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](https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=2417FDCDA2EF2AC7953BD0A28BCD3F77.tpdila09v_1?cidTexte=JORFTEXT000030931899&idArticle=LEGIARTI000030933630&dateTexte=20150727)

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](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000006418314&dateTexte=&categorieLien=cid) 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](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000006418314&dateTexte=&categorieLien=cid) 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,](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000006417202&dateTexte=&categorieLien=cid)des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par [l'article 131-38](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000006417333&dateTexte=&categorieLien=cid), 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](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000025503132&idArticle=LEGIARTI000030935038&dateTexte=&categorieLien=cid)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](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000025503132&idArticle=LEGIARTI000030935040&dateTexte=&categorieLien=cid) du même code.

* L’accès frauduleux
* Le maintien frauduleux
* Les intrusions avec dommages
* L’article 323-3-1
* La tentative
* STAD de l’Etat

**Jérôme Kerviel condamné pour introduction frauduleuse dans un système informatique**

L'ex-trader a été condamné à cinq ans d'emprisonnement, dont deux avec sursis, et à verser à la Société Générale de lourds dommages et intérêts d’un montant de 4,9 milliards d'euros.

(06/10/2010)

Dans son jugement rendu le 5 octobre 2010, le Tribunal de Grande Instance de Paris a condamné Jérôme Kerviel à cinq ans d'emprisonnement, dont deux avec sursis et à verser à la Société Générale, son ancien employeur, de lourds dommages et intérêts d'un montant de 4,9 milliards d'euros. Jérôme Kerviel s'est également vu interdire, à titre définitif, l'exercice direct ou indirect des activités  d'opérateur de marché et toute activité relative aux marchés financiers. Il a d'ores et déjà manifesté son intention d'interjeter appel de cette décision.  
         
L'ancien trader a été déclaré coupable d'abus de confiance vis-à-vis de son ancien employeur, de faux et usage de faux, et d'introduction frauduleuse de données dans un système informatique.  
         
L'infraction d'introduction frauduleuse de données dans un système de traitement automatisé est réprimée par l'article 323-3 du Code pénal et suppose que l'on introduise des données dans un système de traitement automatisé ou que l'on supprime ou modifie des données qu'il contient. Peu importe la nature des informations qui ont été "manipulées", ni même la finalité poursuivie dans la mesure où l a suppression, la modification ou l'introduction a été faite "frauduleusement".  
  
La notion de Système de Traitement Automatisé de Données (STAD) est définie (par les travaux parlementaires de la loi Godfrain) comme tout ensemble composé d'un ou plusieurs unités de traitement, de mémoires, de logiciels, d'organes entrées-sorties, et de liaisons qui concourent à un résultat déterminé.  
  
Cette définition couvre notamment les logiciels de messagerie électronique ; mémoires d'ordinateur ; serveurs ; liaisons télécom...  
        
L'élément matériel de l'infraction est constitué du simple accès ou maintien frauduleux dans un STAD, ce caractère frauduleux s'appréciant au regard de ce qu'autorise l'administrateur ou le détenteur du STAD.  
La jurisprudence considère que "l'accès à un STAD tombe sous le coup de la loi pénale dès lors qu'il est le fait d'une personne qui n'a pas le droit d'y accéder" (CA Toulouse, 21 janvier 1999).  
  
Par ailleurs, l'intention frauduleuse doit être démontrée car il s'agit d'un élément constitutif du délit pénal.  
         
Or, comme le rappelle le jugement du 5 octobre dernier, l'élément moral de cette infraction consiste principalement en la conscience et la volonté de l'auteur de porter atteinte à la fiabilité d'un système en y introduisant, en toute connaissance de cause, des données fausses.  
         
Ainsi, dans l'affaire Kerviel, les Magistrats se sont attachés à caractériser en quoi ce délit était "parfaitement" constitué à l'encontre de l'ex-trader. Tout en reconnaissant le caractère "innovant et complexe des techniques employées", les juges décrivent en effet de quelle manière Jérôme Kerviel a "sciemment saisi des opérations sans réalité économique, qu'il a par la suite pour partie annulées, dans le seul but de masquer ses engagements hors mandat et hors limites".  
         
Dans la mesure où la plupart des systèmes de traitement automatisé de données ne sont ni conçus, ni destinés à permettre de déceler une introduction frauduleuse, il est recommandé aux entreprises de se doter d'une charte d'utilisation des ressources informatiques, qui doit faire partie intégrante du contrat de travail, et dont le non-respect permettra de faciliter la preuve du caractère intentionnel de la manipulation des données.  
         
Soulignons de l'autre côté, le manque de contrôle de la banque sur les agissements de son ancien salarié, qui s'apparente tout de même une certaine négligence.  
Affaire à suivre...

Julie Jacob

Détaillez les spécificités de cette affaire au regard du droit pénal (les éléments de l’infraction pénale.

1. **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](https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=3998B1B7F520FD345244DBC9E5D743B8.tpdila09v_1?cidTexte=JORFTEXT000023707312&idArticle=LEGIARTI000023708771&dateTexte=20160831&categorieLien=id#LEGIARTI000023708771)

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 ?



La consécration du vol « 2.0 ».

2810 lectures

Par Jonathan Elkaim, Avocat.- vendredi 4 septembre 2015

Dans un arrêt en date du 20 mai 2015, la Chambre criminelle de la Cour de cassation a jugé que les dispositions de l’article 311-1 du Code pénal relative à la « soustraction frauduleuse d’autrui » s’appliquent en matière de transfert de fichiers informatiques.

Au cours du mois d’août 2012, un internaute dont le pseudonyme est « Bluetouff » a réussi à accéder librement, via les fonctionnalités du moteur de recherche Google, à la base de données de l’Agence nationale de sécurité sanitaire de l’alimentation, de l’environnement et du travail (ANSES).

Cet accès a été réalisé au moyen d’une requête spécifique aux termes de laquelle Bluetouff a interrogé le célèbre moteur de recherche grâce à plusieurs mots clés précis.

Toutefois, un tel accès n’a été possible que parce qu’une faille dans le système de sécurité du site internet de l’ANSES avait été détectée.

L’internaute Bluetouff en avait d’autant plus conscience qu’il a constaté que la connexion au système nécessitait une authentification et un mot de passe afin d’accéder aux fichiers convoités.

Par ce moyen, Bluetouff a téléchargé, et rendu accessible via son blog, plus de 7 Giga-octets de fichiers informatiques extraits de la base de données de l’ANSES.

C’est dans ce contexte que l’ANSES a déclenchée l’action publique en déposant plainte pour « intrusion dans un système informatique et vol de données informatiques ».

Au cours de l’instruction, Bluetouff a précisé aux enquêteurs que l’authentification et le mot de passe n’étaient pas immédiatement perceptibles par l’internaute puisque celui-ci n’a pu constater leur nécessité qu’après avoir parcouru l’arborescence des répertoires et accédé à la page d’accueil.

Un tel aveu a semble-t-il convaincu le tribunal correctionnel de Créteil lequel a jugé que Bluetouff pouvait « *légitimement penser* » que les données stockées étaient « *en libre accès et qu’il pouvait parfaitement se maintenir dans le système* ».

En outre, la juridiction de premier degré a jugé que l’article 311-1 du Code pénal ne pouvait recevoir application en l’espèce, dans la mesure où aucun support matériel contenant ces données n’avait été soustrait à l’ANSES.

La Cour d’appel de Paris dans un arrêt du 5 février 2014 (n°13/04833), tout en écartant le caractère frauduleux de l’accès aux données litigieuses, a jugé que le maintien de Bluetouff dans un système de traitement automatisé de données (STAD), nécessitant un « *contrôle d’accès et la nécessité d’une authentification par identifiant et mot de passe* », était frauduleux.

Ce faisant, la Cour d’appel fait grief à l’internaute de ne pas s’être immédiatement déconnecté après avoir constaté la présence de contrôles d’accès.

Mais surtout, la Cour d’appel infirme le jugement du tribunal correctionnel sur la qualification pénale attachée à la copie des fichiers informatiques litigieux.

En effet, les juges du fond ont considéré que le vol de fichiers était manifestement constitué à raison « *des copies de fichiers informatiques inaccessibles au public* » réalisées « *à des fins personnelles à l’insu et contre le gré de leur propriétaire* ».

La Cour de cassation, saisie d’un pourvoi, devait donc se prononcer sur le point de savoir si la copie de fichiers en l’absence d’autorisation et de dépossession de son propriétaire peut être qualifiée de vol au sens de l’article 311-1 du Code pénal.

La Haute juridiction répond clairement par l’affirmative.

En se maintenant « *dans un système de traitement automatisé après avoir découvert que celui-ci était protégé* » tout en soustrayant « *des données qu’il a utilisées sans le consentement de leur propriétaire* », Bluetouff a, pour la Cour de cassation, manifestement commis un vol.

Une telle qualification permet désormais de lever toute ambiguïté sur la nature mais également sur l’exigence de dépossession de la chose.

La Cour de cassation indique désormais qu’il importe peu que le propriétaire de données informatiques n’en soit pas dépossédé, dans la mesure où le vol sera caractérisé par la seule soustraction des données en l’absence de son consentement.

Une telle décision a priori « avant-gardiste » démontre la volonté d’adapter le droit aux nécessités de notre temps et de protéger le secret des informations, nouvelle ruée vers l’or contemporaine.

L’arrêt de la Cour de cassation fait ici écho à la volonté affichée du législateur de réprimer le vol d’information.

La récente modification de l’article 323-3 du Code pénal par la loi n°2014-1353 du 13 novembre 2014 (JORF n°0263 du 14 novembre 2014 page 19162 texte n°5) punissant toute introduction frauduleuse dans un STAD mais également toute détention, extraction, reproduction, transmission, suppression des données contenues par 5 ans d’emprisonnement et 75.000 € d’amende, suffit à s’en convaincre.

Une telle approche suscite néanmoins quelques interrogations, dans la mesure où le vol sanctionne une atteinte au droit fondamental de propriété qui se matérialise par la dépossession illégitime du propriétaire.

Même si la Cour de cassation prend soin de préciser qu’en matière immatérielle le délit est constitué par la soustraction de fichiers sans autorisation, il n’en est pas moins qu’une telle définition s’éloigne de celle classiquement retenue.

Dès lors, il est possible de s’interroger sur la pertinence d’une telle qualification dans la mesure où la reproduction illicite de données issues d’un STAD aurait pu être sanctionnée soit sur le fondement de la contrefaçon, en matière de droit d’auteur, soit sur celui du droit sui generis des bases de données.

En l’espèce, le délit de contrefaçon en matière de droit d’auteur n’aurait a priori pu trouver application dans la mesure où les données de l’ANSES constituent des documents publics.

Toutefois, le producteur d’une base de données est protégé contre tout usage ou extraction réalisés sans son consentement.

L’article L.342-1 du Code de la propriété intellectuelle dispose à ce titre que « *le producteur d’une base de données a le droit d’interdire : 1° L’extraction, par transfert permanent ou temporaire de la totalité ou d’une partie qualitativement ou quantitativement substantielle du contenu d’une base de données sur un autre support, par tout moyen et sous toute forme que ce soit(…)* ».

En l’espèce, l’extraction non autorisée de plus de 7 Giga-octets de données pourrait caractériser un délit d’extraction frauduleuse susceptible de poursuites pénales.

La Cour de cassation a sans doute souhaité marquer son passage à l’ère numérique. et pour cela pas de doutes, elle y est parvenue.

En savoir plus sur http://www.village-justice.com/articles/consecration-vol,20344.html#tvjuf0vkL3lZiRDC.99

Le vol de données informatiques

**Article juridique** publié le **11/12/2015 à 10:48**, vu **1411 fois**, [3 commentaire(s)](http://www.legavox.fr/blog/noe-marmonier/donnees-informatiques-20088.htm#ancre_com), Auteur : [Noé MARMONIER](http://www.legavox.fr/blog/noe-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 cloturer 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](https://www.doctrine.fr/d/CASS/2018/CE80A1EB3BE453A6E62C0)et repéré par [Lexradio](https://lexradio.fr/news/44783769-Caract%C3%A9risation-d-une-atteinte-%C3%A0-un-STAD-par-l-utilisation-d-un-i-keylogger-i#.WnF5u2Sh53E.twitter) 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](https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006418316&cidTexte=LEGITEXT000006070719) et [323-3-1](https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006418323&cidTexte=LEGITEXT000006070719)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.