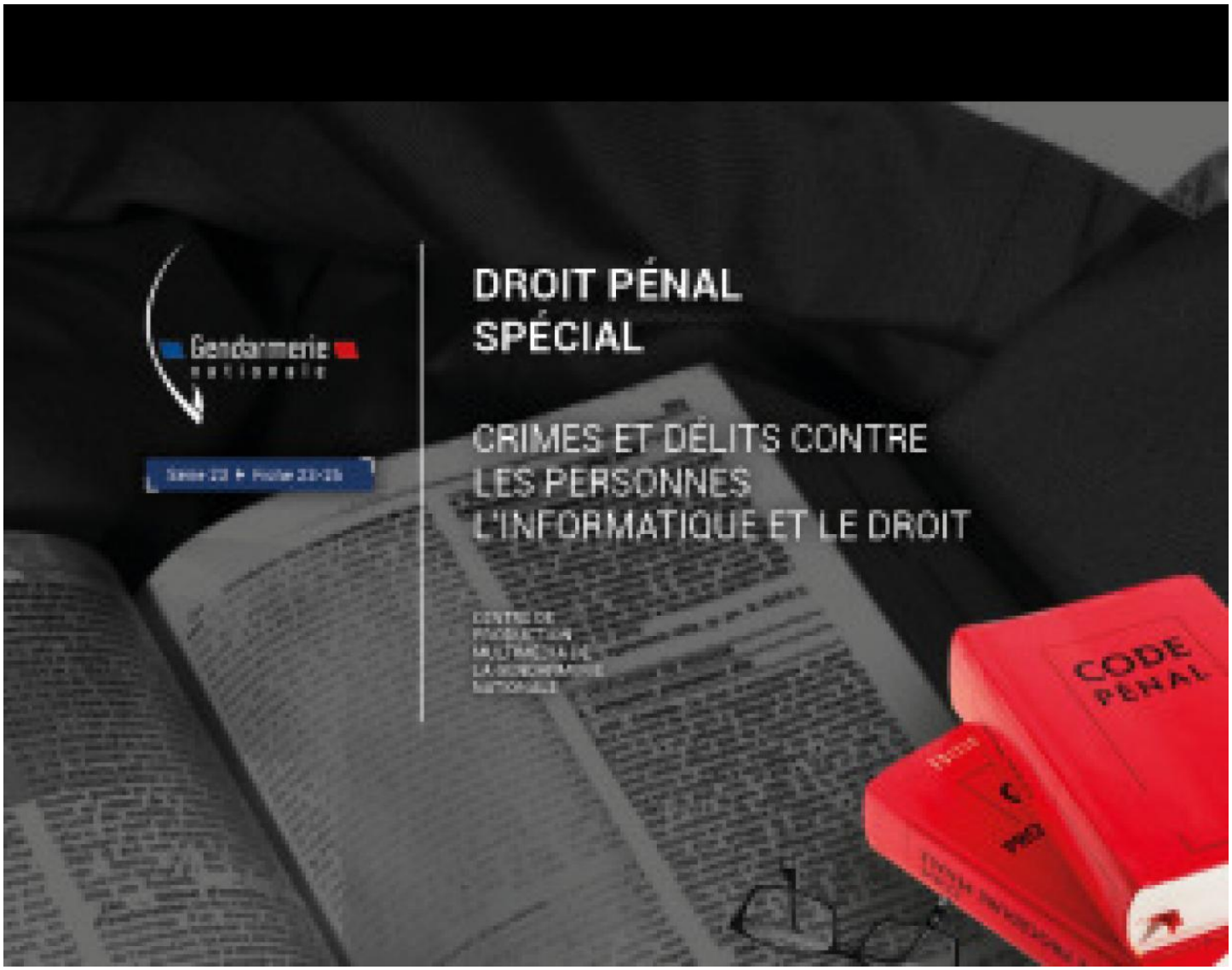
MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
*Liberté*
*Égalité*
*Fraternité*

# Gendarmerie nationale




# L'informatique et le droit

**1) Avant-propos** ..... 3
**2) Principes législatifs** ..... 3
2.1) Fondement juridique ..... 3
2.2) Respect des grandes valeurs ..... 3
2.3) Définitions ..... 3
**3) Protection de la personne humaine** ..... 4
3.1) Commission nationale de l'informatique et des libertés (CNIL) ..... 4
3.2) Composition ..... 4
3.3) Missions ..... 4
3.4) Possibilités d'actions de la CNIL ..... 5
3.5) Les sanctions prononcées par la CNIL ..... 5
3.6) Nature juridique du contentieux ..... 6
3.7) Droits individuels ..... 6

**4) Formalités préalables à la mise en oeuvre des traitements automatisés** ..... 7
4.1) Dispositions communes ..... 7
4.2) Autorisation et demande d'avis ..... 7
4.3) Mesures de sécurité ..... 8
**5) Modalités de fonctionnement des systèmes** ..... 8
5.1) Conditions de licéité des traitements de données à caractère personnel ..... 8
5.2) Nature des données ..... 8
5.3) Obligations incombant aux responsables de traitements ..... 9
**6) Les menaces informatiques** ..... 10
6.1) Les types de menaces ..... 11
6.2) La protection contre les menaces ..... 11
**7) La fraude informatique** ..... 12
7.1) Logiciels ..... 12
7.2) Domaine ..... 12
7.3) Caractéristiques ..... 12
7.4) Supports de données informatiques ..... 13
**8) Lutte contre la fraude** ..... 14
8.1) Dispositifs de lutte ..... 14
8.2) L'enquêteur face aux nouvelles technologies ..... 15
8.3) Les unités spécialisées en gendarmerie ..... 17
8.4) L'office anti-cybercriminalité ..... 17
**9) Infractions** ..... 19
9.1) Atteintes aux systèmes de traitement automatisé de données ..... 19
9.2) Administration d'une plateforme en ligne pour permettre la cession de produits illicites ..... 27
9.3) Intermédiation ou séquestre pour faciliter la cession de produits illicites ..... 30
9.4) Participation à un groupement formé ou à une entente établie en vue de la préparation d'une ou des infractions relatives à la fraude informatique ..... 31
9.5) Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques ..... 32
9.6) Infractions aux règles fixées lors de la déclaration des traitements ou fichiers ..... 37
9.7) Autres infractions ..... 43

# 1) Avant-propos

La mise en oeuvre de l'informatique a considérablement augmenté les moyens des divers pouvoirs, politique, administratif, économique et judiciaire. Son utilisation présente de nombreux avantages pour la sécurité des personnes et le développement des entreprises. En contrepartie, l'informatique comporte le risque d'atteinte à la vie privée par les contrôles, discriminations voire l'inexactitude des renseignements réunis.

La difficulté réside alors d'une part dans l'obligation d'une libre circulation de l'information et d'autre part dans la préservation des libertés individuelles dans le traitement des données nominatives.

Afin de pallier ce vide juridique, la loi n° 78-17 du 6 janvier 1978 a été créée. Celle-ci concerne les fichiers automatisés sans préjudice aux dispositions déjà existantes visant également les fichiers manuels.

Cette loi a été modifiée par la loi n° 2018-493 du 20 juin 2018.

# 2) Principes législatifs

## 2.1) Fondement juridique

Dès 1970, la France prévoit la création d'un fichier automatisé : le fichier des conducteurs, mais l'automatisation du casier judiciaire compromet ce projet.

En 1974, le projet SAFARI (système automatisé pour les fichiers administratifs et le répertoire des individus) provoque une prise de conscience des possibilités de l'informatique. Chaque individu y serait en effet recensé par un identifiant unique, *« le numéro national d'identité ».*

Une commission *« Informatique et libertés »* est créée. Elle rendra son rapport en 1975. Ce rapport servira de support à l'élaboration de la loi du 6 janvier 1978. Celle-ci est modifiée à plusieurs reprises pour prendre en compte les évolutions permanentes des procédés.

D'autres lois comme la *« loi HADOPI »* ou *« loi création et Internet **[loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet]** »* étoffent les mesures mises en place pour lutter contre les dérives qu'engendrent la démocratisation et l'amélioration du réseau Internet.

## 2.2) Respect des grandes valeurs

L'informatique doit être au service de chaque citoyen (Loi n° 78-17 du 6 janvier 1978, art. 1). Son développement doit s'opérer dans le cadre de la coopération internationale.

Les valeurs auxquelles l'informatique ne doit pas porter atteinte sont :

- les Droits de l'homme ;
- les libertés individuelles ou publiques ;
- la vie privée ;
- l'identité humaine.

## 2.3) Définitions

Constitue une donnée à caractère personnel, toute information relative à une personne physique identifiée ou qui peut être identifiée.

Constitue un traitement de données à caractère personnel, toute opération ou tout ensemble d'opérations portant sur de telles données quel que soit le procédé utilisé *(collecte, enregistrement, utilisation, diffusion, rapprochement, interconnexion, verrouillage, effacement...)* (Loi n° 78-17 du 6 janvier 1978, art. 2).

Constitue un fichier de données à caractère personnel, tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.

Le responsable d'un traitement de données est la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens (Loi n° 78-17 du 6 janvier 1978, art. 3 al. 1).

Le destinataire d'un traitement de données est toute personne habilitée à en recevoir communication autre que la personne concernée, le responsable du traitement, les personnes chargées de traiter les données et que les autorités légalement habilitées à en demander communication dans le cadre de leur mission (Loi n° 78-17 du 6 janvier 1978, art. 3 al. 2).

# 3) Protection de la personne humaine

## 3.1) Commission nationale de l'informatique et des libertés (CNIL)

Le contrôle de l'application des règles relatives aux traitements automatisés des données se fait en France d'une manière administrative contrairement à d'autres pays ayant mis en place un code de déontologie et un ordre chargé de la discipline professionnelle.

L'organe public de surveillance mis en place sous couvert de la loi du 6 janvier 1978 est la Commission nationale de l'informatique et des libertés (CNIL).

Son siège se situe au 8, rue Vivienne - 75083 Paris CEDEX 02, site Web : **www.cnil.fr.**

## 3.2) Composition

La CNIL est une autorité administrative indépendante composée de dix-huit membres nommés pour mandat de cinq ans renouvelable une fois (loi (Loi n° 78-17 du 6 janvier 1978 modifiée par la loi n° 2018-493 du 20 juin 2018, art. 9). Elle comprend :

deux députés désignés par l'Assemblée nationale ;

deux sénateurs désignés par le Sénat ;

deux membres du Conseil économique, social et environnemental, élus par cette assemblée ;

deux membres ou anciens membres du Conseil d'Etat, d'un grade au moins égal à celui de conseiller ;

deux membres ou anciens membres de la Cour de cassation, d'un grade au moins égal à celui de conseiller ;

deux membres ou anciens membres de la Cour des comptes, d'un grade au moins égal à celui de conseiller maître ;

trois personnalités qualifiées pour leur connaissance du numérique ou des questions touchant aux libertés individuelles, nommées par décret ;

deux personnalités qualifiées pour leur connaissance du numérique, désignées respectivement par le président de l'Assemblée nationale et par le président du Sénat.

le président de la Commission d'accès aux documents administratifs, ou son représentant.

La formation restreinte de la commission est composée d'un président et de cinq autres membres élus par la commission en son sein. Les membres du bureau ne sont pas éligibles à la formation restreinte.

## 3.3) Missions

La CNIL *(Loi n° 78-17 du 6 janvier 1978 modifiée par la loi n° 2018-493 du 20 juin 2018, art. 8)* :

- informe les personnes concernées et les responsables de traitements de leurs droits et obligations ;
- vérifie l'application de la présente loi ;
- délivre des autorisations, donne des avis, reçoit des déclarations ;
- établit et publie certaines normes concernant les traitements de données à caractère personnel dont la mise en oeuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés ;
- reçoit les réclamations, pétitions et plaintes ;
- répond aux demandes d'avis des pouvoirs publics ou des juridictions, conseille lors de la mise en oeuvre de traitements ;
- informe le procureur de la République des infractions dont elle a connaissance et peut présenter

ses observations dans les procédures pénales ;

- procède à des vérifications portant sur tous traitements et peut obtenir les supports d'informations utiles à ses missions ;
- homologue et publie des référentiels ou des méthodologies permettant de certifier de la conformité à la présente loi des processus d'anonymisation des données à caractère personnel ;
- répond aux demandes d'accès ;
- donne des avis sur la conformité à la présente loi, porte une appréciation sur les garanties d'un traitement, délivre un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel ;
- se tient informée de l'évolution des technologies et rend publique son appréciation ;
- est consultée sur tout projet de loi ou de décret relatif à la protection des personnes ;
- propose au Gouvernement des mesures législatives ou réglementaires ;
- peut apporter son concours en matière de protection des données ;
- peut être associée à la représentation française internationale et à des négociations internationales relatives à la protection des données à la demande du Premier ministre ;
- conduit une réflexion sur les problèmes éthiques et les questions de société soulevés par l'évolution des technologies numériques ;
- promeut l'utilisation des technologies protectrices de la vie privée.

En formation restreinte, elle prononce les sanctions à l'encontre des responsables de traitements qui ne respectent pas les obligations découlant de la présente loi *(Loi n° 78-17 du 6 janvier 1978, art. 16.*

Pour l'accomplissement de ses missions, la commission peut procéder par voie de recommandation et prendre des décisions individuelles ou réglementaires.

Elle peut saisir pour avis l'Autorité de régulation des communications électroniques et des postes de toute question relevant de la compétence de celle-ci et présente chaque année au Président de la République et au Premier ministre un rapport public rendant compte de l'exécution de sa mission.

L'article L32 du codes des postes et des communications électroniques dresse les définitions de l'ensemble des termes liés aux communications électroniques et mobiles.

### 3.4) Possibilités d'actions de la CNIL

Pour l'exécution de contrôles des traitements de données, les membres et agents de la CNIL ont accès, de 6 heures à 21 heures, aux lieux, locaux, enceintes, installations ou établissements servant à la mise en oeuvre de ces traitements et qui sont à usage professionnel *(Loi n° 78-17 du 6 janvier 1978, art. 19)*.

Le procureur de la République territorialement compétent doit être préalablement informé. En cas d'opposition du responsable des lieux, la visite ne peut se dérouler qu'avec l'autorisation du juge des libertés et de la détention.

Les membres et agents peuvent demander communication des documents nécessaires, quel qu'en soit le support et en prendre copie. Ils peuvent accéder aux programmes informatiques, aux données, et en demander la transcription.

Des experts peuvent les assister si nécessaire. Un procès-verbal des vérifications et visites, signé contradictoirement, est dressé.

### 3.5) Les sanctions prononcées par la CNIL

La CNIL peut prononcer un avertissement ou une mise en demeure. Si la personne ne respecte pas la mise en demeure, la commission peut prononcer, après une procédure contradictoire :

- un avertissement ;

- une sanction pécuniaire ;
- une injonction de cesser le traitement de données ;
- un retrait de l'autorisation accordée *(Loi n° 78-17 du 6 janvier 1978, art. 20)*.

En cas d'urgence et après une procédure, elle peut décider :

- de l'interruption du traitement de données ;
- du verrouillage de certaines données pour une durée maximale de trois mois.

La commission peut en outre, informer le Premier ministre afin qu'il prenne des mesures immédiates ou, en cas d'atteinte grave aux droits et libertés, demander par la voie du référé l'intervention de la juridiction compétente.

Les sanctions sont prononcées sur la base d'un rapport, et notifiées au responsable du traitement, qui peut déposer des observations et se faire représenter ou assister *(*Loi n° 78-17 du 6 janvier 1978, art. 22).« « » »

La Commission est habilitée à communiquer des informations aux autorités exerçant des compétences analogues aux siennes dans d'autres États membres de la Communauté européenne, et ce à leur demande *(Loi n° 78-17 du 6 janvier 1978, art. 25)*.

## 3.6) Nature juridique du contentieux

C'est une autorité administrative indépendante n'ayant pas le statut de juridiction. La CNIL n'est ni soumise au pouvoir hiérarchique, ni au pouvoir de tutelle du Gouvernement. L'indépendance de la CNIL est garantie par le fait que ses membres ne reçoivent, dans l'exercice de leurs attributions, d'instruction d'aucune autorité. En outre, les ministres, autorités publiques, dirigeants d'entreprises publiques ou privées, comme les détenteurs ou utilisateurs de traitements ou de fichiers de données à caractère personnel, ne peuvent s'opposer à l'action de la commission *(Loi n° 78-17 du 6 janvier 1978, art. 8.*

Soumise au seul contrôle juridictionnel du Conseil d'État, elle est néanmoins tenue de publier annuellement un rapport présenté au président de la République et au Premier ministre, rendant compte de l'exécution de sa mission.

Les décisions de la Commission étant de nature administrative, elles peuvent donc faire l'objet de recours en annulation pour excès de pouvoir et engager la responsabilité de l'État. La juridiction compétente est le Conseil d'État.

Les décisions internes (nominations d'agents de la Commission) relèvent des tribunaux administratifs.

L'avis motivé de la Commission ne peut être assimilé à une décision et ne relève donc pas du juge, pas plus que les décisions préparatoires *(Arrêt en CE du 13 février 1991)*.

## 3.7) Droits individuels

### 3.7.1) Droit d'opposition

Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement *(Loi n° 78-17 du 6 janvier 1978, art. 38)*. Elle peut également s'opposer à leur utilisation à des fins de prospection notamment commerciale.

### 3.7.2) Droit d'accès

Toute personne physique justifiant de son identité a le droit d'interroger le responsable du traitement de données pour obtenir des informations, ainsi que la communication ou une copie de données *(Loi n° 78-17 du 6 janvier 1978, art. 38).* Le juge compétent peut, en cas de risque, ordonner des mesures de nature à éviter toute dissimulation ou disparition. Le responsable du traitement peut s'opposer aux demandes manifestement abusives.

Ce droit d'accès ne s'applique pas lorsque les données sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée et pendant une durée n'excédant pas celle nécessaire aux seules finalités d'établissement de statistiques ou de recherches historiques ou scientifiques.

Lorsqu'un traitement intéresse la sûreté de l'État, la défense ou la sécurité publique, la demande de droit d'accès est adressée à la CNIL qui effectue les investigations *(Loi n° 78-17 du 6 janvier 1978, art. 31)*. Ce droit d'accès indirect s'applique aux traitements des administrations publiques et des personnes privées chargées d'une mission de service public qui doivent prévenir, rechercher ou constater les infractions, contrôler ou recouvrer des impositions.

#### 3.7.3) Droit de rectification

Toute personne physique justifiant de son identité peut exiger que les données la concernant soient rectifiées, complétées, mises à jour, verrouillées ou effacées si elles s'avèrent inexactes, incomplètes, équivoques, périmées ou si leur collecte, utilisation, communication ou conservation est interdite *(Loi n° 78-17 du 6 janvier 1978, art. 50)*. En cas de contestation, la charge de la preuve incombe au responsable auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les données contestées ont été communiquées par l'intéressé ou avec son accord.

Les héritiers d'une personne décédée peuvent également demander la mise à jour de données relatives à la personne disparue.

**De la protection des lanceurs d'alerte**

La loi 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, un délit, une menace ou un préjudice pour l'intérêt général, une violation ou une tentative de dissimulation d'une violation d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, du droit de l'Union européenne, de la loi ou du règlement. Lorsque les informations n'ont pas été obtenues dans le cadre des activités professionnelles mentionnées au I de l'article 8 [de la loi n° 2016-1691 du 9 décembre 2016], le lanceur d'alerte doit en avoir eu personnellement connaissance. (I, art. 6, loi n° 2016-1691 du 9 décembre 2016) "

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 (art. 6 à 16) prévoit un dispositif protégeant les lanceurs d'alerte. Sont également protégées, dans le cadre de l'article 6-1 de cette même loi, les facilitateurs ayant aidé un lanceur d'alerte à effectuer un signalement ou une divulgation.

## 4) Formalités préalables à la mise en oeuvre des traitements automatisés

### 4.1) Dispositions communes

La plupart des traitements automatisés de données à caractère personnel font l'objet d'une déclaration auprès de la CNIL *(Loi n° 78-17 du 6 janvier 1978, art. 32 )*. La déclaration comporte l'engagement que le traitement satisfait aux exigences de la loi.

Pour les catégories de traitement dont la mise en oeuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés, la CNIL établit et publie des normes destinées à simplifier l'obligation de déclaration *(Loi n° 78-17 du 6 janvier 1978, art. 35)* . La Commission peut d'ailleurs décider de dispenser certains de ces traitements de déclaration.

### 4.2) Autorisation et demande d'avis

Certains traitements doivent, pour être mis en oeuvre, avoir obtenu l'autorisation de la CNIL, ou être autorisés par arrêté du ou des ministres compétents, après avis motivé et publié de la Commission, ou encore être autorisés par décret en Conseil d'État après avis motivé et publié de la CNIL.

Le ministre de l'Intérieur est autorisé à mettre en oeuvre des traitements de données à caractère personnel, pour « *la prévention des atteintes à la sécurité publique* » et « *les enquêtes administratives liées à la sécurité publique* », ayant pour finalité de recueillir, de conserver et d'analyser les informations qui concernent des personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique (Décret n° 2009-1249 du 16 octobre 2009).

La commission se prononce sur les demandes d'autorisation ou d'avis dans un délai de deux mois à compter de la réception des demandes, délai qui peut être renouvelé une fois sur décision de son président *(Loi n° 78-17 du 6 janvier 1978, art. 34)*. Si elle ne s'est pas formulée dans le délai, la réponse est présumée négative pour les demandes d'autorisation et favorable pour les demandes d'avis.

### 4.3) Mesures de sécurité

La CNIL met à la disposition du public la liste des traitements ayant fait l'objet d'une formalité préalable à leur mise en oeuvre, en précisant leur dénomination et finalité, les coordonnées du responsable, les catégories de données. Elle tient également à la disposition du public ses avis, décisions ou recommandations.

## 5) Modalités de fonctionnement des systèmes

### 5.1) Conditions de licéité des traitements de données à caractère personnel

Les données doivent être (Loi n° 78-17 du 6 janvier 1978, art. 4) :

- collectées et traitées de manière loyale et licite ;
- collectées pour des finalités déterminées, explicites et légitimes ;
- adéquates, pertinentes et non excessives au regard des finalités et de leurs traitements ultérieurs ;
- exactes, complètes et, si nécessaire, mises à jour ;
- conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

Un traitement de données doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes (Loi n° 78-17 du 6 janvier 1978, art. 5) :

- le respect d'une obligation légale incombant au responsable du traitement ;
- la sauvegarde de la vie de la personne concernée ;
- l'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;
- l'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures pré-contractuelles prises à sa demande ;
- la réalisation de l'intérêt légitime du responsable ou du destinataire du traitement, sous réserve de ne pas léser l'intérêt, les droits ou les libertés de la personne.

### 5.2) Nature des données

#### 5.2.1) Principe

La collecte ou le traitement de données à caractère personnel qui fait apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale, relatives à la santé ou à la vie sexuelle de la personne est interdit.

#### 5.2.2) Exceptions

Certaines données ne sont pas soumises à cette interdiction *(Loi n° 78-17 du 6 janvier 1978, art. 30)* :

- lorsque la personne a donné son consentement exprès, sauf si la loi prévoit que l'interdiction ne peut être levée par ce consentement ;
- les traitements nécessaires à la sauvegarde de la vie humaine ;

- les traitements mis en oeuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical ;
- les données rendues publiques par la personne concernée ;
- les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ;
- les traitements mis en oeuvre par un professionnel de la santé ou par une personne tenue au secret professionnel aux fins de médecine préventive, diagnostics médicaux, administration de soins ou de la gestion de services de santé ;
- les traitements statistiques réalisés par l'Institut national de la statistique et des études économiques ou l'un des services statistiques ministériels ;
- les traitements nécessaires à la recherche dans le domaine de la santé ;
- si les données sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation reconnu conforme par la CNIL et avec son autorisation ;
- certains traitements, automatisés ou non, justifiés par l'intérêt public.

#### 5.2.3) Les données relatives aux infractions, condamnations et mesures de sûreté

Par ailleurs, les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en oeuvre que par :

- les juridictions, autorités publiques et personnes morales gérant un service public ;
- les auxiliaires de justice pour les besoins de leurs missions ;
- les personnes morales agissant au titre des droits des auteurs, artistes, interprètes et producteurs.

## 5.3) Obligations incombant aux responsables de traitements

#### 5.3.1) Obligations de sécurité

Le responsable du traitement est tenu de prendre toutes les précautions utiles au regard de la nature des données, et notamment, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès *(Loi n° 78-17 du 6 janvier 1978, art. 37)*.

Toute violation de données à caractère personnel dans le cadre de la fourniture au public de services de communications électroniques fait l'objet d'une notification par le fournisseur de service d'une part, à la CNIL et d'autre part, sous certaines conditions, à l'intéressé.

Les données ne peuvent être traitées par sous-traitance que sur instructions du responsable du traitement. Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en oeuvre des mesures de sécurité et de confidentialité *(Loi n° 78-17 du 6 janvier 1978, art. 57)*..

Par ailleurs, le responsable ne peut transférer des données à caractère personnel vers un État n'appartenant pas à la Communauté européenne que si le niveau de protection de la vie privée et des libertés et droits des personnes est suffisant *(Loi n° 78-17 du 6 janvier 1978, art. 112)*.

Cependant un transfert de données vers un État ne remplissant pas ces conditions peut être opéré avec le consentement exprès de la personne concernée par décision de la CNIL ou si le transfert est nécessaire :

- à la sauvegarde de la vie de cette personne ;
- à la sauvegarde de l'intérêt public ;
- à la constatation, l'exercice ou la défense d'un droit en justice *(Loi n° 78-17 du 6 janvier 1978, art. 113)* ;
- à la constatation d'un registre destiné à l'information du public ;
- à l'exécution d'un contrat entre le responsable du traitement et d'un tiers, dans l'intérêt de la personne concernée.

#### 5.3.2) Obligation d'information

Le responsable du traitement doit informer la personne concernée (Loi n° 78-17 du 6 janvier 1978, art. 104) :

- de l'identité du responsable ou de son représentant ;
- de la finalité poursuivie par le traitement ;
- du caractère obligatoire ou facultatif des réponses ;
- des conséquences d'un défaut de réponse ;
- des destinataires de données ;
- de ses droits à l'égard des traitements de données ;
- des transferts de données envisagés à destination d'un État non-membre de la communauté européenne.

La personne utilisant des réseaux de communication électroniques doit être informée de manière claire et complète, de la finalité de toute action tendant à accéder à des informations stockées dans son équipement terminal, ou à y inscrire des informations et des moyens dont elle dispose pour s'y opposer.

Ces dispositions ne s'appliquent pas si l'action est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande de l'utilisateur, ou a pour finalité de permettre la communication par voie électronique.

Cette obligation d'information ne s'applique pas aux données mises en oeuvre pour le compte de l'État et intéressant la sûreté de l'État, la défense, la sécurité publique ou ayant pour objet l'exécution de condamnations pénales, de mesures de sûreté, la prévention, la recherche, la constatation ou la poursuite d'infractions pénales.

#### 5.3.3) Cas particuliers de traitements de données à caractère personnel

##### 5.3.3.1) Traitements aux fins de journalisme et d'expression littéraire et artistique

La limitation de la durée de conservation, l'interdiction de collecter certaines données, des traitements sur les infractions, l'obligation de déclaration, l'autorisation par la CNIL, l'information préalable, les droits d'accès et de rectification, les règles de transfert de données ne s'appliquent pas lorsque la finalité du traitement est *(Loi n° 78-17 du 6 janvier 1978, art. 80)* :

- l'expression littéraire et artistique ;
- l'exercice à titre professionnel de l'activité de journaliste.

Cependant, ces dispositions n'empêchent nullement l'application du Code civil, des lois relatives à la presse et du Code pénal qui prévoient les conditions d'exercice du droit de réponse et qui préviennent, limitent ou répriment les atteintes à la vie privée et à la réputation.

##### 5.3.3.2) Traitements aux fins de recherches dans le domaine de la santé

Les traitements automatisés de données à caractère personnel dont la finalité est ou devient la recherche ou les études dans le domaine de la santé ainsi que l'évaluation ou l'analyse des pratiques ou des activités de soins ou de prévention sont soumis à une réglementation particulière.

L'autorisation de la CNIL doit ensuite être accordée.

Les membres des professions de santé peuvent transmettre des données à caractère personnel dans le cadre d'un traitement autorisé *(Loi n° 78-17 du 6 janvier 1978, art. 72)*. Lorsqu'elles permettent l'identification des personnes, elles doivent être codées avant leur transmission, sauf si les finalités sont des études de pharmacovigilance ou des protocoles de recherche réalisés lors d'études coopératives nationales ou internationales, ou encore si une particularité de la recherche l'exige.

Toute personne a le droit de s'opposer à ce que les données à caractère personnel la concernant fassent l'objet de la levée du secret professionnel *(Loi n° 78-17 du 6 janvier 1978, art. 74)*.

L'information des personnes concernées doit être réalisée avant le début du traitement ; elle est fournie aux titulaires de l'autorité parentale pour les mineurs ou représentant légal pour les personnes faisant l'objet d'une mesure de tutelle.

De plus, une information doit être assurée dans tout établissement ou centre où s'exercent des activités de prévention, de diagnostic et de soins effectuant des transmissions de données à caractère personnel.

# 6) Les menaces informatiques

## 6.1) Les types de menaces

La menace la plus dangereuse aujourd'hui et depuis les débuts de l'informatique est la captation de données pouvant être utilisées frauduleusement.

Autrefois, cette fraude nécessitait la présence physique de l'auteur près de la machine sur laquelle étaient stockées les données. Mais depuis la généralisation des connexions aux réseaux et notamment Internet, celle-ci peut se faire à distance.

Il existe plusieurs types de menaces dont les conséquences sont plus ou moins dangereuses pour l'utilisateur. Les plus courants sont :

- le virus informatique est un type de logiciel malveillant caché dans un logiciel légitime. Chaque fois qu'un utilisateur ouvre le logiciel infecté, il permet au virus de se propager. Il agit discrètement et se réplique à une vitesse fulgurante grâce aux échanges de données, que ce soit par une clé USB ou un réseau informatique ;
- le virus ne doit pas être confondu avec un ver informatique, qui se répand sur le réseau Internet. Ce dernier peut s'installer sur un ordinateur à partir d'un courriel, par téléchargement d'un fichier ou par messagerie instantanée. Il est beaucoup plus courant que le virus informatique de nos jours ;
- le logiciel espion ou «*cheval de troie*». Depuis quelques années, Les virus classiques ont cédé le pas à ces logiciels espions. Ceux-ci infectent silencieusement l'ordinateur grâce à une application en apparence légitime. Une fois dans l'ordinateur, le logiciel peut faire ce qu'il veut : enregistrer les mots de passe ou accéder à la caméra pour enregistrer les moindres faits et gestes de l'utilisateur ;
- les spams ou pourriels. Il s'agit de communications électroniques non désirées ayant pour conséquence l'augmentation des ressources des réseaux et créant une pollution virtuelle engendrant une perte de temps et d'argent. En tant que tels, les pourriels ne font pas partie des menaces informatiques, mais si on les ouvre ou si l'on clique sur leur lien, ils peuvent implanter un ver informatique sur l'ordinateur ;
- l'attaque par déni de service est causée en inondant un serveur ou un site web de requêtes dans le but de le rendre indisponible. L'attaque par déni de service peut être perpétrée par un petit nombre de ressources. Un pirate peut utiliser son seul ordinateur pour contrôler des zombies, c'est-à-dire d'autres ordinateurs infectés qui obéiront à ses commandes. Ces ordinateurs peuvent avoir précédemment été infectés par des virus ou des vers ;
- le phishing ou « *hameçonnage* » est une des menaces informatiques les plus facile à identifier. Il s'agit d'un courriel qui ressemble à s'y méprendre à celui d'un service connu, comme une institution bancaire. Le fraudeur tente d'obtenir des informations personnelles en incitant l'utilisateur à cliquer sur un lien, par exemple pour vérifier l'identification d'un compte de carte de crédit.

## 6.2) La protection contre les menaces

Afin de lutter contre ces « *attaques virtuelles* » pouvant avoir des conséquences plus ou moins graves, l'utilisateur d'un ordinateur doit équiper son système de logiciels (antivirus, pare-feu,...) et faire preuve d'une grande vigilance.

Il s'agit d'une lutte permanente où les utilisateurs et concepteurs de logiciels sont mis à l'épreuve face à des pirates de plus et plus inventifs et réactifs.

La mise à jour des logiciels antivirus est impérative afin qu'ils gardent une efficacité optimale.

# 7) La fraude informatique

## 7.1) Logiciels

Un logiciel ne peut être protégé que s'il répond à une condition d'originalité (résultat d'un effort personnalisé matérialisé dans une structure et portant la marque du travail de l'auteur). De plus et sous peine d'inopposabilité, il doit faire l'objet d'un contrat de nantissement du droit d'exploitation du logiciel et être inscrit sur un registre spécial à l'Institut national de la propriété industrielle (INPI). Enfin, la durée de protection du droit d'auteur est fixée à cinquante ans à compter du décès du créateur.

D'autre part, l'utilisateur d'un logiciel n'est pas propriétaire, mais il dispose de droits d'usage sous couvert de la licence accordée.

## 7.2) Domaine

La délinquance connaît une migration de plus en plus importante vers le domaine de l'informatique. C'est une sorte de recyclage qui va vers « ce qui rapporte » le plus dans des conditions plus aisées.

Même si dans la petite délinquance le copieur de CD ou DVD existe toujours, les copies illicites réalisées dans les entreprises sont plus inquiétantes. Elles font l'objet de la part d'une organisation internationale d'éditeurs de logiciels, d'une lutte contre la contrefaçon de logiciels.

Les différentes fraudes informatiques qui sont des délits de contrefaçon peuvent s'énumérer ainsi :

- la copie de logiciels ;
- la copie de logiciels sur disque dur d'ordinateurs offerts à la vente ;
- le non-respect de règles de commercialisation (logiciels vendus séparément alors qu'ils sont fournis avec une machine) ;
- la vente de produits « Éducation », en lieu et place de produits complets ;
- la vente de logiciels de mise à jour, en lieu et place de produits complets ;
- la contrefaçon de logiciels à des fins commerciales ;
- la contrefaçon « à l'identique » d'ensembles complets.

## 7.3) Caractéristiques

**Auteurs**

Si l'âge moyen des pirates a tendance à diminuer, les adolescents se limitent souvent à quelques copies par défi, goût de la collection et manque de moyens financiers.

Le pirate informatique se situe dans la tranche d'âge « 18-35 ans » et, bien souvent, exerce une activité dans la société. Il appartient dans plus de 80 % des cas à l'entreprise à laquelle il s'attaque.

**Absence d'éléments de preuve**

Dans la plupart des cas, les manipulations opérées laissent une trace dans le système (logfile) et font l'objet de traitements particuliers dans le cadre de la sécurité décidée par le responsable informatique. Ces éléments sont indispensables à l'enquêteur, mais peuvent avoir fait l'objet d'un effacement de la part du pirate.

**Vitesse d'exécution**

Les malversations peuvent très rapidement prendre une importance économique considérable, sans oublier que le temps de connexion est souvent très court pour les initiés connaissant parfaitement les méandres du système visité.

**Extension mondiale des liaisons de télécommunications**
Chaque site est bien souvent accessible par le réseau internet. Son utilisation permet un point d'entrée. La connaissance des mots de passe « utilisateur » est encore la solution la plus courante pour pénétrer un système. Certains pirates tentent de propager un backdoor (fonctionnalité implantée à l'insu de l'utilisateur) qui donne un accès secret à un logiciel. Ce dernier devient « un cheval de troie » grâce auquel l'auteur peu explorer voire prendre le contrôle d'un ordinateur.

**Absence de véritable contrôle et sécurisation**
L'observation des règles de connexion et de sortie des systèmes est souvent médiocre. Les mots de passe sont disponibles sur le bureau de l'opérateur, mais phénomène encore plus courant, la sécurisation des systèmes est conçue d'une manière légère dans une majorité des cas, ou est absente. En effet, nombre de machines sont dépourvues d'antivirus ou ne sont pas mises à jour.

## 7.4) Supports de données informatiques

**Les ordinateurs**
Les ordinateurs sont utilisés à titre public ou privé. Les systèmes d'exploitation sont très divers et parfois propres à certaines professions. Ces appareils peuvent être reliés par un réseau accédant ou non à un serveur de données, pouvant être lui-même intégré dans un autre réseau de serveurs.

**Le réseau Internet**
Ce système est né aux États-Unis au tout début des années soixante-dix à l'initiative de quelques universitaires qui ont voulu faire communiquer entre eux des réseaux hétérogènes.

L'armée américaine a financé pour partie les recherches du laboratoire ARPA, ce qui a abouti à l'ARPANET. Un nouveau langage entre systèmes (protocole) nommé TCP-IP pour Transfert Control Protocol-Internet Protocol a alors été élaboré. Parmi les grands principes du réseau INTERNET figure celui, essentiel, de la décentralisation. Aucun serveur n'est un site central et le RÉSEAU ne risque pas le blocage en cas de défaillance d'un site. C'est sans doute ce qui a motivé la mise en place d'un tel réseau, dans la crainte d'une perte sérieuse des possibilités de communications. L'autre élément primordial sur le réseau INTERNET est la transmission des données par paquets identifiés qui sont adressés, sans chemin prédéfini, l'essentiel étant pour le système de convoyer les différents paquets de l'émetteur au destinataire désigné.

**les services sur le réseau**
Le trafic peut se décomposer en divers protocoles de communication dont les principaux sont :

**SMTP** : envoi de courriel ;

**POP3** : lecture de courriel rapatrié sur l'ordinateur ;

**IMAP** : lecture de courriel sur un serveur ;

**HTTP** : navigation internet ;

**FTP** : transfert de fichiers entre deux machines ;

**NNTP** : accès aux news group.

**La connexion**
Peu d'éléments sont indispensables afin de se connecter au réseau internet. En effet, il suffit de disposer d'un ordinateur relié avec ou sans fil (Wi-fi) à un modem (modulateur-démodulateur) lui-même relié à une ligne téléphonique ou à une connexion par câble, et enfin de souscrire un abonnement auprès d'un prestataire de services (fournisseur d'accès internet [FAI]). Il peut aussi s'agir de téléphone portable qui offre la possibilité d'accéder à Internet via le réseau de téléphonie mobile. Ce dernier peut aussi servir de modem pour un ordinateur.

À l'aide d'un navigateur internet (logiciel installé sur l'appareil) il est ensuite possible d'accéder au Web (World Wide Web) aussi appelé communément « la toile ».

**Les intranets**
Un réseau local est constitué par la connexion de plusieurs ordinateurs reliés entre eux ou selon une architecture client-serveur. Les ordinateurs alors dotés d'une carte de communication (carte réseau), sont reliés par câble ou par Wi-Fi et travaillent dans leur grande majorité selon le protocole TCP-IP.

Un réseau peut être dit « Intranet » lorsque sa structure matérielle est celle d'un réseau classique, et ses couches logicielles, celles de l'Internet, à la seule différence que le réseau internet s'inscrit dans un circuit fermé. L'Intranet est donc un puissant moyen de communication à l'intérieur d'un organisme.

L'Intranet peut être connecté au réseau mondial Internet via une ou plusieurs passerelles. C'est le cas de l'Intranet gendarmerie.

# 8) Lutte contre la fraude

## 8.1) Dispositifs de lutte

Les fraudes informatiques sont des infractions difficilement décelables par des personnels non initiés.

La gendarmerie a en général connaissance des fraudes sur plainte de la victime, dénonciation d'un témoin ou sur renseignement.

Les efforts de la gendarmerie pour répondre au développement de la délinquance informatique ont été constants : introduction d'une dimension informatique dans les attributions des enquêteurs en délinquance économique et financière (DEFI), création d'un département informatique électronique (INL) à l'IRCGN, puis d'une cellule de surveillance de l'Internet au sein du SCRC. Ces deux dernières entités ont depuis été refondues au sein du commandement de la gendarmerie dans le cyberespace (le ComCyberGend), créé en 2021. C'est désormais le ComCyberGend qui assure, pour la gendarmerie nationale, l'uniformité de l'action de la gendarmerie en matière de délinquance dans le cyberespace.

En 2001, le CNFPJ a initié une formation d'enquêteurs aux nouvelles technologies (N'TECH) avec des matériels adaptés.

Il ne s'agit plus aujourd'hui de répondre à une délinquance très particulière, mais bien d'assurer à l'ensemble des enquêtes judiciaires qui touchent de près ou de loin à Internet, aux réseaux de télécommunications ou à l'utilisation de l'outil informatique, une même qualité de traitement sur l'ensemble du territoire où la gendarmerie exerce sa compétence.

Il est à noter que les membres de la Commission de protection des droits, ainsi que ses agents habilités et assermentés devant l'autorité judiciaire à l'article L. 331-21 du Code de la propriété intellectuelle, peuvent constater les faits susceptibles de constituer des infractions concernant la diffusion et la protection pénale de la propriété littéraire et artistique sur internet *(Loi n° 2009-1311 du 28 octobre 2009)*. Ces infractions peuvent être punies de la peine complémentaire de suspension de l'accès à un service de communication au public en ligne mentionnée aux articles L. 335-7 et L. 335-7-1 du Code précité.

**Saisies pénales d'actifs numériques**

Afin de renforcer la réactivité des opérations de saisies portant sur des crypto-actifs, par dérogation aux dispositions de l'article 706-153 du CPP, l'article 706-154 du code de procédure pénale permet, depuis l'entrée en vigueur de la loi n°2023-22 du 24 janvier 2023 dite " LOPMI", à l'officier de police judiciaire de procéder, avec l'autorisation obtenue par tout moyen du procureur de la République ou du juge d'instruction, à la saisie d'actifs numériques mentionnés à l'article L54-10-1 du code monétaire et financier, qu'il s'agisse donc de jetons ou de crypto-actifs.

Sur saisine du procureur de la République ou du juge d'instruction, le juge des libertés et de la détention doit se prononcer par ordonnance motivée sur le maintien ou la levée de la saisie des actifs numériques dans un délai de dix jours à compter de sa réalisation - une faculté d'appel (non suspensif) devant la chambre de l'instruction étant reconnue au ministère public, au propriétaire de l'actif numérique et, s'ils sont connus, aux tiers ayant des droits sur cet actif.

Aux termes des dispositions de l'article L54-10-1 du code monétaire et financier, les actifs numériques regroupent les jetons et crypto-actifs qui correspondent à des actifs numériques représentant un ou plusieurs droits sous la forme numérique. Les actifs numériques présentent la caractéristique d'être plus rapidement transférables que les fonds détenus sur un compte bancaire. Les facilités de dissimulation et de dissipation qu'ils offrent à leurs bénéficiaires sont à l'origine d'une utilisation accrue dans le cadre de la délinquance lucrative.

Le recours aux actifs numériques est constaté au service de la commission de plusieurs type d'infractions. Il peut s'agir d'infractions dont le mode opératoire est totalement nouveau (en matière de cryptojacking par exemple), d'infractions traditionnelles ayant recours aux actifs numériques (comme à l'occasion d'une attaque par rançongiciel) ou encore d'infractions de blanchiment ou de financement du terrorisme [Cf. circulaire DACG n° CRIM-2023-02/H2-03.02.2023 du 3 février 2023].

## 8.2) L'enquêteur face aux nouvelles technologies

**Avant l'intervention**

Comme dans toute affaire judiciaire, l'enquête sur l'environnement est impérative. Il est primordial de connaître le milieu dans lequel va se situer l'intervention. Selon qu'il s'agisse d'un particulier, d'une entreprise ou d'un centre informatique, la manière d'opérer et les moyens à mettre en oeuvre sont différents.

Il est nécessaire de disposer d'un inventaire du parc à explorer avec, si possible, son architecture de réseau et les moyens de communication vers l'extérieur.

Plus techniquement, il faut même connaître les systèmes utilisés. La qualification des personnels est nécessaire.

L'enquêteur doit s'entourer d'un personnel qualifié, même si l'affaire semble a priori simple.

En présence d'un site connecté, il est important d'isoler le site en faisant débrancher les modems.

De plus, l'interpellation du délinquant doit s'effectuer à l'extérieur du domicile ou dans un lieu permettant d'éviter la destruction des données.

**Pendant l'intervention**

L'accès au système informatique doit être interdit à tous les utilisateurs.

**Constatations**

Une planche photographique doit être réalisée (environnement dans lequel se trouve l'ordinateur et surtout pour la connectique de chaque machine).

Si l'ordinateur est allumé, il ne faut exécuter aucun programme, n'ouvrir aucun fichier. La moindre icône peut être le déclencheur d'un système d'effacement de données. Il faut :

- faire une photographie du bureau visible à l'écran ;
- noter et comparer l'heure et la date affichée sur le bureau ;
- noter le libellé des fenêtres réduites dans la barre des tâches (passer le pointeur sur chacune sans les ouvrir) ;
- noter le nom des programmes actifs dans la barre des tâches (passer le pointeur sur chaque icône sans cliquer) ;
- débrancher la prise de courant. Pour un ordinateur portable, enlever la batterie puis débrancher la prise d'alimentation. Ne jamais éteindre autrement ;
- vérifier la présence de disques dans le lecteur optique. Un outil semblable à un trombone permet d'ouvrir le lecteur hors alimentation ;
- ouvrir le scanner pour y vérifier la présence éventuelle de documents.

Les données qui sont de détention ou d'usage dangereux ou illicites doivent être effacées sur le support original.

L'article 60-3 du code de procédure pénale, modifié par la loi n° 2023-22 du 24 janvier 2023, permet aux OPJ et, sous leur contrôle, aux APJ ou assistants d'enquête, de requérir toute personne qualifiée afin de procéder à l'ouverture des scellés des objets qui sont le support de données informatiques pour réaliser une ou plusieurs copies de ces données ou de procéder aux opérations techniques nécessaires à leur mise à la disposition de l'OPJ, afin de permettre leur exploitation sans porter atteinte à leur intégrité.

La personne requise fait mention des opérations effectuées dans un rapport établi conformément aux articles 163 et 166 du CPP. Les opérations peuvent être réalisées par les services ou les organismes de police technique et scientifique de la police nationale et de la gendarmerie nationale dans les conditions prévues aux deuxième et troisième alinéas de l'article 60 du CPP (i.e.: pas besoin de réquisition pour des opérations techniques effectuées par des militaires de la gendarmerie au profit d'unités de gendarmerie).

**Saisies**

Une fois les constatations réalisées, il ne faut pas hésiter à saisir tout objet pouvant servir à la manifestation de la vérité et ne se trouvant pas nécessairement dans l'unité centrale. De ce fait :

- saisir les logiciels et documentations pour exploitation ultérieure ;
- saisir tous les supports quel que soit leur type (CD, DVD, clé USB, cartes mémoires, disques dur) ;
- saisir toutes notes sur lesquelles apparaissent des identifiants (login/mot de passe, des adresses mail, des URL,...).

Ne jamais explorer un ordinateur, une clé USB ou tout autre support numérique en direct.

L'ensemble de ces mesures s'applique aux différents types d'appareils (téléphones portables, lecteurs multimédias,...)

**Des enquêtes sous pseudonyme**

La loi du 24 janvier 2023 complète la liste des actes que les enquêteurs agissant dans le cadre d'une enquête sous pseudonyme dans les conditions prévues à l'article 230-46 du CPP peuvent accomplir aux fins de constater les crimes et les délits punis d'une peine d'emprisonnement commis par la voie des communications électroniques sans en être pénalement responsables.

Désormais, en vue de l'acquisition, de la transmission ou de la vente par les personnes susceptibles d'être les auteurs de ces infractions de tout contenu, produit, substance, prélèvement ou service, y compris illicite, les officiers ou agents de police judiciaires, peuvent mettre à la disposition de ces personnes des moyens juridiques ou financiers, ainsi que des moyens de transport, de dépôt, d'hébergement, de conservation et de télécommunication de (CP, article 230-46, 4°).

Comme pour les actes autorisés aux termes du 3° du même article, cette mise à disposition nécessite une autorisation préalable du procureur de la République ou du juge d'instruction saisi des faits. Cette autorisation peut être donnée par tout moyen. Elle doit être mentionnée ou versée au dossier de la procédure à peine de nullité étant précisé que les actes autorisés ne peuvent constituer une incitation à commettre ces infractions.

**Scellés**

Après la pose du scellé, il doit être impossible d'accéder ou de manipuler l'appareil ou son contenu, sans le briser.

## 8.3) Les unités spécialisées en gendarmerie

La gendarmerie possède un dispositif qui comprend notamment :

- des enquêteurs formés à la lutte contre la délinquance liée aux technologies numériques (N'TECH) au sein des BDRIJ, des SR et des SOLC ainsi que des enquêteurs qualifiés " introduction aux cybermenaces " (ICM) au sein des unités élémentaires ;
- des militaires formés à identifier, tracer et saisir la cryptomonnaie (FINTECH) au sein des SR et du C3N ;
- le commandement de la gendarmerie dans le cyberespace (ComCyberGend) : en particulier le C3N (division des opérations) et ses antennes au sein de certaines SR ainsi que la division de l'appui aux opérations numériques ;
- la division du renseignement du SCRCGN ;
- l'observatoire central des systèmes de transport intelligents du SCRCGN.

Ce dispositif :

- fournit une aide technique et juridique aux unités, avec un apport de moyens adaptés ;
- répond aux sollicitations des juridictions d'instruction ;
- collecte des informations, analyse, met en place des plans d'actions ;
- met à disposition des moyens nationaux ou internationaux.

## 8.4) L'office anti-cybercriminalité

Par décret n° 2000-405 du 15 mai 2000, a été créé au ministère de l'Intérieur (rattaché à la direction générale de la Police nationale, direction nationale de la police judiciaire), un office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.

Cet office est devenu l'office anti-cybercriminalité (OFAC) en 2023 [Décret n° 2023-1083 du 23 novembre 2023 portant création de l'office anti-cybercriminalité et article D8-1 du code de procédure pénale.].

La direction générale de la gendarmerie nationale, la direction générale de la sécurité intérieure, la direction générale des douanes et droits indirects, la direction générale de la concurrence, de la consommation et de la répression des fraudes et le ministère de la justice sont associées aux activités de cet office.

### 8.4.1) Compétence centrale

L'office contribue à la répression des formes spécialisées, organisées ou transnationales de la cybercriminalité et aux actions de prévention en la matière sous réserve des missions confiées à l'autorité nationale de sécurité des systèmes d'information (ANSSI) visée à l'article L2321-1 du code de la défense.

En effet, conformément à l'article L2321-1 du code de la défense, dans le cadre de la stratégie de sécurité nationale et de la politique de défense, c'est le Premier ministre qui définit la politique et qui coordonne l'action gouvernementale en matière de sécurité et de défense des systèmes d'information. Il dispose à cette fin de l'ANSSI, qui assure la fonction d'autorité nationale de défense des systèmes d'information.

L'office a pour domaine de compétence les infractions spécifiques à la criminalité liée aux technologies de l'information et de la communication, sans préjudice de celui des services de l'Etat chargés de la prévention et de la détection des atteintes aux intérêts fondamentaux de la Nation visés à l'article L811-3 du code de la sécurité intérieure (indépendance nationale, intégrité du territoire, intérêts majeurs, prévention du terrorisme, etc.).

**8.4.2) Compétence élargie**

Dans les conditions fixées à l'article 3 du décret n° 2023-1083 du 23 novembre 2023 portant création de l'office anti-cybercriminalité, sa compétence s'étend également aux infractions dont la commission est facilitée par ou liée à l'utilisation de ces technologies.

**8.4.3) Missions**

L'office est chargé :
1° D'animer et de coordonner, au niveau national, et au plan opérationnel la lutte contre les auteurs et complices d'infractions spécifiques à la criminalité liée aux technologies de l'information et de la communication dans son champ de compétence ;
2° De mener des enquêtes judiciaires en matière de cybercriminalité sous l'autorité du procureur de la République ou du juge d'instruction ;
3° De procéder, à la demande de l'autorité judiciaire, à tous actes d'enquête et de travaux techniques d'investigations numériques en assistance aux services chargés d'enquêtes de police judiciaire sur les infractions dont la commission est facilitée par ou liée à l'utilisation des technologies de l'information et de la communication, sans préjudice de la compétence des autres offices centraux de police judiciaire et des services de l'Etat chargés d'apporter une assistance technique à l'activité judiciaire ;
4° D'apporter assistance aux services de la police nationale, de la gendarmerie nationale, de la direction générale des douanes et droits indirects, de la direction générale de la concurrence, de la consommation et de la répression des fraudes et de tout autre service, en cas d'infractions visées aux deuxième et troisième alinéas de l'article 2 du présent décret, quand ils en font la demande. Cette assistance ne dessaisit pas les services demandeurs ;
5° D'intervenir d'initiative, avec l'accord de l'autorité judiciaire, chaque fois que les circonstances l'exigent, pour s'informer sur place des faits relatifs aux investigations conduites ;
6° De participer, dans son domaine de compétence, à des actions de formation ;
7° De recueillir et analyser le renseignement criminel dans son domaine de compétence et de contribuer à la production d'états de la menace induits par la cybercriminalité.

A cet effet, l'office centralise, analyse, exploite et communique aux services de la police nationale, de la gendarmerie nationale, de la direction générale des douanes et droits indirects et de la direction générale de la concurrence, de la consommation et de la répression des fraudes, ainsi qu'aux autres administrations et services publics de l'Etat concernés, toutes informations opérationnelles relatives aux faits et infractions liés aux technologies de l'information et de la communication. Il établit également les liaisons utiles avec les organismes du secteur privé concernés.

Dans le cadre de la législation applicable, notamment en matière de secret professionnel, les services de la police nationale, de la gendarmerie nationale, de la direction générale des douanes et droits indirects, ainsi que les autres administrations et services publics de l'Etat concernés, adressent, dans les meilleurs délais, à l'OFAC les informations dont ils ont connaissance ou qu'ils détiennent, relatives aux infractions visées aux deuxième et troisième alinéas de l'article 2 du décret n° 2023-1083 du 23 novembre 2023, à leurs auteurs et à leurs complices.

Pour les infractions relevant de sa compétence, l'office adresse toutes indications utiles à l'identification ou à la recherche des délinquants aux services de la police nationale, de la gendarmerie nationale, de la direction générale des douanes et droits indirects, de la direction générale de la concurrence, de la consommation et de la répression des fraudes, ainsi qu'aux autres administrations et services publics de l'Etat concernés et, sur leur demande, tous les renseignements utiles aux enquêtes dont ils sont saisis.
Chaque fois que les circonstances l'exigent, il intervient d'initiative avec l'accord de l'autorité judiciaire pour s'informer sur place des faits relatifs à l'enquête conduite.

Il collecte les informations détenues par les différents services.

Dans le domaine international comme dans le domaine national, il joue un rôle important de centralisation et de rediffusion des informations au profit des services compétents, de nature à permettre l'identification et la recherche des délinquants.
Depuis le mois de juin 2009 (Arrêté du 16 juin 2009), il a été créé au sein de la Direction générale de la Police nationale une plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS).

Elle est composée d'un site Internet et d'un traitement automatisé de données à caractère personnel.

L'objectif de cette plate-forme est de permettre aux utilisateurs et acteurs d'internet de signaler, sans préjudice du respect dû aux correspondances privées, des sites ou des contenus contraires aux lois et règlements diffusés sur Internet auprès de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.

Cet Office qui recueille de manière centralisée l'ensemble des signalements, effectue des rapprochements et oriente les données vers les services enquêteurs compétents en vue de leur exploitation.
Pour les infractions relevant de sa compétence définie au deuxième alinéa de l'article 2 du décret n° 2023-1083 pré-cité, l'OFAC constitue, pour la France, le point de contact central dans les échanges opérationnels internationaux. Il contribue au niveau national à l'animation et à la coordination des travaux préparatoires nécessaires et participe aux activités des organismes et enceintes internationaux. Sans préjudice de l'application des conventions internationales, il entretient les liaisons opérationnelles avec les services spécialisés des autres pays et avec les organismes internationaux en vue de rechercher toute information relative aux infractions ainsi qu'à l'identification et à la localisation de leurs auteurs.

# 9) Infractions

## 9.1) Atteintes aux systèmes de traitement automatisé de données

### 9.1.1) Accès ou maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données

**Éléments constitutifs**

- **Élément légal**
  Ce délit est prévu et réprimé par l'article 323-1 du Code pénal.
- **Élément matériel**
  - Il faut :
    - un accès ou un maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données. Il s'agit de protéger les systèmes de traitement automatisé de données des intrusions faites par les « pirates » de l'informatique. L'accès ou le maintien dans un système de traitement n'est pas autorisé dès lors que l'on cherche à s'introduire indûment dans un système protégé. La présence d'un dispositif de sécurité est très importante. Elle démontre que le système n'est accessible qu'aux personnes autorisées. L'accès révèle le caractère irrégulier de la manoeuvre. Par système de traitement automatisé de données, il faut comprendre l'ensemble ordinateur-mémoires (contenant) et les informations enregistrées sur les supports magnétiques (contenu)
    - entendre par quiconque, toute personne utilisatrice, habilitée ou non, à se servir du

système de traitement automatisé de données.

- **Élément moral**
    - Il est caractérisé par l'intention coupable. L'accès ou le maintien dans le système de traitement automatisé de données ne constitue une infraction que s'il est conscient et frauduleux. L'intention de nuire n'est pas nécessaire. L'action ou le maintien même par jeu ou défi technique est moralement coupable. S'agissant d'un délit intentionnel, l'accès par inadvertance ou le maintien inconscient n'est pas incriminé. Il faut au minimum que l'auteur de l'acte agisse sciemment, mais il n'est pas nécessaire qu'il ait l'intention de nuire. *Exemple : l'entrée par erreur ne caractérise pas l'accès frauduleux mais le maintien conscient à la suite de cette erreur est punissable.*

**Circonstances aggravantes**
Le délit est aggravé lorsqu'il en est résulté :

- la suppression de données contenues dans le système
- la modification de ces données
- l'altération du fonctionnement de ce système (CP, art. 323-1, al. 2).

Il en est de même lorsque cette infraction a été commise :

- à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'État (CP, art. 323-1, al. 3) ;
- en bande organisée (CP, art. 323-4-1) ;
- lorsque ces faits ont pour effet d'exposer autrui à un risque immédiat de mort ou de blessures de nature à entraîner une mutilation ou une infirmité permanente ou de faire obstacle aux secours destinés à faire échapper une personne à un péril imminent ou à combattre un sinistre présentant un danger pour la sécurité des personnes (CP, art. 323-4-2).

**Pénalités**

| Infractions | Qualifications | Prévues et réprimées | Peines |
|---|---|---|---|
| Accès ou maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données [La loi dite LOPMI n°2023-22 du 24 janvier 2023 a aggravé les peines des infractions prévues à l'article 323-1 du code pénal et a également modifié l'article 323-4-1 pour élargir la commission en " bande organisée " à l'ensemble des infractions prévues par le 323-1 CP et non plus seulement lorsque des systèmes mis en oeuvre par l'Etat sont visés.] | Délit | CP, art. 323-1, al. 1 | Emprisonnement de trois ans<br>Amende de 100 000 euros |
| Suppression ou modification de données contenues dans le système ou altération du fonctionnement de ce système suite à un accès ou à un maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données | Délit | CP, art. 323-1, al. 2 | Emprisonnement de cinq ans<br>Amende de 150 000 euros |
| Accès ou maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'État | Délit | CP, art. 323-1, al. 1 et 3 | Emprisonnement de sept ans<br>Amende de 300 000 euros |

| | | | |
|---|---|---|---|
| Suppression ou modification de données contenues dans le système ou altération du fonctionnement de ce système suite à un accès ou à un maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'État | Délit | CP, art. 323-1 | Emprisonnement de sept ans<br>Amende de 300 000 euros |
| Accès ou maintien frauduleux, commis en bande organisée, dans tout ou partie d'un système de traitement automatisé de données | Délit | CP, art. 323-1, al. 1 et 323-4-1 | Emprisonnement de 10 ans<br>Amende de 300 000 euros |
| Suppression ou modification de données contenues dans le système ou altération du fonctionnement de ce système, commis en bande organisée, suite à un accès ou à un maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données | Délit | CP, art. 323-1 al. 2 et 323-4-1 | Emprisonnement de 10 ans<br>Amende de 300 000 euros |
| Accès ou maintien frauduleux, commis en bande organisée, dans tout ou partie d'un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'État | Délit | CP, art. 323-1, al. 1 et 3 et 323-4-1 | Emprisonnement de 10 ans<br>Amende de 300 000 euros |
| Suppression ou modification de données contenues dans le système ou altération du fonctionnement de ce système, commis en bande organisée, suite à un accès ou à un maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'État | Délit | CP, art. 323-1 et 323-4-1 | Emprisonnement de 10 ans<br>Amende de 300 000 euros |
| Accès ou maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données ayant pour effet d'exposer autrui à un risque immédiat de mort ou de blessures de nature à entraîner une mutilation ou une infirmité permanente ou de faire obstacle aux secours destinés à faire échapper une personne à un péril imminent ou à combattre un sinistre présentant un danger pour la sécurité des personnes | Délit | CP, art. 323-1, al. 1 et 323-4-2 | Emprisonnement de 10 ans<br>Amende de 300 000 euros |
| Suppression ou modification de données contenues dans le système ou altération du fonctionnement de ce système suite à un accès ou à un maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données ayant pour effet d'exposer autrui à un risque immédiat de mort ou de blessures de nature à entraîner une mutilation ou une infirmité permanente ou de faire obstacle aux secours destinés à faire échapper une personne à un péril imminent ou à combattre un sinistre présentant un danger pour la sécurité des personnes | Délit | CP, art. 323-1, al. 2 et 323-4-2 | Emprisonnement de 10 ans<br>Amende de 300 000 euros |

| | | | |
|---|---|---|---|
| Accès ou maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'État ayant pour effet d'exposer autrui à un risque immédiat de mort ou de blessures de nature à entraîner une mutilation ou une infirmité permanente ou de faire obstacle aux secours destinés à faire échapper une personne à un péril imminent ou à combattre un sinistre présentant un danger pour la sécurité des personnes | Délit | CP, art. 323-1, al. 1 et 3 et 323-4-2 | Emprisonnement de 10 ans<br>Amende de 300 000 euros |
| Suppression ou modification de données contenues dans le système ou altération du fonctionnement de ce système suite à un accès ou à un maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'État ayant pour effet d'exposer autrui à un risque immédiat de mort ou de blessures de nature à entraîner une mutilation ou une infirmité permanente ou de faire obstacle aux secours destinés à faire échapper une personne à un péril imminent ou à combattre un sinistre présentant un danger pour la sécurité des personnes | Délit | CP, art. 323-1 et 323-4-2 | Emprisonnement de 10 ans<br>Amende de 300 000 euros |

**Tentative**
La tentative, expressément prévue à l'article 323-7 du Code pénal, est punissable des mêmes peines que le délit.

**Responsabilité des personnes morales**
Les personnes morales peuvent être condamnées à certaines peines prévues par l'article 131-39 du Code pénal (CP, art. 323-6).

**Possibilité de recours à la procédure simplifiée d'ordonnance pénale**
La loi du 24 janvier 2023 vient modifier la liste des infractions prévues par l'article 398-1 du CPP et ainsi étendre le champ de compétence de la procédure de jugement correctionnel à juge unique prévue par l'article 398 du CPP aux délits d'accès et de maintien frauduleux dans un système de traitement automatisé de données prévus au premier alinéa de l'article 323-1 du code pénal.

Au-delà de la possibilité d'orienter le jugement de ces délits devant le tribunal correctionnel statuant à juge unique, il pourra désormais être décidé de recourir à la procédure simplifiée de l'ordonnance pénale. Cette extension, qui recouvre notamment les situations de piratage d'un compte de messagerie électronique ou d'un réseau social, offrira ainsi la possibilité d'un traitement simplifié de ce type d'infractions lorsque la personnalité de l'auteur, l'ampleur du préjudice ou la qualité de la victime le justifieront.

### 9.1.2) Entrave ou altération du fonctionnement d'un système automatisé de données

**Éléments constitutifs**

- **Élément légal**
  - Ce délit est prévu et réprimé par l'article 323-2 du Code pénal.
- **Élément matériel**
  - Il faut une entrave ou une altération du fonctionnement d'un système de traitement de données. Les techniques susceptibles de fausser (entraver ou altérer) le fonctionnement d'un système sont très diverses. On peut citer les bombes logiques, les virus, le cheval de

Troie mais aussi des sabotages de matériel.

- **Élément moral**
    - Il est caractérisé par l'intention coupable. La maladresse n'est pas constitutive de l'intention coupable. Il faut la conscience de l'entrave apportée, ou d'une violation délibérée d'un interdit même sans volonté de nuire ou de causer un préjudice.

**Circonstances aggravantes**
Le délit est aggravé lorsque les faits sont exercés à l'encontre d'un système de traitement automatisé de données mis en oeuvre par l'État (CP, art. 323-2, al. 2).

Il en est de même lorsque cette infraction a été commise :

- en bande organisée (CP, art. 323-4-1) ;
- lorsque ces faits ont pour effet d'exposer autrui à un risque immédiat de mort ou de blessures de nature à entraîner une mutilation ou une infirmité permanente ou de faire obstacle aux secours destinés à faire échapper une personne à un péril imminent ou à combattre un sinistre présentant un danger pour la sécurité des personnes (CP, art. 323-4-2).

**Pénalités**

| Infractions | Qualifications | Prévues et réprimées | Peines |
|---|---|---|---|
| Entrave ou altération du fonctionnement d'un système de traitement automatisé de données | Délit | CP, art. 323-2, al. 1 | Emprisonnement de cinq ans<br>Amende de 150 000 euros |
| Entrave ou altération du fonctionnement d'un système de traitement automatisé de données mis en oeuvre par l'État | Délit | CP, art. 323-2 | Emprisonnement de sept ans<br>Amende de 300 000 euros |
| Entrave ou altération, en bande organisée, du fonctionnement d'un système de traitement automatisé de données | Délit | CP, art. 323-2, al. 1 et 323-4-1 | Emprisonnement de dix ans<br>Amende de 300 000 euros |
| Entrave ou altération, en bande organisée, du fonctionnement d'un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'État | Délit | CP, art. 323-2 et 323-4-1 | Emprisonnement de dix ans<br>Amende de 300 000 euros |
| Entrave ou altération du fonctionnement d'un système de traitement automatisé de données ayant pour effet d'exposer autrui à un risque immédiat de mort ou de blessures de nature à entraîner une mutilation ou une infirmité permanente ou de faire obstacle aux secours destinés à faire échapper une personne à un péril imminent ou à combattre un sinistre présentant un danger pour la sécurité des personnes | Délit | CP, art. 323-2, al. 1 et 323-4-2 | Emprisonnement de dix ans<br>Amende de 300 000 euros |

| | | | |
|---|---|---|---|
| Entrave ou altération du fonctionnement d'un système de traitement automatisé de données mis en oeuvre par l'État ayant pour effet d'exposer autrui à un risque immédiat de mort ou de blessures de nature à entraîner une mutilation ou une infirmité permanente ou de faire obstacle aux secours destinés à faire échapper une personne à un péril imminent ou à combattre un sinistre présentant un danger pour la sécurité des personnes | Délit | CP, art. 323-2 et 323-4-1 et 323-4-2 | Emprisonnement de dix ans<br>Amende de 300 000 euros |

**Tentative**
La tentative, expressément prévue à l'article 323-7 du Code pénal, est punissable des mêmes peines que le délit.

**Responsabilité des personnes morales**
Les personnes morales peuvent être condamnées à certaines peines prévues par l'article 131-39 du Code pénal (CP, art. 323-6)

### 9.1.3) Introduction, extraction, détention, reproduction, transmission, suppression ou modification frauduleuse de données dans un système de traitement automatisé

**Éléments constitutifs**

- **Élément légal**
  - Ce délit est prévu et réprimé par l'article 323-3 du Code pénal.
- **Élément matériel**
  - Il faut :
    - une introduction, une extraction, une détention, une reproduction, une transmission, une suppression ou une modification de données dans un système de traitement automatisé ;
    - par le fait de quiconque ;
    - que cette action soit frauduleuse.
- **Élément moral**
  - Il est caractérisé par l'intention coupable.
  - Celle-ci résulte de la volonté de nuire par exemple par l'introduction de données de type virus informatique.

**Circonstances aggravantes**
Le délit est aggravé lorsque les faits sont exercés à l'encontre d'un système de données à caractère personnel mis en oeuvre par l'État (CP, 323-3, al. 2)

Il en est de même lorsque cette infraction a été commise en bande organisée (CP, art. 323-4-1) ou lorsque ces faits ont pour effet d'exposer autrui à un risque immédiat de mort ou de blessures de nature à entraîner une mutilation ou une infirmité permanente ou de faire obstacle aux secours destinés à faire échapper une personne à un péril imminent ou à combattre un sinistre présentant un danger pour la sécurité des personnes (CP, art. 323-4-2).

**Pénalités**

| Infractions | Qualifications | Prévues et réprimées | Peines |
|---|---|---|---|
| | | | |

| | | | |
|---|---|---|---|
| Introduction, extraction, détention, reproduction, transmission, suppression ou modification frauduleuse de données dans un système de traitement automatisé | Délit | CP, art. 323-3, al. 1 | Emprisonnement de cinq ans<br>Amende de 150 000 euros |
| Introduction, extraction, détention, reproduction, transmission, suppression ou modification frauduleuse de données dans un système de traitement automatisé mis en oeuvre par l'État | Délit | CP, art. 323-3 | Emprisonnement de sept ans<br>Amende de 300 000 euros |
| Introduction, extraction, détention, reproduction, transmission, suppression ou modification frauduleuse de données dans un système de traitement automatisé commises en bande organisée | Délit | CP, art. 323-3, al. 1 et 323-4-1 | Emprisonnement de dix ans<br>Amende de 300 000 euros |
| Introduction, extraction, détention, reproduction, transmission, suppression ou modification frauduleuse de données dans un système de traitement automatisé mis en oeuvre par l'État commises en bande organisée | Délit | CP, art. 323-3 et 323-4-1 | Emprisonnement de dix ans<br>Amende de 300 000 euros |
| Introduction, extraction, détention, reproduction, transmission, suppression ou modification frauduleuse de données dans un système de traitement automatisé ayant pour effet d'exposer autrui à un risque immédiat de mort ou de blessures de nature à entraîner une mutilation ou une infirmité permanente ou de faire obstacle aux secours destinés à faire échapper une personne à un péril imminent ou à combattre un sinistre présentant un danger pour la sécurité des personnes | Délit | CP, art. 323-3, al. 1 et 323-4-2 | Emprisonnement de dix ans<br>Amende de 300 000 euros |
| Introduction, extraction, détention, reproduction, transmission, suppression ou modification frauduleuse de données dans un système de traitement automatisé mis en oeuvre par l'État ayant pour effet d'exposer autrui à un risque immédiat de mort ou de blessures de nature à entraîner une mutilation ou une infirmité permanente ou de faire obstacle aux secours destinés à faire échapper une personne à un péril imminent ou à combattre un sinistre présentant un danger pour la sécurité des personnes | Délit | CP, art. 323-3 et 323-4-2 | Emprisonnement de dix ans<br>Amende de 300 000 euros |

**Tentative**
La tentative, expressément prévue à l'article 323-7 du Code pénal, est punissable des mêmes peines que le délit.

**Responsabilité des personnes morales**
Les personnes morales peuvent être condamnées à certaines peines prévues par l'article 131-39 du Code pénal (CP, art. 323-6).

**9.1.4) Importation, détention, offre, cession ou mise à disposition, sans motif légitime, d'un équipement,**

**d'un instrument, d'un programme informatique ou donnée conçu ou adapté pour une atteinte frauduleuse aux données d'un système de traitement automatisé**

**Éléments constitutifs**

- **Élément légal**
  - Ce délit est prévu et réprimé par l'article 323-3-1 du Code pénal.
- **Élément matériel**
  - Il faut :
    - une importation, détention, offre, cession ou mise à disposition d'un équipement, un instrument, un programme informatique ou toute donnée ;
    - sans motif légitime ;
    - que l'équipement, l'instrument, le programme informatique ou toute donnée soient conçus ou spécialement adaptés pour commettre l'un des actes de piratage prévus aux articles 323-1 à 323-3 du Code pénal.
- **Élément moral**
  - Il est caractérisé par l'intention coupable.

**Cette infraction a été conçue pour lutter contre la prolifération des virus sur les réseaux informatiques.**

**Circonstance aggravante**

Le délit est aggravé lorsque cette infraction a été commise en bande organisée (CP, art. 323-4-1);

à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'État;

ou lorsqu'il a pour effet d'exposer autrui à un risque immédiat de mort ou de blessures de nature à entraîner une mutilation ou une infirmité permanente ou de faire obstacle aux secours destinés à faire échapper une personne à un péril imminent ou à combattre un sinistre présentant un danger pour la sécurité des personnes (CP, art. 323-4-2).

**Pénalités**

| Infractions | Qualifications | Prévues et réprimées | Peines |
|---|---|---|---|
| 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 du code pénal, y compris à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'Etat | Délit | CP, art. 323-3-1 | Peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée |

| | | | |
|---|---|---|---|
| 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 du code pénal, commis en bande organisée, y compris à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'Etat | Délit | CP, art. 323-3-1 et 323-4-1 | Dix ans d'emprisonnement<br>300 000 euros d'amende |
| 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 du code pénal ayant pour effet d'exposer autrui à un risque immédiat de mort ou de blessures de nature à entraîner une mutilation ou une infirmité permanente ou de faire obstacle aux secours destinés à faire échapper une personne à un péril imminent ou à combattre un sinistre présentant un danger pour la sécurité des personnes, y compris à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'Etat | Délit | CP, art. 323-3-1 et 323-4-2 | Dix ans d'emprisonnement<br>300 000 euros d'amende |

**Tentative**
La tentative, expressément prévue à l'article 323-7 du Code pénal, est punissable des mêmes peines que le délit.

**Responsabilité des personnes morales**
Les personnes morales peuvent être condamnées à certaines peines prévues par l'article 131-39 du Code pénal (CP, art. 323-6).

**Dispositions relatives à l'assurance des risques de cyberattaques**
Afin de renforcer la capacité des autorités à réagir rapidement et efficacement à une cyberattaque et de permettre une meilleure articulation avec l'objectif d'indemnisation de ses conséquences préjudicielles, la loi dite " LOPMI" entrée en vigueur en 2023 a inséré un nouvel article L12-10-1 dans le code des assurances qui subordonne le versement d'une somme en application de la clause d'un contrat d'assurance visant à indemniser un assuré des pertes et dommages causés par une atteinte à un système de traitement automatisé de données mentionnée aux articles 323-1 à 323-3-1 du code pénal au *dépôt d'une plainte de la victime*.

Ce dépôt de plainte doit intervenir au plus tard soixante-douze heures après la connaissance de l'atteinte par la victime. Ces nouvelles dispositions - qui entreront en vigueur trois mois après la promulgation de la loi du 24 janvier 2023 - s'appliqueront uniquement aux personnes morales et aux personnes physiques victimes de cyber-attaques dans le cadre de leur activité professionnelle.

## 9.2) Administration d'une plateforme en ligne pour permettre la cession de produits illicites

**Eléments constitutifs**

- **Elément légal**

Ce délit est prévu et réprimé par l'article 323-3-2, I, du code pénal. [Article créé par la loi n°2023-22 du 24 janvier 2023 dite " LOPMI " dans le cadre des dispositions relatives à la révolution numérique du ministère de l'Intérieur.]

- **Eléments matériels**

Il faut :

1. le fait, pour une personne dont l'activité consiste à fournir un service de plateforme en ligne,
2. de permettre, sciemment,
3. la cession de produits, de contenus ou de services dont la cession, l'offre, l'acquisition ou la détention sont manifestement illicites,
4. lorsque ladite personne chargée de fournir ce service restreint son accès aux personnes utilisant des techniques d'anonymisation de connexion ou
5. qu'elle contrevient aux obligations mentionnées au V de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ou celles mentionnées aux articles 15,16 et 18 du règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/ CE.
   [Il s'agit, pour les personnes dont l'activité consiste à fournir des services d'accès à internet ou des services d'hébergement de détenir et de conserver les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires.]

- **Elément moral**

Il est caractérisé par l'intention coupable. Il faut la conscience de l'entrave apportée ou d'une violation délibérée d'un interdit.

**Circonstance aggravante**
Les faits sont aggravés lorsqu'ils ont été commis en bande organisée (III, art. 323-3-2 du code pénal).

**Pénalités**

| Infractions | Qualifications | Prévues et réprimées par | Peines |
|---|---|---|---|
| Le fait, pour une personne dont l'activité consiste à fournir un service de plateforme en ligne mentionné au 4 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique qui restreint l'accès à ce service aux personnes utilisant des techniques d'anonymisation des connexions ou qui ne respecte pas les obligations mentionnées au V du même article 6 ou celles mentionnées aux articles 15,16 et 18 du règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022, de permettre sciemment la cession de produits, de contenus ou de services dont la cession, l'offre, l'acquisition ou la détention sont manifestement illicites | Délit | CP, 323-3-2, I | 7 ans d'emprisonnement<br>500 000 euros d'amende |
| Circonstance aggravante : | | | |

| | | | |
|---|---|---|---|
| Fait, commis en bande organisée, pour une personne dont l'activité consiste à fournir un service de plateforme en ligne, de permettre sciemment la cession de produits, de contenus ou de services dont la cession, l'offre, l'acquisition ou la détention sont manifestement illicites, lorsque ladite personne chargée de fournir ce service restreint son accès aux personnes utilisant des techniques d'anonymisation de connexion ou qu'elle contrevient aux obligations mentionnées au V de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique | Délit | CP, 323-3-2, I et III | 10 ans d'emprisonnement<br>1 000 000 euros d'amende |

**Tentative**
La tentative des infractions prévues aux I et III de l'article 323-3-2 du code pénal est punie des mêmes peines.

**Responsabilité pénale des personnes morales**
Les personnes morales encourent, outre l'amende suivant les modalités prévues par l'article 131-38 CP, les peines prévues par l'article 131-39 CP (CP, art. 323-6).

## 9.3) Intermédiation ou séquestre pour faciliter la cession de produits illicites

**Elément constitutifs**

- **Elément légal**

Ce délit est prévu et réprimé par l'article 323-3-2, I et II, du code pénal.

- **Eléments matériels**

Il faut :

1. le fait de proposer,
2. par l'intermédiaire d'un fournisseur de plateformes en ligne
3. ou au soutien de transactions permises par ces plateformes,
4. lorsque les opérateurs de ces plateformes en restreignent l'accès aux personnes utilisant des techniques d'anonymisation de connexion ou
5. que ces derniers contreviennent aux obligations mentionnées au VI de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique,
6. des prestations d'intermédiation
7. ou des prestations de séquestre,
8. lorsque ces deux types de prestations ont pour objet unique ou principal de mettre en oeuvre, de dissimuler ou de faciliter les opérations mentionnées I de l'article 323-3-2 du code pénal.

- **Elément moral**

Il est caractérisé par l'intention coupable.

**Circonstance aggravante**
Les faits sont aggravés lorsqu'ils ont été commis en bande organisée (III, art. 323-3-2 du code pénal).

**Pénalités**

| Infractions | Qualifications | Prévues et réprimées par | Peines |
|---|---|---|---|
| Fait de proposer, par l'intermédiaire d'un fournisseur de plateformes en ligne ou au soutien de transactions permises par ces dernières, des prestations d'intermédiation qui ont pour objet unique ou principal de mettre en oeuvre, de dissimuler ou de faciliter les opérations mentionnées au I de l'article 323-3-2 du code pénal | Délit | CP, 323-3-2, I et II | 5 ans d'emprisonnement<br>150 000 euros d'amende |
| Fait de proposer, par l'intermédiaire d'un fournisseur de plateformes en ligne ou au soutien de transactions permises par ces dernières, des prestations de séquestre qui ont pour objet unique ou principal de mettre en oeuvre, de dissimuler ou de faciliter les opérations mentionnées au I de l'article 323-3-2 du code pénal | Délit | CP, 323-3-2, I et II | 5 ans d'emprisonnement<br>150 000 euros d'amende |
| Circonstance aggravante : | | | |
| Fait, commis en bande organisée, de proposer, par l'intermédiaire d'un fournisseur de plateformes en ligne ou au soutien de transactions permises par ces dernières, des prestations d'intermédiation qui ont pour objet unique ou principal de mettre en oeuvre, de dissimuler ou de faciliter les opérations mentionnées au I de l'article 323-3-2 du code pénal | Délit | CP, 323-3-2, I, II et III | 10 ans d'emprisonnement<br>500 000 euros d'amende |

| | | | |
|---|---|---|---|
| Fait, commis en bande organisée, de proposer, par l'intermédiaire d'un fournisseur de plateformes en ligne ou au soutien de transactions permises par ces dernières, des prestations de séquestre qui ont pour objet unique ou principal de mettre en oeuvre, de dissimuler ou de faciliter les opérations mentionnées au I de l'article 323-3-2 du code pénal | Délit | CP, 323-3-2, I, II et III | 10 ans d'emprisonnement<br>500 000 euros d'amende |

**Tentative**
La tentative des infractions prévues aux I, II et III de l'article 323-3-2 du code pénal est punie des mêmes peines.

**Responsabilité pénale des personnes morales**
Les personnes morales encourent, outre l'amende suivant les modalités prévues par l'article 131-38 CP, les peines prévues par l'article 131-39 CP (CP, art. 323-6).

Ayant été intégré à la liste de l'article 706-73-1 (12°) du code de procédure pénale, le recours aux techniques spéciales d'enquêtes est permis dans le cadre des infractions prévues par l'article 323-3-2 du CP. Les juridictions interrégionales spécialisées (JIRS) et la juridiction nationale de lutte contre la criminalité organisée (JUNALCO) disposent par ailleurs d'une compétence concurrente pour traiter de ces nouvelles infractions, sous réserve qu'elles présentent un critère de grande ou de très grande complexité (art. 706-75 du CPP). Afin de pouvoir exercer ses compétences, il est rappelé que la JUNALCO doit pouvoir bénéficier d'une remontée d'informations pertinente par le mécanisme de la double information qui doit être mise en oeuvre à son profit par les offices centraux et services à compétence nationale ainsi que par les JIRS, à la lumière des critères supra énoncés [Circulaire DACG n° JUSD2303546C du 3 février 2023 concernant la LOPMI 2023-22.].

## 9.4) Participation à un groupement formé ou à une entente établie en vue de la préparation d'une ou des infractions relatives à la fraude informatique

**Éléments constitutifs**

- **Élément légal**
  - Ce délit est prévu et réprimé par l'article 323-4 du Code pénal.
- **Élément matériel**
  - Il faut :
    - qu'il y ait participation, par quiconque, à un groupement même non structuré ou une entente réunissant au moins deux personnes ;
    - que ce groupement ou cette entente soit établi pour préparer :
      - soit un accès frauduleux à un système de traitement automatisé de données,
      - soit une atteinte au bon fonctionnement d'un système de traitement automatisé de données. Par atteinte, il faut comprendre l'introduction de données, la suppression ou la modification de données ou du mode de traitement ou de transmission de données,
      - soit l'importation, la détention, l'offre, la cession ou la mise à disposition d'un équipement conçu ou adapté pour commettre l'un des actes de piratage visés à l'article 323-1 à 323-3 du Code pénal ;
    - que la préparation de ces infractions soit caractérisée par un ou plusieurs faits matériels. L'incrimination vise essentiellement les actes préparatoires aux accès

frauduleux ou en vue d'atteintes au bon fonctionnement d'un système de traitement automatisé de données. Les actes préparatoires peuvent se révéler, par exemple :

- par la détention d'un listage, d'un programme, d'un système informatique,
- par la connaissance non autorisée d'un code d'accès à un système de traitement automatisé de données.

- **Élément moral**
  - Il est caractérisé par l'intention coupable.
  - La participation consciente et volontaire à un groupement ou à une entente établie en vue de préparer des actes frauduleux est constitutive de l'intention coupable.

**Pénalités**

| Infractions | Qualifications | Prévues et réprimées | Peines |
|---|---|---|---|
| Participation à un groupement formé ou à une entente établie en vue de la préparation d'une ou plusieurs infractions relatives à la fraude informatique | Délit | CP, art. 323-4 | Peines prévues pour l'infraction elle-même visée par les articles 323-1 à 323-3-1 du Code pénal ou pour l'infraction la plus sévèrement réprimée |

**Tentative**
La tentative de ce délit n'est pas punissable et elle n'est pas concevable puisqu'il s'agit déjà de simples actes préparatoires érigés en infraction.

**Responsabilité des personnes morales**
Les personnes morales peuvent être condamnées à certaines peines prévues par l'article 131-39 du Code pénal (CP, art. 323-6).

## 9.5) Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques

### 9.5.1) Traitements de données à caractère personnel sans respect des formalités préalables à leur mise en oeuvre

**Éléments constitutifs**

- **Élément légal**
  - Ce délit est prévu et réprimé par l'article 226-16 du Code pénal.
- **Élément matériel**
  - Il faut :
    - procéder à des traitements de données à caractère personnel ;
    - ne pas respecter les formalités préalables à leur mise en oeuvre. Suivant le cas, la formalité préalable consiste en la prise d'un acte réglementaire après avis de la CNIL pour un traitement au profit d'un service ou établissement public *(loi n° 78-17 du 6 janvier 1978, art. 20, 3° III*) ou une déclaration à la CNIL pour un traitement par un établissement privé *(loi n° 78-17 du 6 janvier 1978, art. 16)* ;
    - que l'auteur soit :
      - celui qui fait procéder au traitement,
      - celui qui procède à celui-ci.
- **Élément moral**

- Il est caractérisé par l'intention coupable.
- C'est la conscience de ne pas respecter les formalités préalables. La négligence constitue également l'intention coupable.

**Pénalités**

| Infraction | Qualification | Prévue et réprimée | Peines |
|---|---|---|---|
| Traitements de données à caractère personnel sans respect des formalités préalables à leur mise en oeuvre | Délit | CP, art. 226-16 | Emprisonnement de cinq ans<br>Amende de 300 000 euros |

**Responsabilité des personnes morales**
Les personnes morales peuvent être condamnées à certaines peines prévues par l'article 131-39 du Code pénal (CP, art. 226-24).

**9.5.2) Traitements de données à caractère personnel sans prendre les précautions utiles pour préserver leur sécurité**

**Éléments constitutifs**

- **Élément légal**
  Ce délit est prévu et réprimé par l'article 226-17 du Code pénal.
- **Élément matériel**
  - Il faut :
    - procéder ou faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites aux articles du règlement de 27 avril 2016 et de la loi n° 78-17 du 6 janvier 1978 ;
    - ne pas prendre de précaution. Cela consiste notamment en :
      - une déformation des informations,
      - un dommage aux informations,
      - une communication à des tiers non autorisés ;
    - que l'auteur soit :
      - celui qui procède au traitement,
      - celui qui fait procéder à celui-ci.
- **Élément moral**
  - Il est caractérisé par l'intention coupable.
  - Cette dernière se déduit de la négligence consistant à ne pas prendre toutes les précautions utiles pour préserver des informations.

**Pénalités**

| Infraction | Qualification | Prévue et réprimée | Peines |
|---|---|---|---|
| Traitements de données à caractère personnel sans prendre les précautions utiles pour préserver leur sécurité | Délit | CP, art. 226-17 | Emprisonnement de cinq ans<br>Amende de 300 000 euros |

**Responsabilité des personnes morales**
Les personnes morales peuvent être condamnées à certaines peines prévues par l'article 131-39 du Code pénal (CP, art. 226-24).

### 9.5.3) Défaut de notification d'une violation de données à caractère personnel

**Éléments constitutifs**

- **Élément légal**
  - Ce délit est prévu et réprimé par l'article 226-17-1 du Code pénal.
- **Élément matériel**
  Il faut :
  - qu'un fournisseur de services de communications électroniques ou un responsable de traitement,
  - ne procède pas à la notification d'une violation de données à caractère personnel,
  - à la CNIL ou à l'intéressé.
- **Élément moral**
  - Il est caractérisé par l'intention coupable.

**Pénalités**

| Infractions | Qualifications | Prévues et réprimées | Peines |
|---|---|---|---|
| Défaut de notification d'une violation de données à caractère personnel | Délit | CP, art. 226-17-1, al 1 | Emprisonnement de cinq ans<br>Amende de 300 000 euros |

**Responsabilité des personnes morales**
Les personnes morales peuvent être condamnées à certaines peines prévues par l'article 131-39 du Code pénal (CP, art. 226-24).

### 9.5.4) Collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite

**Éléments constitutifs**

- **Élément légal**
  - Ce délit est prévu et réprimé par l'article 226-18 du Code pénal.
- **Élément matériel**
  - Il faut collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite.
  - S'applique aussi aux fichiers non automatisés ou mécanographiques dont l'usage ne relève pas exclusivement de l'exercice du droit à la vie privée.
- **Élément moral**
  - Il est caractérisé par l'intention coupable.
  - L'usage d'un moyen frauduleux, déloyal ou illicite démontre l'intention.

**Pénalités**

| Infractions | Qualifications | Prévues et réprimées | Peines |
|---|---|---|---|
| Collecte de données à caractère personnel par un moyen frauduleux | Délit | CP, art. 226-18 | Emprisonnement de cinq ans<br>Amende de 300 000 euros |

**De plus, la constitution et l'utilisation à des fins de prospection ou de promotion commerciale de fichiers, composés à partir de prescriptions médicales ou de pathologies diagnostiquées, constituent un délit puni de deux ans d'emprisonnement et de 75 000 euros d'amende, dès lors que ces fichiers permettent d'identifier directement ou indirectement le professionnel prescripteur (CSP, art. L. 4113-7 et L. 4163-9).**

**Responsabilité des personnes morales**
Les personnes morales peuvent être condamnées à certaines peines prévues par l'article 131-39 du Code pénal (CP, art. 226-24).

**9.5.5) Traitement de données à caractère personnel malgré l'opposition légitime de la personne concernée**

**Éléments constitutifs**

- **Élément légal**
  Ce délit est prévu et réprimé par l'article 226-18-1 du Code pénal.
- **Élément matériel**
  - Il faut :
    - procéder à un traitement de données à caractère personnel concernant une personne physique. S'applique aussi aux fichiers non automatisés ou mécanographiques dont l'usage ne relève pas exclusivement de l'exercice du droit à la vie privée ;
    - procéder à un traitement malgré l'opposition de cette personne, lorsque le traitement répond à des fins de prospection ou lorsque cette opposition est fondée sur des raisons légitimes.
- **élément moral**
  - Il est caractérisé par l'intention coupable.

**Pénalités**

| Infractions | Qualifications | Prévues et réprimées | Peines |
|---|---|---|---|
| Traitement de données à caractère personnel concernant une personne physique, malgré l'opposition légitime de la personne | Délit | CP, art. 226-18-1 | Emprisonnement de cinq ans<br>Amende de 300 000 euros |

**Responsabilité des personnes morales**
Les personnes morales peuvent être condamnées à certaines peines prévues par l'article 131-39 du Code pénal (CP, art. 226-24).

### 9.5.6) Conservation en mémoire informatisée, sans le consentement exprès de l'intéressé

**Éléments constitutifs**

- **Élément légal**
  - Ce délit est prévu et réprimé par les articles 226-19 du Code pénal.
- **Élément matériel**
  - Il faut :
    - conserver en mémoire informatisée des données à caractère personnel. S'applique aussi aux fichiers non automatisés ou mécanographiques dont l'usage ne relève pas exclusivement de l'exercice du droit à la vie privée ;
    - que la loi n'ait pas prévu de dérogation ;
    - que les données fassent apparaître, directement ou indirectement, les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales ou les moeurs de l'intéressé
    - ou des données concernant des infractions, des condamnations ou des mesures de sûreté.
- **Élément moral**
  - Il est caractérisé par l'intention coupable.

**Pénalités**

| Infraction | Qualification | Prévue et réprimée | Peines |
|---|---|---|---|
| Conservation en mémoire informatisée sans le consentement exprès de l'intéressé | Délit | CP, art. 226-19 | Emprisonnement de cinq ans<br>Amende de 300 000 euros |

**Responsabilité des personnes morales**
Les personnes morales peuvent être condamnées à certaines peines prévues par l'article 131-39 du Code pénal (CP, art. 226-24).

### 9.5.7) Traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé sans information de la personne concernée

**Éléments constitutifs**

- **Élément légal**
  - Ce délit est prévu et réprimé par l'article 226-19-1, alinéa 1 et 1°, du Code pénal.
- **Élément matériel**
  - Il faut :
    - procéder à un traitement de données à caractère personnel dans le cadre de la recherche dans le domaine de la santé concernant une personne physique. S'applique aussi aux fichiers non automatisés ou mécanographiques dont l'usage ne relève pas exclusivement de l'exercice du droit à la vie privée ;
    - un défaut d'information individuel et préalable de la personne sur ses droits.
- **Élément moral**
  - Il est caractérisé par l'intention coupable.

**Pénalités**

| Infraction | Qualification | Prévue et réprimée | Peines |
|---|---|---|---|
| Traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé, sans information individuelle et préalable des personnes physiques sur leur droit d'accès, de rectification et d'opposition, la nature des informations transmises et les destinataires des données | Délit | CP, art. 226-19-1, al. 1 et 1° | Emprisonnement de cinq ans<br>Amende de 300 000 euros |

**Responsabilité des personnes morales**
Les personnes morales peuvent être déclarées pénalement responsables de ces infractions (CP, art. 226-24)

**9.5.8) Traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé malgré l'opposition de la personne concernée**

**Éléments constitutifs**

- **Élément légal**
  - Ce délit est prévu et réprimé par l'article 226-19-1, 2° du Code pénal.
- **Élément matériel**
  - Il faut :
    - procéder à un traitement de données à caractère personnel dans le cadre de la recherche dans le domaine de la santé concernant une personne physique. S'applique aussi aux fichiers non automatisés ou mécanographiques dont l'usage ne relève pas exclusivement de l'exercice du droit à la vie privée ;
    - une opposition de la personne concernée ou :
      - l'absence de consentement éclairé et exprès de la personne, lorsqu'il est prévu par la loi,
      - le refus exprimé de son vivant par la personne décédée.
- **Élément moral**
  - Il est caractérisé par l'intention coupable.

**Pénalités**

| Infraction | Qualification | Prévue et réprimée | Peines |
|---|---|---|---|
| Traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé, malgré l'opposition de la personne concernée ou en l'absence de consentement éclairé et exprès ou malgré le refus exprimé de son vivant par la personne décédée | Délit | CP,art. 226-19-1, 2° | Emprisonnement de cinq ans<br>Amende de 300 000 euros |

**Responsabilité des personnes morales**
Les personnes morales peuvent être condamnées à certaines peines prévues par l'article 131-39 du Code pénal (CP, art. 226-24).

## 9.6) Infractions aux règles fixées lors de la déclaration des traitements ou fichiers

### 9.6.1) Conservation de données à caractère personnel au-delà de la durée prévue par la demande d'avis ou la déclaration préalable à la mise en oeuvre du traitement informatisé

**Éléments constitutifs**

- **Élément légal**
  - Ce délit est prévu et réprimé par l'article 226-20, alinéa 1, du Code pénal.
- **Élément matériel**
  - Il faut :
    - conserver des données à caractère personnel sous une forme nominative, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions légales ;
    - conserver ces données au-delà de la durée prévue par la demande d'avis ou la déclaration préalable à la mise en oeuvre du traitement informatisé ;
    - hors les cas prévus par la loi.
- **Élément moral**
  - Il est caractérisé par l'intention coupable.

**Pénalités**

| Infraction | Qualification | Prévue et réprimée | Peines |
|---|---|---|---|
| Conservation de données à caractère personnel au-delà de la durée prévue par la demande d'avis ou la déclaration préalable | Délit | CP, art. 226-20, al. 1 | Emprisonnement de cinq ans<br>Amende de 300 000 euros |

**Le fait de ne pas détruire les enregistrements de vidéo protection dans le délai fixé par l'autorisation qui ne peut excéder un mois, hormis le cas d'une enquête judiciaire ou d'une information judiciaire, constitue un DÉLIT puni de trois ans d'emprisonnement et de 45 000 euros d'amende.**

**Responsabilité des personnes morales**
Les personnes morales peuvent être condamnées à certaines peines prévues par l'article 131-39 du Code pénal (CP, art. 226-24).

### 9.6.2) Traitement de données à caractère personnel conservées au-delà de la durée prévue par la demande d'avis ou la déclaration préalable à la mise en oeuvre du traitement informatisé, à des fins autres qu'historiques, statistiques ou scientifiques

**Éléments constitutifs**

- **Élément légal**
  - Ce délit est prévu et réprimé par l'article 226-20, alinéa 2, du Code pénal.
- **Élément matériel**
  - Il faut :
    - traiter des données à caractère personnel, à des fins autres qu'historiques, statistiques ou scientifiques, sauf si ce traitement a été autorisé par la loi ;
    - traiter ces données à caractère personnel conservées au-delà de la durée prévue par la demande d'avis ou la déclaration préalable à la mise en oeuvre du traitement

informatisé ;
- hors les cas prévus par la loi.

- **Élément moral**
  - Il est caractérisé par l'intention coupable.

**Pénalités**

| Infraction | Qualification | Prévue et réprimée | Peines |
|---|---|---|---|
| Traitement de données à caractère personnel au-delà de la durée prévue par la demande d'avis ou la déclaration préalable à la mise en oeuvre du traitement informatisé, à des fins autres qu'historiques, statistiques ou scientifiques | Délit | CP, art. 226-20, al. 2 | Emprisonnement de cinq ans<br>Amende de 300 000 euros |

**Responsabilité des personnes morales**
Les personnes morales peuvent être condamnées à certaines peines prévues par l'article 131-39 du Code pénal (CP, art. 226-24).

### 9.6.3) Détournement de la finalité de données à caractère personnel détenues à l'occasion de leur traitement

**Éléments constitutifs**
- **Élément légal**
  Ce délit est prévu et réprimé par l'article 226-21 du Code pénal.
- **Élément matériel**
  - Il faut :
    - détenir des données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement ;
    - détourner ces données de leur finalité. La finalité de ces informations est définie par :
      - la loi,
      - l'acte réglementaire autorisant le traitement automatisé,
      - la décision de la CNIL autorisant un traitement automatisé ayant pour fin la recherche dans le domaine de la santé,
      - les déclarations préalables à la mise en oeuvre du traitement automatisé.
- **Élément moral**
  - Il est caractérisé par l'intention coupable.

**Pénalités**

| Infraction | Qualification | Prévue et réprimée | Peines |
|---|---|---|---|
| Détournement de la finalité de données à caractère personnel détenues à l'occasion de leur traitement | Délit | CP, art. 226-21 | Emprisonnement de cinq ans<br>Amende de 300 000 euros |

**Les enregistrements visuels de vidéoprotection sont considérés comme des informations nominatives, lorsqu'ils sont utilisés pour la constitution d'un fichier nominatif (CSI, art. L. 251-1 et L. 254-1). L'utilisation des images à d'autres fins que celles pour lesquelles elles sont autorisées constitue un délit puni de trois ans d'emprisonnement et de 45 000 euros d'amende.**

**Responsabilité des personnes morales**
Les personnes morales peuvent être condamnées à certaines peines prévues par l'article 131-39 du Code pénal (CP, art. 226-24).

### 9.6.4) Divulgation à un tiers n'ayant pas qualité pour les recevoir, de données à caractère personnel recueillies à l'occasion d'un traitement, sans autorisation de l'intéressé, avec effet de porter atteinte à sa personnalité

**Éléments constitutifs**

- **Élément légal**
  - Ce délit est prévu et réprimé par l'article 226-22, al. 1 et 2 du Code pénal.
- **Élément matériel**
  - Il faut :
    - avoir recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des informations nominatives ;
    - porter ces informations nominatives à la connaissance d'un tiers qui n'a pas qualité pour les recevoir ;
    - ne pas avoir l'autorisation de l'intéressé ;
    - agir par imprudence ou négligence ;
    - que la divulgation de ces informations soit de nature à porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, peu importe donc le résultat ou la motivation.
- **Élément moral**
  - Il est caractérisé par l'intention coupable.
  - Dans le cas de l'imprudence ou de la négligence, la peine sera moins élevée.
  - La poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit (CP, art. 226-22, al. 3).

**Pénalités**

| Infractions | Qualification | Prévues et réprimées | Peines |
|---|---|---|---|
| Divulgation faite sciemment à un tiers n'ayant pas la qualité pour les recevoir, de données à caractère personnel recueillies à l'occasion de leur traitement, sans autorisation de l'intéressé, avec effet de lui nuire | Délit | CP, art. 226-22, al. 1 | Emprisonnement de cinq ans<br>Amende de 300 000 euros |
| Divulgation, par imprudence ou négligence, de données à caractère personnel recueillies à l'occasion de leur traitement, avec effet de lui nuire | | CP, art. 226-22, al. 1 et 2 | Emprisonnement de trois ans<br>Amende de 100 000 euros |

**Responsabilité des personnes morales**
Les personnes morales peuvent être condamnées à certaines peines prévues par l'article 131-39 du Code pénal (CP, art. 226-24).

### 9.6.5) Transfert de données à caractère personnel

**Éléments constitutifs**

- **Élément légal**
  - Ce délit est prévu et réprimé par l'article 226-22-1 du Code pénal.
- **Élément matériel**
  - Il faut :
    - procéder ou faire procéder à un transfert de données à caractère personnel,
    - faisant l'objet ou destinées à faire l'objet d"un traitement vers un État n'appartenant pas à l'UE ou à une organisation internationale ( *Loi n° 78-17 du 6 janvier 1978, art. 112 à 114).*
- **Élément moral**
  - Il est caractérisé par l'intention coupable.

**Pénalités**

| Infraction | Qualification | Prévue et réprimée | Peines |
|---|---|---|---|
| Transfert de données à caractère personnel | Délit | CP, art. 226-22-1 | Emprisonnement de cinq ans<br>Amende de 300 000 euros |

**Responsabilité des personnes morales**
Les personnes morales peuvent être condamnées à certaines peines prévues par l'article 131-39 du Code pénal (CP, art. 226-24).

### 9.6.6) Entrave à l'action de la CNIL

**Éléments constitutifs**

- **Élément légal**
  - Ce délit est prévu et réprimé par l'article 226-22-2 du Code pénal.
- **Élément matériel**
  - le fait d'entraver soit :
    - en s'opposant à l'exercice des missions confiées à ses membres ou aux agents habilités *(Loi n° 78-17 du 6 janvier 1978, art. 10*) lorsque la visite à été autorisée par le juge ;
      en refusant de communiquer à ses membres ou agents habilités les renseignements et documents utiles à leur missions, ou en dissimulant les dits documents ou renseignements ou en les faisant disparaître ;
    - soit en communiquant des informations qui ne sont pas conformes.
- **Élément moral**
  - Il est caractérisé par l'intention coupable.

**Pénalités**

| Infraction | Qualification | Prévue et réprimée | Peines |
|---|---|---|---|
| Entrave à l'action de la CNIL | Délit | CP, art. 226-22-2 | Emprisonnement d'un an<br>Amende de 15 000 euros |

**Responsabilité des personnes morales**
Les personnes morales peuvent être condamnées à certaines peines prévues par l'article 131-39 du Code pénal (CP, art. 226-24).

### 9.6.7) Constitution et utilisation de fichiers médicaux commerciaux avec identification directe ou indirecte du professionnel prescripteur

**Éléments constitutifs**

- **Élément légal**
  - Ce délit est prévu et réprimé par les articles L. 4113-7 et L. 4163-9 du Code de la santé publique.
- **Élément matériel**
  - Il faut :
    - constituer et utiliser des fichiers constitués à partir de données issues directement ou non de prescriptions ou d'informations médicales mentionnées au Code de la santé publique ;
    - se servir de ces fichiers à des fins de prospection ou de promotion commerciale ;
    - pouvoir identifier, grâce à eux, le professionnel prescripteur (directement ou indirectement).
- **Élément moral**
  - Il est caractérisé par l'intention coupable.
  - L'auteur ou l'utilisateur du fichier n'ignore pas, en agissant ainsi, qu'il enfreint la loi.

**Pénalités**

| Infraction | Qualification | Prévue et réprimée | Peines |
|---|---|---|---|
| Constitution et utilisation, à des fins de prospection et de promotion commerciale, de fichiers composés à partir de données médicales ou d'informations médicales mentionnées au Code de la sécurité sociale et permettant d'identifier directement ou indirectement le professionnel prescripteur | Délit | CSP, art. L. 4113-7 et L. 4163-9 | Emprisonnement de deux ans<br>Amende de 75 000 euros |

## 9.7) Autres infractions

### 9.7.1) Contrefaçon, par édition ou reproduction d'oeuvre de l'esprit, au mépris des lois et règlements relatifs à la propriété des auteurs

**Éléments constitutifs**

- **Élément légal**
  - Ce délit est prévu et réprimé par les articles L. 335-2, alinéas 1 et 2, et L. 335-3, alinéas 1 et 2, du Code de la propriété intellectuelle.
- **Élément matériel**
  - Il faut :
    - l'existence d'écrits, de compositions musicales, de dessins, de peintures, ou de toute autre production imprimée ou gravée ;
    - qu'au mépris des lois et règlements relatifs à la propriété des auteurs, l'oeuvre soit éditée, reproduite, représentée ou diffusée, totalement ou partiellement, par quelque moyen que ce soit par l'auteur.
- **Élément moral**
  - Il est caractérisé par l'intention coupable. Elle est souvent constituée par le défi, l'appât du gain, voire la revente des copies par l'auteur du forfait.

**Cette infraction s'applique à la captation d'une oeuvre cinématographique ou audiovisuelle en salle de spectacle cinématographique (CPI, art. L. 335-3, al. 3).**

**Pénalités**

| Infraction | Qualification | Prévue et réprimée | Peines |
|---|---|---|---|
| Contrefaçon d'une oeuvre de l'esprit | Délit | Code de la propriété intellectuelle, art. L. 335-2, al. 1 et 2, et art. L. 335-3, al. 1 et 2 | Emprisonnement de trois ans<br>Amende de 300 000 euros |

**Circonstance aggravante**

Les délits visés à l'article L. 335-2 al. 1, 2 et 3 du Code de la propriété intellectuelle sont aggravés lorsqu'ils sont commis en bande organisée.

### 9.7.2) Édition, mise à disposition, ou communication au public d'un logiciel manifestement destiné à la mise à disposition du public d'oeuvres ou objets protégés

**Éléments constitutifs**

- **Élément légal**
  - Ce délit est prévu et réprimé par les articles L. 335-2-1, al. 1 et 1° du Code de la propriété intellectuelle.
- **Élément matériel**
  - Il faut :
    - l'existence d'oeuvre de l'esprit ou d'objets protégés ;
    - qu'un logiciel manifestement destiné à la mise à disposition du public non autorisé, d'oeuvres ou d'objets protégés, soit édité, mis à la disposition ou communiqué au public, sciemment et sous quelque forme que ce soit.

- **Élément moral**
  - Il est caractérisé par l'intention coupable.

**Pénalités**

| Infractions | Qualifications | Prévues et réprimées | Peines |
|---|---|---|---|
| Édition, mise à disposition ou communication au public d'un logiciel manifestement destiné à la mise à disposition du public non autorisée d'oeuvres ou d'objets protégés | Délit | Code de la propriété intellectuelle, art. L. 335-2-1, al. 1 et 1° | Emprisonnement de trois ans<br>Amende de 300 000 euros |

**L'incitation à l'usage d'un logiciel prévu à l'article L. 335-2-1, 1°, du Code de la propriété intellectuelle, y compris à travers une annonce publicitaire est puni de la même peine.**

**9.7.3) Négligence caractérisée après recommandations adressées par l'Autorité de régulation de la communication audiovisuelle et numérique**

Négligence caractérisée par au minimum deux constatations de l'utilisation d'un compte internet à des fins de reproduction, de représentation ou de mise à disposition ou de communication au public d'oeuvres ou d'objets ayant fait l'objet de recommandations par l'Autorité de régulation de la communication audiovisuelle et numérique.

**Éléments constitutifs**

- **Élément légal**
  - Cette contravention pénale de 5e classe est prévue et réprimée par l'article R. 335-5 du Code de la propriété intellectuelle.
- **Élément matériel**
  - Il faut :
    - la constatation d'un téléchargement illicite par l'Autorité de régulation de la communication audiovisuelle et numérique ;
    - une recommandation, adressée par la cette autorité au titulaire de l'accès au service de communication au public en ligne, de mettre en oeuvre un moyen de sécurisation de son accès interdisant tout renouvellement de cette faute ;
    - une absence ou insuffisance des moyens de sécurisation mis en oeuvre ;
    - la constatation d'un nouveau téléchargement illicite dans l'année suivant la première constatation .
- **Élément moral**
  - Il est caractérisé par l'intention coupable.

**Pénalités**

| Infraction | Qualification | Prévue et réprimée | Peines |
|---|---|---|---|
| Négligence caractérisée après recommandations adressées par l'Autorité de régulation de la communication audiovisuelle et numérique | Contravention de 5e classe | Code de la propriété intellectuelle, art. R. 335-5 | Amende de 1 500 euros<br>CP, art. 131-13 |

### 9.7.4) Contraventions de police en cas de violation de certaines dispositions de la loi n° 78-17 du 6 janvier 1978

**Pénalités**

| Infractions | Qualifications | Prévues et réprimées | Peines |
|---|---|---|---|
| Recueil d'informations nominatives sans informer la personne de l'identité du responsable du traitement, de sa finalité ;<br>du caractère obligatoire ou facultatif de la réponse ;<br>des conséquences d'un défaut de réponse ;<br>des destinataires des informations ;<br>de ses droits d'opposition, d'interrogation, d'accès et de rectification | Contravention de 5e classe | CP, art. R.625-10 | Amende de 1 500 euros<br>CP, art. 131-13 |
| Opposition à l'exercice du droit d'accès par le titulaire du fichier | | CP, art. R. 625-11 | |
| Opposition à l'exercice du droit de rectification | | CP, art. R.625-12 | |