu. Tout doit être cadré, avec l'accord écrit de la direction, ou de l'autorité responsable. A noter que l'accord peut être amendé en cours de test, avec une nouvelle fois la signature des parties concernées.

La seule limite infranchissable : la vie privée, qui est protégée en France. L'audit ne peut donc pas s'appuyer sur les correspondances privées, dans les mails notamment.
Plusieurs points doivent retenir la vigilance pour le contrat. Ses clauses doivent être claires. Il doit également préciser qu'il n'y a pas d'obligation de résultat. Il doit aussi être conforme à l'état de l'art. Tous les outils et logiciels utilisés pour le test doivent être listés, et validés. A noter qu'il ne faut pas oublier qu'il faut également avoir, le cas échéant, l'autorisation d'accéder aux adresses IP d'un tiers, celles d'un hébergeur par exemple. Ce dernier doit aussi donner son accord écrit.

**"La seule limite infranchissable : la vie privée"**

**Les tests peuvent-ils alors avoir recours à l'ingénierie sociale ? Certains employés peuvent se sentir manipulés...**
L'ingénierie sociale passant par l'intrusion dans des correspondances privées, elle n'est donc pas légale. En revanche, l'auditeur peut par exemple se faire passer pour un technicien informatique, s'il a l'accord de la direction. Si personne ne vérifie que le soi disant technicien en est bien un avant de le laisser entrer, c'est bien qu'il y a une faute, qui va servir de faille.

**Y-a-il déjà eu des plaintes ?**
Avant de penser à un procès, il peut toujours y avoir discussion. Cela peut être la solution préférable pour des raisons d'images, car la SSII attaquée qui a effectué le test ne goûterait guère une telle publicité.

Cependant, pénétrer un système de traitement automatique de données et agir sur celui-ci sans autorisation est bien puni par la loi. Cela relève du code pénal. Les peines prévoient des amendes et de la prison ferme.

Test d'intrusions, quels risques juridiques ?

# Le vol de données informatiques

**Article juridique** publié le **11/12/2015 à 10:48**, vu **1411 fois**, 3 commentaire(s), Auteur : Noé MARMONIER

***La "technologisation" rend plus friable les remparts de protection des données informatiques. Toute entreprise ou administration publique peut être exposée à une intrusion dans son système informatique et à un pillage des données. Ces données n'en demeurent pas moins des biens, propriété exclusive de l'entité qui les détient. L'intrusion dans le système informatique de cet établissement constitue une infraction pénale.***

L'introduction dans un système de traitement automatisé de données et le maintien dans ce système, après découverte de son caractère protégé, caractérise le délit de maintien frauduleux dans un système de traitement automatisé de données, (STAD), article 323-1 du Code pénal et un vol, article 311-1 et 311-3 du Code pénal.

L'objectif de cette intrusion est la captation des données informatiques qui composent le STAD.

Les enjeux ne sont pas neutres, impliquant la violation de données confidentielles, de secrets d'affaires ou de droit de propriété intellectuelle.

De plus en plus fréquemment, les juridictions ont à connaitre de cette infraction complexe.

La position du droit pénal évolue sur la fraude informatiques et le vol de données informatiques.

En témoigne l'arrêt rendu dans l'affaire "Bluetouff" par la chambre criminelle de la Cour de cassation le 20 mai 2015 (*n°14.81336*).

La Cour de cassation confirme la condamnation du blogueur "Bluetouff", du chef de maintien frauduleux dans un STAD... et de vol.

L'infraction de vol est-elle adaptée aux soustractions de données informatiques ? Oui, antérieurement à 2014, faute de mieux, et non aujourd'hui !

L'arrêt du 20 mai 2015 important, il illustre le changement de paradigme. La Cour retient que la captation de données informatiques, à l'insu de leur propriétaire et la fixation sur un support des données constitue un vol, au sens de l'article 311-1 du Code pénal, une soustraction frauduleuse du bien d'autrui.

La Cour retient que les données informatiques, par essence dématérialisées, constituent des biens susceptibles de faire l'objet d'une appropriation frauduleuse. La solution est curieuse.

La qualification de vol retenue en l'espèce est critiquable car le vol sanctionne une dépossession frauduleuse, or, en l'espèce, elle est retenue pour un téléchargement, dont le titulaire des données conserve une liberté d'utilisation.

Le principe de l'interprétation stricte de la loi pénale s'en est trouvé quelque peu atteint...

La qualification d'abus de confiance semble davantage appropriée et déjà retenue en jurisprudence, contre le salarié qui capte frauduleusement les données informatiques de son employeur (*C.Cass. crim. 22 octobre 2014, n°13-82630*).

Les données informatiques sont-elles devenues un bien, susceptible de soustraction frauduleuse ? NON !

Le débat semble cloturé avec la récente modification de l'article 323-3 du Code pénal, par la loi n°2014-1353 du 13 novembre 2014, qui étend le champ d'application de l'introduction dans un STAD aux actes, notamment, d'extraction frauduleuse de données.

La répression est plus sévère que le vol, cinq ans d'emprisonnement et 150.000 Euros d'amende, contre trois ans et 45.000 Euros d'amende encourus pour le vol.

La qualification de vol fait office d'infraction-relais pour les faits commis antérieurement à l'entrée en vigueur de la loi du 13 novembre 2014, plus sévère car créeant un nouvel interdit pénal (l'extraction), la répression encourue étant aussi plus sévère que le vol.

La loi nouvelle étant plus sévère, sur l'incrimination... comme sur la peine, point de rétroactivité !

La loi n°2015-912 du 24 juillet 2015 a aggravé la peine d'amende encourue de l'article 323-3 du Code pénal, passant de 75.000 Euros à 150.000 Euros.

C'est pourquoi le fondement du vol a été employé dans l'affaire "Bluetouff", même s'il est discutable.

Il est à noter que le fondement du vol n'a pas été employé dans le cadre d'une affaire examinée par le Tribunal correctionnel d'Annecy, dont le jugement a été rendu le 04 décembre 2015.

En l'espèce, une inspectrice du travail et un salarié d'une entreprise était poursuivis pour l'introduction dans un STAD d'une entreprise, et l'extraction de données de l'entreprise, informations concernant des licenciements à venir, publiées dans la presse.

Le vol n'a pas été retenu pour cette extraction, seule une condamnation pour l'accès et le maintien dans un STAD a été prononcée, démontrant ainsi, l'inadaptation de la loi pénale qui existait jusqu'à la loi du 13 novembre 2014, permettant de réprimer l'extraction de données informatiques.

Désormais, c'est le texte spécialisé de l'article 323-3 du Code pénal qu'il convient d'appliquer à la soustraction de données informatiques, conformément à l'adage *specialia generalibus derogant*.

**Le vol de données ?**

# La Cour de cassation précise les infractions entourant l'usage et la détention d'un keylogger

La Cour de cassation a rendu le 16 janvier 2018 un arrêt concernant l'usage et la détention d'un keylogger matériel. Ces enregistreurs de frappe installés en douce ont été considérés comme une atteinte à un système de traitement automatisé de données (STAD). Dans le même temps, elle a détaillé le « motif légitime » qui excuse leur détention.

Les faits qui ont conduit à cet arrêt mis en ligne par Doctrine.fr et repéré par Lexradio se sont déroulés à Nice voilà plusieurs années. Le 12 novembre 2013, très exactement, le service informatique du CHU de Nice a découvert la présence d'un keylogger matériel sur les ordinateurs de deux praticiens hospitaliers.

L'enquête s'est rapidement orientée sur un médecin contractuel, en conflit avec un professeur de l'établissement devant l'Ordre des médecins. La perquisition a été fructueuse : un keylogger a été retrouvé à son domicile, tout comme des captures d'écrans réalisées sur les deux ordinateurs en question. Des captures stockées sur une clef USB et dans l'ordinateur portable, tous les deux saisis...

Finalement, le médecin, pris la main dans le sac, a reconnu avoir acheté ce dispositif d'écoute de frappes. Il avoua l'avoir installé dans l'espoir de récupérer des courriels susceptibles de lui être utiles dans le cadre de son litige professionnel.

La cour d'appel d'Aix-en-Provence, le 8 novembre 2016, a conclu à l'atteinte à un système automatisé de données et détention « *sans motif légitime d'équipement, d'instrument de programme ou données conçus ou adaptés* » pour un tel piratage. Infractions prévues aux articles 323-1 et 323-3-1 du Code pénal.

Il fut alors condamné à quatre mois de prison avec sursis, outre la confiscation de son matériel et des intérêts civils.

## Accès à un système informatique par keylogger

Seulement, l'affaire a été portée devant la Cour de cassation. Argument du prévenu : le keylogger « *ne permet pas en lui-même l'accès aux données contenues dans un ordinateur, mais seulement la capture des caractères frappés sur le clavier* ». Nuance ! Dans son esprit, il n'y aurait donc pas d'accès frauduleux à un STAD (piratage d'un système informatique).

Mieux, soutenait-il, les ordinateurs équipés de cette oreille électronique étaient librement accessibles à tous les employés de service. Les données n'étant pas confidentielles, le critère de la fraude ne pouvait être retenu.

L'argumentaire n'a pas vraiment porté. La Cour de cassation a rejeté son pourvoi en rappelant que le keylogger lui avait permis de prendre connaissance des codes de messagerie des deux autres confrères.

Dans son analyse, la mauvaise foi, l'élément matériel et l'élément intentionnel de l'infraction ont tous été caractérisés puisque ce dispositif a été installé « *pour intercepter à leur insu, par l'espionnage de la frappe du clavier les codes d'accès et accéder aux courriels échangés par les deux praticiens* ».

Conclusion : « *se rend coupable de l'infraction prévue à l'article 323-1 du code pénal la personne qui, sachant qu'elle n'y est pas autorisée, accède à l'insu des victimes, à un système de traitement automatisé de données* ».

## Se défendre dans un litige professionnel n'est pas un « motif légitime »

Tout aussi intéressant, le Code pénal punit certes le simple fait « *d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre un ou plusieurs* » actes de piratages.

Toutefois, la disposition empêche toute condamnation dès lors que le prévenu démontre l'existence d'un « *motif légitime, notamment de recherche ou de sécurité informatique* ».

Les juges du fond, qui n'ont pas été contredits par la Cour de cassation, ont repoussé l'argumentaire de l'apprenti pirate. Selon ce dernier, la défense de sa situation professionnelle devant l'Ordre des médecins outre sa réputation entraient bien dans la liste des motifs légitimes, qui n'est pas limitative dans le marbre de la loi (du fait de l'adverbe *notamment*).

Pour la justice, au contraire, le « *motif* » exposé par à l'article 323-3-1 « *se limite aux seules personnes habilitées à assurer la maintenance et la sécurité d'un parc informatique* ». C'est là une importante précision… ou restriction apportée à cette disposition.

**Tefal : un administrateur réseau condamné pour fraude informatique**

Le tribunal correctionnel d'Annecy n'a pas reconnu le statut de lanceur d'alerte à une inspectrice du travail et à un administrateur réseau de Tefal auxquels la direction de la société reprochait d'être à l'origine de la publication de documents sur de futurs licenciements. Au contraire, par un jugement du 4 décembre 2015, le tribunal condamne le salarié pour accès et maintien frauduleux à un traitement automatisé de données, atteinte au secret des correspondances électroniques et l'inspectrice du travail pour recel de correspondances et violation du secret professionnel.

L'administrateur réseau en charge de différents comptes, en conflit avec son employeur sur le paiement d'heures supplémentaires, découvre par hasard un document dans lequel il apparaît que la société veut le licencier en utilisant des moyens déloyaux. Pour en savoir plus, il décide de consulter les serveurs sur lesquels sont stockés les fichiers des documents partagés au sein de Tefal. Il accède ainsi au répertoire des ressources humaines et découvre un document sur lequel figure les noms d'une inspectrice du travail et de son supérieur hiérarchique, ainsi que des éléments laissant entendre que la direction de Tefal exercerait des pressions sur elle. Il en fait une copie écran qu'il enregistre sur la carte SD de son téléphone portable. Il a également copié un document intitulé « msg ». Suite à sa découverte, il alerte la fonctionnaire via sa messagerie professionnelle. Celle-ci lui répond en lui conseillant d'utiliser sa messagerie personnelle. C'est ainsi que le salarié de Tefal lui a transmis les documents. L'inspectrice du travail en conflit avec sa hiérarchie, qui lui reprochait d'être trop rigide dans ses relations avec Tefal, a transmis les documents à différents syndicats de salariés qui se sont retrouvés publiés dans la presse. D'où le dépôt de plainte de la société Tefal.

Le tribunal a refusé d'appliquer le statut protecteur de lanceur d'alerte figurant à l'article L. 1132-3-3 du code du travail. En ce qui concerne l'administrateur réseau, il rappelle que ce texte de droit du travail a été créé par la loi du 6 décembre 2013, soit après les faits. Par ailleurs, « s'agissant des documents obtenus par celui-ci à la suite de son intrusion dans le système de traitement automatisé de la société Tefal, il n'en a pas eu connaissance dans l'exercice de ses fonctions, ils ne le concernaient pas personnellement et n'étaient pas nécessaires à l'exercice de sa défense dans un cadre prudhommal ». Le tribunal dit cependant que « ébranlé à la lecture du document attestant de l'intention de la société Tefal de le licencier, [il aurait pu] utiliser ultérieurement ce document, qu'il a affirmé avoir trouvé par hasard dans la photocopieuse, dans le cadre d'une action prudhommale ». Quant à l'application de ce texte à l'inspectrice du travail, le tribunal considère que « les documents diffusés aux organisations du travail par Mme P. n'ont pas été obtenus dans le cadre de l'exercice de ses fonctions, ils n'ont pas été utilisés dans le strict exercice de sa défense et il n'est pas établi qu'ils constituent un crime ou un délit ».

En revanche, le tribunal considère que l'informaticien s'est introduit et s'est maintenu frauduleusement dans le système d'information de l'entreprise, de manière intentionnelle. Il a accédé à des serveurs et consulté des fichiers sans lien avec sa fonction, s'y est maintenu dans une intention autre que celle d'exécuter son travail habituel de développement de Wifi. Par ailleurs, même s'il ne s'est pas introduit dans la boîte email du DRH, il a eu accès à ses emails, via le partage. Il l'a fait en toute connaissance de cause et en violation de la charte informatique de l'entreprise, annexée au règlement général. Selon le tribunal, l'interception, l'utilisation et le détournement de la correspondance électronique de mauvaise foi sont caractérisés.

Quant à l'inspectrice du travail, le tribunal estime que l'infraction de recel de détournement de correspondances électroniques apparaît constituée. « Elle ne pouvait ignorer, tant par le contenu

des mails, que par l'identité des destinataires, qu'ils avaient été obtenus sans l'accord des titulaires des boîtes mail ; l'évidence de cette connaissance est renforcée par l'organisation de leur envoi anonyme ». Elle n'a pas non plus respecté le secret professionnel en diffusant aux organisations syndicales des documents internes à Tefal rendant possible leur diffusion dans la presse, publication qui a conduit à l'identification du salarié auteur de la fuite et à son licenciement.
Cette décision est frappée d'appel.

1) **Rappeler les principaux délits prévus par la loi Godfrain en matière de fraude informatique**
2) **Rappelez les 3 éléments de la mise en œuvre de la responsabilité pénale**
3) **Quels sont les délits reprochés à l'administrateur réseau dans cette affaire ?**
4) **Quelle difficulté les juges doivent-ils surmonter dans ce cas concernant la culpabilité d'un administrateur réseau sur les délits de fraudes informatiques retenus ?**
5) **Quels arguments retiennent-ils dans cette affaire ?**
6) **Quelle défense est invoquée par l'administrateur réseau ?**
7) **Quelle est la décision des juges concernant l'administrateur réseau ?**

**Article L1132-3-3** Créé par LOI n°2013-1117 du 6 décembre 2013 - art. 35
Aucune personne ne peut être écartée d'une procédure de recrutement ou de l'accès à un stage ou à une période de formation en entreprise, aucun salarié ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire, directe ou indirecte, notamment en matière de rémunération, au sens de l'article L. 3221-3, de mesures d'intéressement ou de distribution d'actions, de formation, de reclassement, d'affectation, de qualification, de classification, de promotion professionnelle, de mutation ou de renouvellement de contrat, pour avoir relaté ou témoigné, de bonne foi, de faits constitutifs d'un délit ou d'un crime dont il aurait eu connaissance dans l'exercice de ses fonctions.
En cas de litige relatif à l'application du premier alinéa, dès lors que la personne présente des éléments de fait qui permettent de présumer qu'elle a relaté ou témoigné de bonne foi de faits constitutifs d'un délit ou d'un crime, il incombe à la partie défenderesse, au vu des éléments, de prouver que sa décision est justifiée par des éléments objectifs étrangers à la déclaration ou au témoignage de l'intéressé. Le juge forme sa conviction après avoir ordonné, en cas de besoin, toutes les mesures d'instruction qu'il estime utiles.

## QUELLE PROTECTION POUR LES LANCEURS D'ALERTE EN FRANCE ? 18 juillet 2022

La loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique dite loi Sapin II a créé le statut général du lanceur d'alerte et renforce ainsi les droits des personnes qui dénoncent.

La loi Sapin II prévoit l'obligation de mettre en œuvre des procédures d'alerte pour recueillir les signalements émanant du personnel ou des collaborateurs extérieurs ou occasionnels des personnes morales de droit public et les personnes de droits privé de plus de cinquante salariés.

La protection des lanceurs d'alerte a récemment été renforcée par la loi du 22 mars 2022 visant à améliorer la protection des lanceurs d'alerte qui transpose la directive (UE) 2019/1937 du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union.

**Qu'est-ce qu'un lanceur d'alerte ?**

La loi Sapin II modifiée par la loi du 22 mars dernier définit le lanceur d'alerte comme une personne physique qui signale ou divulgue, sans contrepartie financière directe et de bonne foi, des informations portant sur un crime ou un délit, une menace ou un préjudice pour l'intérêt général, une violation ou une tentative de dissimulation d'une violation de droit international ou de l'Union Européenne, de la loi ou du règlement. La condition de désintéressement prévue par la loi Sapin II a été remplacée par la notion d'absence de contrepartie financière.

Par ailleurs, il n'est plus nécessaire que l'objet du signalement soit « grave et manifeste » ni que le lanceur d'alerte ait eu personnellement connaissance des faits qu'il signale, exception faite des informations qui n'auraient pas été obtenues dans le cadre professionnel.

Les faits, informations ou documents couverts par le secret de la défense nationale, le secret médical, le secret judiciaire ou le secret professionnel entre un avocat et son client sont exclus du régime de l'alerte.

**Une protection étendue à l'entourage du lanceur d'alerte**

Dans le cadre des débats sur la transposition de la directive, le Défenseur des droits a suggéré de permettre aux personnes morales telles que les organisations syndicales et les associations de bénéficier du statut de facilitateur au sens de la directive européenne. La loi du 22 mars 2022 a étendu certaines protections offertes aux lanceurs d'alerte notamment la protection contre les représailles, aux personnes physiques et aux personnes morales à but non lucratif qui sont en lien avec les lanceurs d'alerte.

**Une simplification des canaux de signalement**

Sous l'empire de la loi Sapin II, la protection du lanceur d'alerte était conditionnée au fait que la procédure graduée (signalement d'abord adressé au supérieur hiérarchique puis en cas d'inaction aux autorités administratives et judiciaires et en dernier ressort au public) soit respectée. Cette procédure entrainait un risque accru de représailles. Désormais, le lanceur d'alerte peut donc choisir entre le signalement interne et le signalement externe aux autorités compétentes ou au Défenseur des droits. La divulgation publique ne sera possible que dans certaines conditions : absence de traitement d'un signalement externe dans un certain délai, risques de représailles, danger grave et imminent.

La loi Sapin II a instauré une protection contre les représailles judiciaires pouvant intimider les lanceurs d'alerte. En effet, les comportements visant à empêcher la révélation de faits (en faisant obstacle au signalement par exemple) ou à nuire aux lanceurs d'alerte sont sanctionnés pénalement et civilement.

La loi Sapin II a également instauré une protection contre les représailles professionnelles pouvant décourager les lanceurs d'alerte dans le secteur privé et pour les fonctionnaires. En effet, les lanceurs d'alerte ne peuvent faire l'objet de mesures de rétorsion (sanction, licenciement, mesure discriminatoire directe ou indirecte en termes de rémunération, reclassement, affectation, qualification, classification, promotion professionnelle, mutation ou renouvellement de contrat) et il ne peut être fait obstacle à leur recrutement ou sélection pour avoir dénoncer des faits. Les lanceurs d'alerte bénéficient d'un allégement de la charge de la preuve pour prouver ce type de représailles

en cas de contentieux.

La loi du 22 mars 2022 a complété la liste des représailles interdites (intimidation, atteinte à la réputation sur les réseaux sociaux, orientation abusive vers des soins…).

**L'irresponsabilité pénale du lanceur d'alerte en cas de révélation d'un secret protégé par la loi**

Le régime de protection est également complété par un régime d'irresponsabilité pénale du lanceur d'alerte qui révélerait un secret protégé par la loi, à condition que cette divulgation soit nécessaire et proportionnée à la sauvegarde des intérêts en cause, qu'elle intervienne dans le respect des procédures de signalement prévues par la loi et que la personne réponde aux critères de définition du lanceur d'alerte.

La loi du 22 mars 2022 a précisé que toute personne qui soustrait, détourne ou recèle des documents contenant les informations dont il a eu connaissance de manière licite et qu'il signale ou divulgue ne sera pas pénalement responsable.

**L'instauration d'une garantie de préservation de l'anonymat**

La loi précise que les procédures de signalement mises en œuvre par les acteurs publics et privés doivent « garantir une stricte confidentialité de l'identité des auteurs du signalement ». Les éléments de nature à identifier le lanceur d'alerte ne peuvent ainsi être divulgués, sauf à l'autorité judiciaire, qu'avec le consentement de celui-ci. Le fait de divulguer des éléments confidentiels est sanctionné pénalement.

## Dossier 2 : Le nouveau statut des lanceurs d'alertes

1) **Quelles sont les caractéristiques d'un lanceur d'alertes**
2) **De quelles protections un lanceur d'alertes bénéficie-t-il ?**
3) **Comment faire un signalement dans ce cadre ?**

---

**Affaire Tefal : la condamnation d'une inspectrice du travail confirmée en cassation**

Après sept ans de procédure judiciaire, Laura Pfeiffer a été sanctionnée pour violation du secret professionnel et recel de documents confidentiels appartenant à la filiale du groupe Seb.
Par Bertrand Bissuel Publié le 11 mars 2021

Laura Pfeiffer vient de perdre une manche décisive dans la bataille judiciaire qui l'oppose, depuis un peu plus de sept années, à la société Tefal. Le 3 mars, la Cour de cassation a confirmé la condamnation prononcée contre cette inspectrice du travail qui se voyait reprocher deux infractions pénales : la violation du secret professionnel et le recel de documents obtenus au prix d'une atteinte au secret des correspondances électroniques. L'arrêt rendu par la chambre criminelle de la haute juridiction constitue le énième épisode d'un feuilleton hors du commun – souvent présenté comme « l'affaire Tefal » –, qui a déclenché, pendant des mois, de fortes turbulences au ministère du travail. Une histoire à tiroirs, qui n'est pas encore tout à fait terminée.
Les faits incriminés portent sur des e-mails envoyés et reçus en 2013 par la direction de l'usine Tefal à Rumilly (Haute-Savoie). Ils avaient été communiqués à Laura Pfeiffer par un salarié de l'entreprise, Christophe M., qui se les était procurés de façon illicite. Ces courriels pouvaient accréditer l'idée qu'il y avait une collusion entre le fabricant d'articles de cuisine et Philippe Dumont, le supérieur hiérarchique de l'inspectrice du travail, afin que celle-ci change de comportement et se montre plus indulgente à l'égard des patrons du site de Rumilly. Persuadée que son chef relayait les pressions de Tefal, la fonctionnaire avait communiqué les courriels en question à plusieurs syndicats et la querelle avait fait à la « une » de L'Humanité, en décembre 2013.
L'industriel avait déposé une plainte contre X pour « introduction frauduleuse dans un système de traitement automatisé de données ». Les investigations avaient permis d'identifier l'inspectrice du travail et sa « taupe », Christophe M. Tous deux avaient été condamnés, en première instance puis en appel – Laura Pfeiffer se voyant

infliger 3 500 euros d'amende avec sursis.
Eventuels prolongements de l'affaire
L'agent de contrôle avait saisi la Cour de cassation, en revendiquant le statut de « lanceuse d'alerte » désireuse de signaler un délit : en l'occurrence, la tentative de Tefal d'entraver son action, avec la complicité de son supérieur hiérarchique. La notion de lanceur d'alerte ayant évolué depuis la loi dite « Sapin II » de décembre 2016, la Cour de cassation avait estimé, en 2018, qu'il fallait réexaminer le dossier. Un nouveau procès avait donc eu lieu devant la cour d'appel de Lyon : une fois de plus, les débats avaient tourné en défaveur de Laura Pfeiffer.

Commentaire : Le statut de lanceur d'alerte ?