CHARTE DE BON USAGE DU SYSTEME D'INFORMATION DE L'AP-HP

Annexe 1 : Les principaux textes législatifs et réglementaires

Mai 2015

La présente annexe de la charte informatique reprend les principaux textes législatifs et réglementaires concourant au droit applicable à l'utilisation du système d'information de l'AP-HP.

LE RESPECT DE LA CONFIDENTIALITE DES DONNEES DE SANTE

Le respect de la vie privée comprend toutes les dimensions du respect de l'intimité de la personne et de sa volonté. En ce qui concerne les informations, il ne se résume pas à la confidentialité. Il prend de nombreuses formes :

- le droit de détenir des droits sur ses informations personnelles (donc de limiter les droits de ceux qui en ont connaissance)
- le droit au secret des informations personnelles donc le droit de s'opposer aux traitements ou aux échanges de celles-ci
- les droits dérivant des lois informatique et libertés : droit à l'information préalable, droit d'accès et de rectification, droit d'opposition, droit à l'oubli

Le secret professionnel est régi par le code pénal art 226-13 par les codes de déontologie à valeur réglementaire et par le code de santé publique (art R 1112-7 et L1110-4).

Article 226-13 du Code pénal

« La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 € d'amende. »

Code de déontologie médicale « Article R 4127-4 du CSP

« Le secret professionnel institué dans l'intérêt des patients s'impose à tout médecin dans les conditions établies par la loi.
Le secret couvre tout ce qui est venu à la connaissance du médecin dans l'exercice de sa profession, c'est-à-dire non seulement ce qui lui a été confié, mais aussi ce qu'il a vu, entendu ou compris. »

Au-delà, la loi du 4 mars 2002 renforce, complète et précise le contenu du secret professionnel. Elle étend cette obligation à tous les professionnels de santé et plus généralement à tous les professionnels intervenant dans le système de santé.
Elle prévoit également des sanctions pour ceux qui tentent d'obtenir des informations en violation du secret professionnel.

Afin de garantir la confidentialité des informations médicales mentionnées aux alinéas précédents, leur conservation sur support informatique, comme leur transmission par voie électronique entre professionnels, sont soumises à des règles définies par décret en Conseil d'Etat pris après avis public et motivé de la Commission nationale de l'informatique et des libertés.
La carte de professionnel de santé et les dispositifs équivalents agréés sont utilisés par les professionnels de santé, les établissements de santé, les réseaux de santé ou tout autre organisme participant à la prévention et aux soins.
Le fait d'obtenir ou de tenter d'obtenir la communication de ces informations en violation du présent article est puni d'un an d'emprisonnement et de 15 000 euros d'amende.
En cas de diagnostic ou de pronostic grave, le secret médical ne s'oppose pas à ce que la famille, les proches de la personne malade ou la personne de confiance définie à l'article L. 1111-6 reçoivent les informations nécessaires destinées à leur permettre d'apporter un soutien direct à celle-ci, sauf opposition de sa part. Seul un médecin est habilité à délivrer, ou à faire délivrer sous sa responsabilité, ces informations.
Le secret médical ne fait pas obstacle à ce que les informations concernant une personne décédée soient délivrées à ses ayants droit, dans la mesure où elles leur sont nécessaires pour leur permettre de connaître les causes de la mort, de défendre la mémoire du défunt ou de faire valoir leurs droits, sauf volonté contraire exprimée par la personne avant son décès.

Article R. 1112-7 du CSP

Les informations concernant la santé des patients sont soit conservées au sein des établissements de santé qui les ont constituées, soit déposées par ces établissements auprès d'un hébergeur agréé en application des dispositions à l'article L. 1111-8.
Le directeur de l'établissement veille à ce que toutes dispositions soient prises pour assurer la garde et la confidentialité des informations ainsi conservées ou hébergées.

Article L1110-4 du CSP

« Toute personne prise en charge par un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et du secret des informations la concernant.

Excepté dans les cas de dérogation, expressément prévus par la loi, ce secret couvre l'ensemble des informations concernant la personne venues à la connaissance du professionnel de santé, de tout membre du personnel de ces établissements ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. Il s'impose à tout professionnel de santé, ainsi qu'à tous les professionnels intervenant dans le système de santé.

Deux ou plusieurs professionnels de santé peuvent toutefois, sauf opposition de la personne dûment avertie, échanger des informations relatives à une même personne prise en charge, afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge sanitaire possible. Lorsque la personne est prise en charge par une équipe de soins dans un établissement de santé, les informations la concernant sont réputées confiées par le malade à l'ensemble de l'équipe.

Les informations concernant une personne prise en charge par un professionnel de santé au sein d'une maison ou d'un centre de santé sont réputées confiées par la personne aux autres professionnels de santé de la structure qui la prennent en charge, sous réserve :

1. Du recueil de son consentement exprès, par tout moyen, y compris sous forme dématérialisée. Ce consentement est valable tant qu'il n'a pas été retiré selon les mêmes formes ;
2. De l'adhésion des professionnels concernés au projet de santé mentionné aux articles L. 6323-1 et L. 6323-3.

La personne, dûment informée, peut refuser à tout moment que soient communiquées des informations la concernant à un ou plusieurs professionnels de santé.

Afin de garantir la confidentialité des informations médicales mentionnées aux alinéas précédents, leur conservation sur support informatique, comme leur transmission par voie électronique entre professionnels, sont soumises à des règles définies par décret en Conseil d'Etat pris après avis public et motivé de la Commission nationale de l'informatique et des libertés. Ce décret détermine les cas où l'utilisation de la carte de professionnel de santé mentionnée au dernier alinéa de l'article L. 161-33 du code de la sécurité sociale ou un dispositif équivalent agréé par l'organisme chargé d'émettre la carte de professionnel de santé est obligatoire. La carte de professionnel de santé et les dispositifs équivalents agréés sont utilisés par les professionnels de santé, les établissements de santé, les réseaux de santé ou tout autre organisme participant à la prévention et aux soins.

Le fait d'obtenir ou de tenter d'obtenir la communication de ces informations en violation du présent article est puni d'un an d'emprisonnement et de 15 000 euros d'amende.

En cas de diagnostic ou de pronostic grave, le secret médical ne s'oppose pas à ce que la famille, les proches de la personne malade ou la personne de confiance définie à l'article L. 1111-6 reçoivent les informations nécessaires destinées à leur permettre d'apporter un soutien direct à celle-ci, sauf opposition de sa part. Seul un médecin est habilité à délivrer, ou à faire délivrer sous sa responsabilité, ces informations.

Le secret médical ne fait pas obstacle à ce que les informations concernant une personne décédée soient délivrées à ses ayants droit, dans la mesure où elles leur sont nécessaires pour leur permettre de connaître les causes de la mort, de défendre la mémoire du défunt ou de faire valoir leurs droits, sauf volonté contraire exprimée par la personne avant son décès. »

Article 57 de la Loi informatique et libertés »

Les personnes auprès desquelles sont recueillies des données à caractère personnel ou à propos desquelles de telles données sont transmises sont, avant le début du traitement de ces données, individuellement informées :

1. De la nature des informations transmises ;
2. De la finalité du traitement de données ;
3. Des personnes physiques ou morales destinataires des données ;
4. Du droit d'accès et de rectification institué aux articles 39 (droit d'accès) et 40 (droit de rectification) ;
5. Du droit d'opposition institué aux premier (opposition à la levée du secret professionnel) et troisième (refus de traitement après décès) alinéas de l'article 56 ou, dans le cas prévu au deuxième alinéa de cet article, de l'obligation de recueillir leur consentement. »

Ce droit à l'information et au respect de la volonté ne s'oppose pas au droit à la protection vis-à-vis de cette même information. Il impose aux professionnels une réflexion et une appréciation en conscience pour rester en empathie des demandes du patient.

Décret confidentialité du 15 mai 2007 (R1110-1 du CSP)

« Confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique

« Art. R. 1110-1. − La conservation sur support informatique des informations médicales mentionnées aux trois premiers alinéas de l'article L. 1110-4 par tout professionnel, tout établissements et tout réseau de santé ou tout autre organisme intervenant dans le système de santé est soumise au respect de référentiels définis par arrêtés du ministre chargé de la santé, pris après avis de la Commission nationale de l'informatique et des libertés. Ces référentiels s'imposent également à la transmission de ces informations par voie électronique entre professionnels.
« Les référentiels déterminent les fonctions de sécurité nécessaires à la conservation ou à la transmission des informations médicales en cause et fixant le niveau de sécurité requis pour ces fonctions.
« Ils décrivent notamment :

1. « Les mesures de sécurisation physique des matériels et des locaux ainsi que les dispositions prises pour la sauvegarde des fichiers ;
2. « Les modalités d'accès aux traitements, dont les mesures d'identification et de vérification de la qualité des utilisateurs, et de recours à des dispositifs d'accès sécurisés ;
3. « Les dispositifs de contrôle des identifications et habilitations et les procédures de traçabilité des accès aux informations médicales, ainsi que l'histoire des connexions ;
4. « En cas de transmission par voie électronique entre professionnels, les mesures mises en œuvre pour garantir la confidentialité des informations échangées, le cas échéant, par le recours à un chiffrement en tout ou partie de ces informations.

« Art. R. 1110-2. − Pour chaque traitement mis en œuvre par les personnes et les organismes mentionnés à l'article R. 1110-1 et comportant des informations médicales à caractère personnel, le dossier de déclaration ou de demande d'autorisation auprès de la Commission nationale de l'informatique et des libertés décrit les moyens retenus afin d'assurer la mise en conformité de ce traitement avec le référentiel le concernant.
« Le responsable du traitement, au sens de l'article 3 de la loi no 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, est chargé de veiller au respect du référentiel. Il lui appartient notamment de :

1. « Gérer la liste nominative des professionnels habilités à accéder aux informations médicales relevant de ce traitement et la tenir à la disposition des personnes concernées par ces informations ;
2. « 2o Mettre en œuvre les procédés assurant l'identification et la vérification de la qualité des professionnels de santé dans les conditions garantissant la cohérence entre les données d'identification gérées localement et celles recensées par le groupement d'intérêt public mentionné à l'article R. 161-54 du code de la sécurité sociale ;
3. « Porter à la connaissance de toute personne concernée par les informations médicales relevant du traitement les principales dispositions prises pour garantir la conformité au référentiel correspondant.

« Art. R. 1110-3. − En cas d'accès par des professionnels de santé aux informations médicales à caractère personnel conservées sur support informatique ou de leur transmission par voie électronique, l'utilisation de la carte de professionnel de santé mentionnée au dernier alinéa de l'article L. 161-33 du code de la sécurité sociale est obligatoire. »

L'ACCES AUX INFORMATIONS MEDICALES POUR LES PATIENTS

« Article L1110-4 – CSP

En cas de diagnostic ou de pronostic grave, le secret médical ne s'oppose pas à ce que la famille, les proches de la personne malade ou la personne de confiance définie à l'article L. 1111-6 reçoivent les informations nécessaires destinées à leur permettre d'apporter un soutien direct à celle-ci, sauf opposition de sa part. Seul un médecin est habilité à délivrer, ou à faire délivrer sous sa responsabilité, ces informations
Le secret médical ne fait pas obstacle à ce que les informations concernant une personne décédée soient délivrées à ses ayants droit, dans la mesure où elles leur sont nécessaires pour leur permettre de connaître les causes de la mort, de défendre la mémoire du défunt ou de faire valoir leurs droits, sauf volonté contraire exprimée par la personne avant son décès. »

« Art 57- Loi informatique et libertés

Toutefois, ces informations peuvent ne pas être délivrées si, pour des raisons légitimes que le médecin traitant apprécie en conscience, le malade est laissé dans l'ignorance d'un diagnostic ou d'un pronostic grave. »

LE RESPECT DE LA DIGNITE ET DES BONNES MŒURS

Article 227-24 du Code Pénal

« Le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine, soit de faire commerce d'un tel message, est puni de trois ans d'emprisonnement et de 75 000 euros d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur.
Lorsque les infractions prévues au présent article sont soumises par la voie de la presse écrite ou audiovisuelle, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables ».

Article 227-23 du Code Pénal

« Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.
Le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines.
Les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de télécommunications.
La tentative des délits prévus aux alinéas précédents est punie des mêmes peines.
Le fait de détenir une telle image ou représentation est puni de deux ans d'emprisonnement et 30 000 euros d'amende.
Les infractions prévues au présent article sont punies de dix ans d'emprisonnement et de 500 000 Euros d'amende lorsqu'elles sont commises en bande organisée.
Les dispositions du présent article sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette personne était âgée de dix-huit ans au jour de la fixation ou de l'enregistrement de son image ».

LA PROTECTION DES LIBERTES INDIVIDUELLES

Article 9 du Code civil

« Chacun a droit au respect de sa vie privée.
Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé. »

Article 226-16 du Code Pénal

« Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.
Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2º du I de l'article 45 de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ».

Article 226-16-1 A du Code Pénal

Lorsqu'il a été procédé ou fait procéder à un traitement de données à caractère personnel dans les conditions prévues par le I ou le II de l'article 24 de la loi n° 78-17 du 6 janvier 1978 précitée, le fait de ne pas respecter, y compris par négligence, les normes simplifiées ou d'exonération établies à cet effet par la Commission nationale de l'informatique et des libertés est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Article 226-16-1 du Code Pénal

Le fait, hors les cas où le traitement a été autorisé dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 précitée, de procéder ou faire procéder à un traitement de données à caractère personnel incluant parmi les données sur lesquelles il porte le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Article 226-17 du Code Pénal

« Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi nº 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende ».

Article 226-18 du Code Pénal

« Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende ».

Article 226-19 du Code Pénal

« Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende .
Est puni des mêmes peines le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté ».

Article 226-19-1 du Code Pénal

« En cas de traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende le fait de procéder à un traitement :

1. Sans avoir préalablement informé individuellement les personnes sur le compte desquelles des données à caractère personnel sont recueillies ou transmises de leur droit d'accès, de rectification et d'opposition, de la nature des données transmises et des destinataires de celles-ci ;
2. Malgré l'opposition de la personne concernée ou, lorsqu'il est prévu par la loi, en l'absence du consentement éclairé et exprès de la personne, ou s'il s'agit d'une personne décédée, malgré le refus exprimé par celle-ci de son vivant. »

Article 226-20 du Code Pénal

« Le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi.
Est puni des mêmes peines le fait, hors les cas prévus par la loi, de traiter à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa ».

Article 226-21 du Code Pénal

« Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende ».

Article 226-22 du Code Pénal

« Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.
La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 Euros d'amende lorsqu'elle a été commise par imprudence ou négligence.
Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit ».

Article 226-23 du Code Pénal

« Les dispositions de l'article 226-19 sont applicables aux traitements non automatisés de données à caractère personnel dont la mise en oeuvre ne se limite pas à l'exercice d'activités exclusivement personnelles ».

LE RESPECT DU DROIT DE LA PROPRIETE INTELLECTUELLE

Article L122-6 du Code de la Propriété Intellectuelle

« Sous réserve des dispositions de l'article L. 122-6-1, le droit d'exploitation appartenant à l'auteur d'un logiciel comprend le droit d'effectuer et d'autoriser :

1. La reproduction permanente ou provisoire d'un logiciel en tout ou partie par tout moyen et sous toute forme. Dans la mesure où le chargement, l'affichage, l'exécution, la transmission ou le stockage de ce logiciel nécessitent une reproduction, ces actes ne sont possibles qu'avec l'autorisation de l'auteur ;
2. La traduction, l'adaptation, l'arrangement ou toute autre modification d'un logiciel et la reproduction du logiciel en résultant ;
3. La mise sur le marché à titre onéreux ou gratuit, y compris la location, du ou des exemplaires d'un logiciel par tout procédé. Toutefois, la première vente d'un exemplaire d'un logiciel dans le territoire d'un Etat membre de la Communauté européenne ou d'un Etat partie à l'accord sur l'Espace économique européen par l'auteur ou avec son consentement épuise le droit de mise sur le marché de cet exemplaire dans tous les Etats membres à l'exception du droit d'autoriser la location ultérieure d'un exemplaire ».

Article L335-3 du Code de la Propriété Intellectuelle

« Est également un délit de contrefaçon toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur, tels qu'ils sont définis et réglementés par la loi.
Est également un délit de contrefaçon la violation de l'un des droits de l'auteur d'un logiciel définis à l'article L. 122-6 ».

Article L335-2 du Code de la Propriété Intellectuelle

« Toute édition d'écrits, de composition musicale, de dessin, de peinture ou de toute autre production, imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon ; et toute contrefaçon est un délit.
La contrefaçon en France d'ouvrages publiés en France ou à l'étranger est punie de trois ans d'emprisonnement et de 300 000 euros d'amende.
Seront punis des mêmes peines le débit, l'exportation et l'importation des ouvrages contrefaits.
Lorsque les délits prévus par le présent article ont été commis en bande organisée, les peines sont portées à cinq ans d'emprisonnement et à 500 000 euros d'amende».

LE RESPECT DE L'INTEGRITE D'UN SYSTEME INFORMATIQUE

Article 323-1 du Code Pénal

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.
Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende ».

Article 323-2 du Code Pénal

« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende ».

Article 323-3 du Code Pénal

« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende ».

Article 323-5 du Code Pénal

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

1. L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;
2. L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;
3. La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;
4. La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

5. L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;
6. L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;
7. L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35 ».

LE RESPECT DU SECRET DE LA CORRESPONDANCE ECHANGEE PAR LE CANAL INFORMATIQUE

Article 226-4-1 du Code Pénal

« Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende.
Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne. »

Article 226-15 du Code Pénal

« Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45 000 euros d'amende.
Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions ».

Article 432-9 du Code Pénal

« Le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, le détournement, la suppression ou l'ouverture de correspondances ou la révélation du contenu de ces correspondances, est puni de trois ans d'emprisonnement et de 45 000 euros d'amende.
Est puni des mêmes peines le fait, par une personne visée à l'alinéa précédent ou un agent d'un exploitant de réseaux ouverts au public de communications électroniques ou d'un fournisseur de services de télécommunications, agissant dans l'exercice de ses fonctions, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des télécommunications, l'utilisation ou la divulgation de leur contenu ».

LE DEPOT LEGAL DES LOGICIELS ET DES BASES DE DONNEES

Article L 131-2 du Code du Patrimoine

« Les documents imprimés, graphiques, photographiques, sonores, audiovisuels, multimédias, quel que soit leur procédé technique de production, d'édition ou de diffusion, font l'objet d'un dépôt obligatoire, dénommé dépôt légal, dès lors qu'ils sont mis à la disposition d'un public.
Les logiciels et les bases de données sont soumis à l'obligation de dépôt légal dès lors qu'ils sont mis à disposition d'un public par la diffusion d'un support matériel, quelle que soit la nature de ce support.
Sont également soumis au dépôt légal les signes, signaux, écrits, images, sons ou messages de toute nature faisant l'objet d'une communication au public par voie électronique, sont soumis à l'obligation de dépôt légal dès lors qu'ils sont mis à disposition d'un public par la diffusion d'un support matériel, quelle que soit la nature de ce support.
Sont également soumis au dépôt légal les signes, signaux, écrits, images, sons ou messages de toute nature faisant l'objet d'une communication au public par voie électronique ».

Article L 133-1 du Code du Patrimoine

« Le fait, pour toute personne mentionnée à l'article L. 132-2, de se soustraire volontairement à l'obligation de dépôt légal est puni d'une amende de 75 000 Euros. La juridiction répressive peut, après avoir déclaré le prévenu coupable, ajourner le prononcé de la peine en lui enjoignant, sous astreinte le cas échéant, de se conformer, dans un délai fixé, aux prescriptions qu'elle détermine et qui ont pour objet de faire cesser l'agissement illicite et d'en réparer les conséquences.
Dans le cas où la juridiction répressive assortit l'ajournement d'une astreinte, elle doit prévoir le taux et la date à compter de laquelle cette astreinte commencera à courir. L'ajournement, qui ne peut intervenir qu'une seule fois, peut être décidé même si le prévenu ne comparaît pas en personne.

Le juge peut ordonner l'exécution provisoire de la décision d'injonction.
A l'audience de renvoi, qui doit intervenir au plus tard dans le délai d'un an à compter de la décision d'ajournement, la juridiction statue sur la peine et liquide l'astreinte s'il y a lieu. Elle peut, le cas échéant, supprimer cette dernière ou en réduire le montant. L'astreinte est recouvrée par le comptable du Trésor comme une amende pénale. Elle ne peut donner lieu à contrainte judiciaire ».