TELECOM PARISTECH

COURS

SECURITE DES SYSTEMES D'INFORMATION

07 04 2015

Alain Bensoussan Avocats
Le droit du numérique et des technologies avancées

Sommaire analytique

1.Introduction

1. Les systèmes d'information peuvent être définis comme l'ensemble d'éléments en interaction et formant un tout organisé et cohérent, mis en œuvre pour gérer, stocker et permettre l'accès à l'information et définis tant au niveau des politiques que des procédures et des ressources matérielles et humaines

2. La sécurité des systèmes d'information (SSI) recouvre l'ensemble des moyens techniques, organisationnels et humains qui doivent être mis en place dans le but de garantir, au juste niveau requis, la sécurité des informations d'un organisme et des systèmes qui en assurent l'élaboration, le traitement, la transmission ou le stockage.

3.La sécurité des systèmes d'information (SSI) est destinée à assurer la satisfaction des besoins de sécurité relatifs à un système d'information.

4.L'article L111-1 alinéa 1 du Code de la sécurité intérieure dispose :

- « La sécurité est un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives ».

5.La sécurité est ainsi devenue un droit fondamental.

6.Cet article symbolise à lui seul toute l'importance que revêt aujourd'hui la sécurité en général et la sécurité des systèmes d'information en particulier.

7.Le droit de la sécurité des systèmes d'information a connu un développement exceptionnel.

8.En l'espace de moins de 15 ans, le droit de la sécurité des systèmes d'information est devenu un droit autonome, d'une très grande complexité et pour lequel il existe de nombreux risques juridiques pour les acteurs qui n'en maîtriseraient pas tous les aspects.

9.Il faut en effet rappeler que jusqu'en 2001 la sécurité des systèmes d'information était essentiellement abordée à travers les dispositions du Code pénal relatives à ce qu'on appelle l'infraction informatique.

10.Il s'agit en réalité des articles 323-1, 323-2, 323-3 du Code pénal qui visent les cas d'intrusion, d'accès frauduleux, d'altération des systèmes ou des données qu'ils comportent…

11.Le développement de l'usage des systèmes d'information dans l'entreprise, de l'économie numérique mais aussi de la cybercriminalité a conduit la France et d'une manière générale l'ensemble des pays à l'échelle mondiale à élaborer un nouveau corpus de règles dédiées à la « sécurité ».

12.La France a adopté de nombreux textes génériques ou spécifiques comme :

- la loi relative à la sécurité quotidienne du 15 novembre 2001 ;
- la loi pour la sécurité intérieure du 18 mars 2003 ;
- la loi sur la sécurité financière du 1er août 2003 ;
- la loi portant adaptation de la justice aux évolutions de la criminalité du 9 mars 2004 ;
- la loi pour la confiance dans l'économie numérique (partie cybercriminalité) du 21 juin 2004 ;

- la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés du 6 août 2004 ;

- la loi relative à la lutte contre le terrorisme du 23 janvier 2006 ;

- la loi d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011 ;

- la loi relative à la programmation militaire pour les années 2014 à 2019 du 18 décembre 2013.

13.Au plan sectoriel, il existe d'autres textes et obligations réglementaires comme dans le secteur bancaire, le secteur de l'assurance, celui de la santé ou encore celui des services ou infrastructure vitale.

14.D'autres lois touchent la sécurité des systèmes d'information du fait des incidences qu'elles font porter sur les entreprises et notamment la loi dite Hadopi (lutte contre le téléchargement illégal) du 12 juin 2009.

15.En matière de normes et de « best practices » il faut également tenir compte de :

- la norme ISO 270001 et suivantes ;

- les « meilleures pratiques » diffusées par les autorités compétentes comme l'ANSSI, l'Enisa[1] ou la Cnil (Guide relatif à la Sécurité des données personnelles).

16.Il existe également un corps de règles européen et international. On notera en particulier la décision cadre du 24 février 2005 relative aux attaques visant les systèmes d'information et plus récemment la directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information[2].

17.Au niveau international on notera l'adoption le 23 novembre 2001 de la convention de Budapest sur la cybercriminalité.

18.Il faut ajouter à cela un développement exponentiel de la jurisprudence aussi bien dans le domaine de la cybercriminalité que dans celui de la cybersurveillance des salariés.

19.Cette jurisprudence oblige les entreprises à revisiter leurs politiques des systèmes d'information et certains documents d'accompagnement tels que les chartes d'usage à destination des salariés.

20.Ce secteur juridico-technique est en pleine évolution avec l'adoption de la LOPPSI 2 ou encore l'ordonnance du 24 août 2011 modifiant notamment la loi informatique et libertés en prévoyant la notification des failles de sécurité à la Cnil et à l'intéressé pour les fournisseurs de services de communications électroniques au public en ligne. Cette obligation de notification des failles de sécurité a été généralisée à l'ensemble de l'Union européenne par le règlement n° 611/2013 de la Commission européenne du 24 juin 2013[3].

1
file:///C:/Documents%20and%20Settings/AIC/Mes%20documents/Downloads/ThreatLandscapeandPracticeGuide%20-%20French.pdf

2 Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.

3 Règlement n° 611/2013 de la Commission concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques.

2. Le socle de base

2.1 Les atteintes aux systèmes de traitement automatisé de données

21. La loi ne réprime pas de la même manière les accès frauduleux ayant eu une incidence sur les systèmes et les accès frauduleux n'ayant eu qu'une incidence "quelconque" sur l'état desdits systèmes.

2.1.1L'accès frauduleux "sans influence"

22. L'infraction relative à l'accès frauduleux "sans influence" fait l'objet d'une codification à l'article 323-1, alinéa 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".

23. Selon cet article, l'accès est considéré comme susceptible d'une infraction dès lors qu'il est opéré de manière frauduleuse. La question de la preuve renvoie à la théorie générale en matière de délit. Le terme "frauduleux" implique à la fois le caractère volontaire de l'intrusion et la conscience de l'absence de droit.

24. En outre, la preuve de l'infraction est uniquement fondée sur celle de l'action d'accès. Cette notion d'accès s'entend de tout système de pénétration tels que :

- la connexion pirate, tant physique que logique ;
- l'appel d'un programme alors qu'on ne dispose pas de l'habilitation ;
- l'interrogation d'un fichier sans autorisation.

25. Ainsi, le fait même d'être sans lien avec la société à laquelle le système informatique appartient, suffit à caractériser l'accès frauduleux sans droit, ni titre. En revanche, ne sont pas considérées comme constitutives d'une infraction ou d'une prise de connaissance d'information :

- la télédiffusion ;

- la communication par le système informatique, d'informations à une personne non autorisée qui se trouve en situation d'accès normal.

26. De même, ne peut être considérée comme un "accès", la simple visualisation d'un écran par-dessus l'épaule d'un opérateur, sauf si la zone était réservée à des opérateurs habilités et que l'accédant, ne l'étant pas, ne pouvait normalement entrer dans la pièce réservée.

2.1.2L'accès frauduleux "avec influence"

27. L'accès frauduleux "avec influence" est sanctionné à l'article 323-1, alinéa 2 du Code pénal :

"Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, la peine est de trois ans d'emprisonnement et de 45.000 euros d'amende".

28. Outre l'accès qui obéit au même régime juridique que celui défini ci-dessus, il convient d'apporter la preuve d'une influence sur le système de traitement automatisé de données. Cette notion d'influence "négative" est soumise à l'administration, notamment, des preuves suivantes :

- la suppression d'une donnée ;
- la modification d'une donnée ;
- l'altération du fonctionnement.

2.2Le maintien frauduleux dans un système de traitement automatisé de données

29. Le maintien frauduleux dans un système de traitement automatisé de données est également sanctionné par l'article 323-1 du Code pénal.

30. En ce qui concerne l'élément moral, la notion de maintien frauduleux est similaire à celle retenue pour l'accès frauduleux. En revanche, l'élément matériel diffère selon le type de maintien frauduleux : avec ou sans influence.

2.2.1Le maintien frauduleux "sans influence"

31. L'élément matériel relatif au maintien frauduleux "sans influence" est constitué uniquement par la notion de maintien. On appelle maintien dans un système informatique, les états de situation anormale telles que connexion, visualisation ou opérations multiples, alors que l'accédant a pris conscience que ce maintien est "anormal".

32. Les peines prévues sont identiques à celles retenues pour l'accès frauduleux, c'est-à-dire un emprisonnement de deux ans et une amende de 30.000 euros.

2.2.2Le maintien frauduleux "avec influence"

33. En revanche, pour ce qui est de l'élément matériel relatif au maintien frauduleux "avec influence", la présence d'une influence, similaire à celle retenue pour l'accès frauduleux avec influence, est nécessaire. Il en est ainsi pour :

- la suppression de données ;
- la modification de données ;
- l'altération du fonctionnement du système.

34. En outre, l'altération du fonctionnement par maintien ne peut être retenue par la simple opération de maintien. Il faut un acte matériel complémentaire autre que celui d'une modification de l'état du système par le simple fait que l'on soit connecté pendant une certaine durée avec maintien en cet état de connexion.

35. Enfin, les peines sont aggravées de la même manière que l'accès frauduleux avec influence, et sont donc un emprisonnement de trois ans et une amende de 45.000 euros.

2.2.3Les atteintes volontaires au fonctionnement d'un système de traitement de données

36. L'article 323-2 du Code pénal punit ces deux délits :

- d'entrave du système ;
- d'altération du fonctionnement.

2.2.4L'entrave du système

37. En ce qui concerne l'élément moral, le texte du Code pénal a supprimé l'expression "intentionnellement et au mépris des droits d'autrui" car elle est apparue inutile.

38. En effet, dès lors que nous nous trouvons en matière délictuelle, l'intention est implicite. D'autre part, le but du législateur a été d'assurer la réparation pénale des préjudices subis non seulement par le maître du système (l'exploitant de l'ordinateur) mais aussi par des tiers bénéficiaires des traitements informatiques.

39. L'élément matériel de l'infraction est constitué uniquement par l'entrave. Ce concept peut être appréhendé de manière extrêmement large, car il suffit d'une influence "négative" sur le fonctionnement du système pour que le concept d'entrave soit retenu. Il en est ainsi pour :

- les bombes logiques;
- l'occupation de capacité mémoire;
- la mise en place de codification, de barrages et de tous autres éléments retardant un accès normal.

40. L'infraction est sanctionnée par le Code pénal d'un emprisonnement de cinq ans et d'une amende de 75.000 euros d'amende.

2.2.5L'altération du fonctionnement

41. Cette infraction est associée à l'entrave du fonctionnement du système de traitement automatisé. L'élément moral retenu pour la qualification est identique à celui retenu pour l'entrave du fonctionnement du système. Quant à l'élément matériel, la notion d'altération du fonctionnement du système est décrite par la formule "faussé le fonctionnement d'un système de traitement automatisé de données".

42. Alors que l'entrave avait pour objet uniquement de retarder ou d'empêcher, de manière momentanée, le fonctionnement, la notion d'altération renvoie à la modification de cet état de fonctionnement, ayant une influence sur les programmes ou les données.

43. Ainsi, en empêchant l'appel d'un sous-programme ou en accédant à la lecture de telle ou telle instruction, le délinquant peut être amené à altérer le système et fausser ainsi le fonctionnement et les résultats associés. De même, l'introduction d'une bombe logique a pour objet de fausser le fonctionnement lorsque cette bombe logique supprime des informations.

44. L'introduction d'un virus ne sera pas constitutive d'une entrave, mais bien d'une altération du fonctionnement, puisque le système informatique en reproduisant les virus sera altéré au regard du fonctionnement normal du système.

45. Enfin, il peut y avoir altération du fonctionnement du système à travers l'altération d'un élément dudit système, par exemple le réseau de télécommunications.

46. Les peines prévues pour ce type d'infraction sont identiques à celles retenues pour l'entrave du système, c'est-à-dire un emprisonnement de cinq ans et une amende de 75.000 euros.

47. Par ailleurs, des peines complémentaires sont applicables au délit d'atteinte au fonctionnement d'un STAD, elles sont énumérées à l'article 323-5 du Code pénal.

2.3Les atteintes volontaires aux données contenues dans un système de traitement automatisé

48. L'article 323-3 du Code pénal punit :

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

49. Le Code pénal introduit une troisième atteinte aux données : le recel des données (article 321-1).

2.3.1La modification des données

50. L'élément moral est constitué de la même manière que pour l'altération du système. La modification des données suppose une inttention et une volonté de commettre cet acte interdit.

51. Toutefois, l'intention de nuire n'est pas nécessaire pour constituer cette infraction.

52. L'élément matériel est, quant à lui, constitué soit de la suppression de données soit de la modification de données :

53. Comme pour le délit précédent, les peines prévues sont un emprisonnement de cinq ans et une amende de 75.000 euros.

2.3.2L'introduction de données pirates

54. L'introduction de données pirates est sanctionnée par l'article 323-3 du Code pénal, au regard duquel l'intention frauduleuse est constituée dès le moment où l'introduction de données s'effectue avec une volonté de modifier l'état du système et ce, quelle que soit l'influence de cet état.

55. En outre, la simple introduction de données quelles qu'en soient les conséquences sur le système, peut entraîner l'application de l'article 323-3 du Code pénal. Pour la qualification de cette infraction, il n'est pas nécessaire d'ajouter à l'élément matériel, des conséquences sur l'introduction des données.

56. De manière générale, toute altération du système ne peut se faire que par altération logique du système ou par intégration de données et permettra l'application de plusieurs articles. Il n'en est pas de même lorsque celles-ci font l'objet d'une intervention physique et non pas seulement logique.

57. Les peines prévues sont un emprisonnement de cinq ans et une amende de 75.000 euros.

2.3.3 Extraction, détention, reproduction, transmission frauduleuse de données

58. La loi du 13 novembre 2014 a introduit de nouvelles infractions aux STAD à l'article 323-3 du Code pénal.

59. Elle et sanctionne le fait d'extraire, de détenir, de reproduire, de transmettre frauduleusement des données.

60. Techniquement, cela vise la « copie » de données et leur transmission.

61. Ces nouvelles infractions permettent de palier au fait qu'il n'existait pas d'infraction sanctionnant le « vol » de données.

62. Les sanctions maximum sont les suivantes :

- 5 ans de prison et 75000 euros d'amende ;
- Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat : 7 ans de prison et à 100 000 euros d'amende ;
- si bande organisée et à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat : 10 ans de prison et à 150 000 euros d'amende.

2.3.4Le recel de données

63. Cette infraction ne figurait pas dans la loi du 5 janvier 1988 car cette dernière n'avait pas retenu le délit de captation de données que le projet de révision du Code pénal avait proposé de créer.

64. En effet, le délit de recel ne peut en principe exister que s'il y a eu préalablement un vol. Si aucun texte ne prévoit une disposition spécifique sur le vol d'informations, la jurisprudence lui applique largement les dispositions générales de l'article 311-1 du Code pénal.

65. Cependant, le Code pénal réintroduit le délit de recel de données car le préjudice que l'on veut réparer, dans le cas des banques de données, ne vient pas de la copie des données et des informations dont elles sont la représentation numérique mais de leur utilisation par un tiers.

66. Mais plutôt que de retenir ce délit spécifique à l'informatique, le législateur a préféré élargir la disposition générale du recel en couvrant le recel d'informations prévu à l'article 321-1, al.2 du Code pénal :

"Constitue également un recel le fait, en connaissance de cause de bénéficier, par tous moyens, du produit d'un crime ou d'un délit".

67. Le délit de recel nécessite également un élément intentionnel consistant dans la connaissance de la provenance litigieuse des informations. Or, si cet élément de l'infraction n'est pas rapporté, le délit de recel ne peut être constitué.

68. Le recel est puni de cinq ans d'emprisonnement et de 375.000 euros d'amende.

2.4HADOPI

69.Le nouvel article L. 336-3 du Code de la propriété intellectuelle issu de la loi du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet[4] dispose :

> « La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise.
> Le manquement de la personne titulaire de l'accès à l'obligation définie au premier alinéa n'a pas pour effet d'engager la responsabilité pénale de l'intéressé, sous réserve des articles L. 335-7 et L. 335-7-1. »

70.Le manquement à cette obligation de sécurisation de l'accès à un réseau est sanctionné par une contravention de 5ème classe[5].

71.Une telle sanction n'est cependant possible que dans la mesure où une recommandation préalable de mettre en œuvre un moyen de sécurisation de l'accès envoyé par Hadopi a été envoyée et que dans l'année qui suit, l'accès serait à nouveau utilisé aux fins de téléchargement illicite.

72.Afin d'éviter toute sanction, les entreprises se doivent de mettre en place des moyens permettant de se prémunir contre des éventuels téléchargements illégaux depuis la connexion qu'elle met à disposition de ses salariés.

73.Pour les aider dans cette tâche, la Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet (Hadopi) devait labelliser des moyens de sécurisations et en publier une liste. Une grande consultation nationale sur le sujet a été tenue. La HADOPI a ainsi publié des fiches pratiques à destination des internautes relatives à l'offre légale, l'identité numérique, aux usages sur Internet.

[4] Loi n°2009-669 favorisant la diffusion et le protection de la création sur internet du 12-6-2009. L'article . 336-3 du CPI a été modifié par la loi n°2009-1311 du 28-10-2009 - art. 10
[5] Art. R. 335-5 Code de la propriété intellectuelle.

2.5La responsabilité des personnes morales

2.5.1La responsabilité pénale

2.5.1.1Les conditions d'application de la responsabilité des personnes morales

74. L'article 121-2 du Code pénal dispose :

> *"Les personnes morales, à l'exclusion de l'Etat, sont responsables pénalement, selon les distinctions des articles 121-4 à 121-7, des infractions commises, pour leur compte, par leurs organes ou représentants.*
>
> *Toutefois, les collectivités territoriales et leurs groupements ne sont responsables pénalement que des infractions commises dans l'exercice d'activités susceptibles de faire l'objet de conventions de délégation de service public.*
>
> *La responsabilité pénale des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits, sous réserve des dispositions du quatrième alinéa de l'article 121-3. »* ".

75. Le principe général de responsabilité des personnes morales est assorti d'une exception qui concerne l'Etat et de quelques limites.

76. Ces limites concernent tout d'abord la responsabilité des collectivités territoriales ou de leurs groupements qui est limité aux "infractions commises dans l'exercice d'activités susceptibles de faire l'objet de conventions de délégation de service public".

77. Par ailleurs, les partis, groupements politiques, syndicats et institutions représentatives du personnel ne se voient pas appliquer les peines les plus graves comme la dissolution ou le placement sous surveillance judiciaire[6].

78. Pour que la responsabilité des personnes morales puisse être engagée, il faut que l'infraction ait été commise "pour leur compte, par leurs organes ou représentants".

79. Les termes "organes" (assemblée générale, conseil d'administration, conseil municipal...) et "représentants" (gérant, président-directeur général, maire...) excluent les infractions qui seraient commises par l'un des employés de la personne morale.

80. De même que les termes "pour le compte" signifient que la responsabilité de la personne morale ne sera pas engagée lorsque le représentant a agi dans l'exercice ou à l'occasion de l'exercice de ses fonctions mais pour son propre compte et dans son seul intérêt personnel.

81. La procédure des infractions commises par les personnes morales est décrite aux articles 706-41 à 706-46 du Code de procédure pénale, à l'exception des règles applicables aux citations insérées par les articles 51 à 56 de la loi dans les dispositions correspondantes du Code de procédure pénale applicables aux personnes physiques[7].

82. L'article 706-42 prévoit que lorsqu'une personne morale est poursuivie sont compétents soit, comme pour les personnes physiques, le procureur de la République et les juridictions du lieu de l'infraction, soit le procureur de la République et les juridictions du lieu où la personne morale a son siège.

83. La représentation de la personne morale est assurée par le représentant légal ou par une personne bénéficiant d'une délégation de pouvoir, et dans certains cas, par un mandataire de justice (article 706-43).

[6] Art. 131-39 Code pénal.
[7] Article 550 du Code de procédure pénale

84. D'après l'article 706-44, une seule mesure de contrainte peut être prise à l'encontre du représentant de la personne morale qui est celle applicable au témoin: en cas de refus de comparaître, le juge d'instruction ou la juridiction de jugement peut l'y contraindre par la force publique (articles 109, 326, 439, 536). Les autres mesures applicables aux personnes physiques (garde à vue, contrôle judiciaire ou détention provisoire) ne pourront lui être applicables.

85. Par contre, la personne morale pourra être placée sous contrôle judiciaire en vertu de l'article 706-45.

2.5.1.2Les peines applicables aux personnes morales

86. Les peines encourues par les personnes morales pourront tout d'abord être l'amende selon les modalités prévues par l'article 131-38 du Code pénal qui dispose :

"Le taux maximum de l'amende applicable aux personnes morales est égal au quintuple de celui prévu pour les personnes physiques par la loi qui réprime l'infraction.

Lorsqu'il s'agit d'un crime pour lequel aucune peine d'amende n'est prévue à l'encontre des personnes physiques, l'amende encourue par les personnes morales est de 1 000 000 euros. ".

87. En outre, la personne morale pourra se voir appliquer les peines prévues à l'article 131-39 du Code pénal :

> « Lorsque la loi le prévoit à l'encontre d'une personne morale, un crime ou un délit peut être sanctionné d'une ou de plusieurs des peines suivantes :

1. la dissolution, lorsque la personne morale a été créée ou, lorsqu'il s'agit d'un crime ou d'un délit puni en ce qui concerne les personnes physiques d'une peine d'emprisonnement supérieure ou égale à trois ans, détournée de son objet pour commettre les faits incriminés ;

2. l'interdiction, à titre définitif ou pour une durée de cinq ans au plus, d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ;

3. le placement, pour une durée de cinq ans au plus, sous surveillance judiciaire ;

4. la fermeture définitive ou 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 des marchés publics à titre définitif ou pour une durée de cinq ans au plus ;

6. l'interdiction, à titre définitif ou pour une durée de cinq ans au plus, de procéder à une offre au public de titres financiers ou de faire admettre ses titres financiers aux négociations sur un marché réglementé ; ;

7. 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 ou d'utiliser des cartes de paiement ;

8. la confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit ;

9. l'affichage de la décision prononcée ou la diffusion de celle-ci soit par la presse écrite, soit par tout moyen de communication audiovisuelle. »

88.La dissolution qui peut être considérée comme la peine capitale pour une personne morale dans la mesure où elle met fin juridiquement à son existence, est limitée de trois manières :

- elle ne s'applique que pour les infractions les plus graves ;
- elle ne s'applique que si la personne morale a été créée ou détournée de son objet pour commettre l'infraction (crime ou délit puni de plus de trois ans) ;
- elle ne s'applique pas pour les personnes morales de droit public, partis ou groupements politiques, syndicats et institutions représentatives du personnel.

89.Des dispositions spécifiques aux personnes morales concernent la récidive (articles 132-12 à 132-15), le sursis simple (articles 132-32 et 132-34, alinéa 2) et la réhabilitation dont les conditions sont moins exigeantes que pour les personnes physiques (articles 133-14 du Code pénal et 798-1 du Code de procédure pénale).

90.Enfin, la loi a créé un casier judiciaire national des personnes morales[8]. Il comporte un bulletin n°1 et un bulletin n°2. Le droit d'accès à ce dernier a été limité (article 776-1 du Code de procédure pénale) et les mentions qui y sont portées ont été réduites. Enfin, la possibilité la réhabilitation judiciaire est admise plus largement au profit des personnes morales.

91. En ce qui concerne les atteintes aux STAD explicitées plus haut, les personnes morales peuvent être pénalement responsables en application de l'article 323-6 du Code pénal selon lequel :

> « Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39.
>
> L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise. »

2.5.2La responsabilité civile des personnes morales

92. Selon l'article 1384 du Code civil :

> « On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde. (….)
> Les maîtres et les commettants, du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils sont employés ».

93.L'employeur est civilement responsable du fait de l'activité de ses préposés, notamment en cas d'utilisation malveillante des moyens informatiques et de communications électroniques mis à sa disposition.

94.Ainsi, l'employeur du créateur d'un site internet a été condamné sur ce fondement pour avoir mis à disposition de son salarié les moyens techniques nécessaires à la mise en ligne dudit site et parce qu'il n'avait pas interdit l'usage à des fins personnelles des moyens informatiques[9].

[8] Loi n° 92-1336 du 16 décembre 1992 relative à l'entrée en vigueur du nouveau code pénal et à la modification de certaines dispositions de droit pénal et de procédure pénale rendue nécessaire par cette entrée en vigueur

[9] TGI Marseille, 11-6-2003, Société Lucent technologies ; confirmé par CA Aix en Provence 2e ch, 13-03-2006n° pourvoi : n°2006/170

95.Cependant, l'employeur peut s'exonérer de sa responsabilité lorsque celui-ci parvient à démontrer que le préposé a agi hors des fonctions auxquelles il était employé, sans autorisation, et à des fins étrangères à ses attributions[10].

3.Les règlementations spécifiques/sectorielle

3.1Le référentiel général de sécurité (RGS)

96.Le référentiel général de sécurité est un recueil de règles et de bonnes pratiques en matière de sécurité des systèmes d'information.

97.Il est principalement destiné aux autorités administratives qui proposent des services en ligne aux usagers.

98.Il a pour but d'assurer la sécurité des échanges électroniques entre les usagers et les autorités administratives ainsi qu'entre les autorités administratives elles-mêmes.

3.1.1A qui s'applique le RGS ?

99.Sont visés par le RGS et sont donc tenus de l'appliquer les acteurs suivants :

- les administrations de l'Etat, à savoir principalement les Ministères et leurs démembrements ;
- les collectivités territoriales (Conseil régionaux, conseil généraux, communes) ;
- les établissements publics à caractère administratif ;
- les établissements gérant des régimes de protection sociale relevant du code de la sécurité sociale et du code rural ;
- les établissements mentionnés aux articles L 223-16 et L 351-21 du code du travail ;
- les organismes chargés de la gestion d'un service public.

100.Cependant, le RGS ne s'applique que sur les SI. En effet, seules sont concernées, parmi ces autorités administratives, celles qui mettent en œuvre des systèmes d'information susceptibles d'échanger des informations avec d'autres autorités administratives ou avec des usagers.

101.L'ordonnance du 8 décembre 2005 ne reconnaît qu'une exception : les SI relevant du secret de la Défense nationale[11].

3.1.2Les obligations qui pèsent sur les acteurs

102.Les obligations qui pèsent sur les acteurs impliqués sont de trois natures :

- l'utilisation de produits labellisés ;

- l'obligation d'attester formellement auprès des utilisateurs de son système d'information que celui-ci est protégé conformément aux objectifs de sécurité ;

- la protection du SI. L'article 3 du décret du 2 février 2010 prévoit que l'autorité administrative doit, afin de protéger un système d'information :

[10] Cass. Ass. Plen. 19-5-1988, bull. civ. n°5.
[11] Art. 15 de l'ord. 2005-1516, 8-12-2005, relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administrative, prise en application de l'art. 3 de la loi n° 2004-1343, 9-12-2004 de simplification du droit (JO 9-12-2004)

- Identifier l'ensemble des risques pesant sur la sécurité du système et des informations qu'il traite, eu égard notamment aux conditions d'emploi du système ;
- Fixer les objectifs de sécurité, notamment en matière de disponibilité et d'intégrité du système, de confidentialité et d'intégrité des informations, ainsi que d'identification des utilisateurs du système, pour répondre de manière proportionnée au besoin de protection du système et des informations face aux risques ;
- En déduire les fonctions de sécurité et leur niveau qui permettent d'atteindre ces objectifs et respecter les règles correspondantes du référentiel général de sécurité.

103.L'autorité administrative réexamine régulièrement la sécurité du système et des informations en fonction de l'évolution des risques.

3.1.3Valeur juridique et opposabilité du RGS

104.Le RGS est donc obligatoire pour toutes les autorités administratives, à l'exception des SI relevant du secret de la Défense nationale.

105.Tous les autres SI doivent y être conformes.

106.Enfin si les acteurs impliqués doivent mettre leur SI en conformité, cela implique que les prestataires avec lesquels ils travaillent s'engagent sur cette conformité.

107.Aucune sanction n'est prévue en cas d'éventuel manquement.

108.Il s'agit là d'une pratique courante car l'Etat étant supposé appliquer la loi, ne prévoit pas pour lui-même les conditions d'un éventuel manquement.

109.La sanction, si sanction il y a, viendra le plus souvent d'un recours contre l'acteur impliqué qui n'aura pas utilisé un SI conforme. Les sanctions envisageables pourront, par exemple, être la nullité de tous les actes pris *via* le SI ou la suspension, voir l'arrêt du SI.

110. L'arrêté du 13 juin 2014 porte approbation de la version 2 du référentiel général de sécurité et précise les modalités de mise en œuvre de la procédure de validation des certificats électroniques.

111. Le RGS V2.0 consiste en une fusion des politiques de certification types et distingue quatre usages des certificats électroniques :
- signature électronique ;
- authentification ;
- confidentialité ;
- signature électronique et authentification.

112. Le RGS V2.0 intègre notamment le référentiel d'exigences applicable aux prestataires d'audit de la sécurité des systèmes d'information (PASSI).

113. Ce document distingue trois niveaux de sécurité aux exigences croissantes : *, ** et ***.

3.2Réglementation informatique et libertés

114.La loi dite Informatique et libertés réglemente la collecte et l'utilisation de données à caractère personnel et impose notamment au responsable de traitement une obligation générale de sécurité.

115.En effet, l'article 34 de cette loi précise que le responsable du traitement est tenu de prendre :

- «toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

  Des décrets, pris après avis de la Commission nationale de l'Informatique et des libertés, peuvent fixer les prescriptions techniques auxquelles doivent se conformer les traitements mentionnés au 2° et au 6° du II de l'article 8. »

116.Le non-respect de cette obligation est par ailleurs sanctionné à l'article 226-17 du Code pénal qui réprime tout manquement à la sécurité des données d'une peine pouvant aller jusqu'à cinq ans d'emprisonnement et 300.000 euros d'amende.

117.L'ordonnance du 24 août 2011 a inséré un nouvel article 34 bis à la loi Informatique et libertés obligeant le fournisseur de services de communications électroniques au public en ligne à notifier, sans délai, à la Cnil et à la personne intéressée les violations des données à caractère personnel.

118.Le fait de ne pas procéder à cette notification est puni de 5 ans d'emprisonnement et de 300.000 euros d'amende.

119.Le décret du 30 mars 2012 est venu préciser les informations que le fournisseur doit communiquer à :

- la Cnil en cas de violation de données à caractère personnel ;
- la personne concernée en cas de risque d'atteinte aux données à caractère personnel ou à la vie privée d'une personne.

120.Ce texte précise, toutefois, que le fournisseur peut être dispensé de notifier la violation de sécurité à la personne concernée s'il a mis en place des mesure de protection appropriées (la définition de telles mesures étant donnée par le décret) et si la Cnil a constaté que ces mesures ont été mises en œuvre.

121.Le règlement européen du 24 juin 2013 est venu généraliser cette obligation de notification des violations des données à caractère personnel à l'autorité compétente ainsi qu'à la personne concernée, que ce soit un abonné ou un particulier. Il est entré en vigueur le 25 août 2013.

122. Le contenu de la notification devant être adressé à la CNIL est détaillé par le règlement et doit comprendre :

- le nom du fournisseur de service de communication électronique ;
- l'identité et les coordonnées du correspondant à la protection des données ;
- une mention indiquant s'il s'agit d'une première ou d'une deuxième notification
- la date et l'heure de l'incident ;
- les circonstances de la violation de données (ex : perte, vol…) ;
- la nature et la teneur des données concernées ;
- les mesures techniques et d'organisation appliquées ;
- le recours à d'autres fournisseurs ayant joué un rôle (le cas échéant) ;
- un résumé de l'incident à l'origine de la violation ;
- le nombre d'abonnés ou de particuliers concernés ;
- les conséquences et préjudices potentiels pour les abonnés ou les particuliers ;
- les mesures techniques et d'organisation prises pour atténuer les préjudices potentiels ;
- dans le cas où une notification supplémentaire a été envoyée aux abonnés ou aux particuliers :
  - le contenu de la notification ;
  - les moyens de communication utilisés ;
  - le nombre d'abonnés ou de particuliers informés ;

- si les données atteintes concernent des abonnés ou particuliers situés dans d'autres Etats membre de l'Union européenne ;
- la notification à d'autres autorités nationales (le cas échéant).

123.Concernant la notification devant être adressée à l'abonné ou au particulier, celle-ci doit comprendre :

- le nom du fournisseur ;
- l'identité et les coordonnées du correspondant à la protection des données ;
- le résumé de l'incident à l'origine de la violation de données à caractère personnel ;
- la date estimée de l'incident ;
- la nature et la teneur des données à caractère personnel concernées ;
- les conséquences vraisemblables pour l'abonné ou le particulier concerné ;
- les circonstances de la violation ;
- les mesures prises par le fournisseur pour remédier à la violation ;
- les mesures recommandées par le fournisseur pour atténuer les préjudices potentiels.

124.En cas de sous-traitance, l'article 35 de la loi de 1978 modifiée dispose :

> « Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable de traitement.
> Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable de traitement. »

125.Dans le cadre des Assises de la sécurité, la Cnil a publié, en octobre 2010[12], un nouveau guide destiné à faciliter l'application par les responsables de traitements des prescriptions de la loi Informatique et libertés en matière de sécurité des données personnelles.

126.Il est associé à ce guide, constitué de 17 fiches thématiques, un questionnaire, disponible sur le site de la commission, qui permettra aux personnes intéressées d'apprécier le niveau de sécurité des traitements de données mis en œuvre par l'organisme auquel ils sont rattachés.

127. Par ailleurs, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) rédige des guides portant sur la sécurité des systèmes d'information. Elle a notamment publié un guide sur les systèmes d'information industriels dont les mesures détaillées ont été rendues accessibles au public le 21 janvier 2014[13].

4.LOPPSI 2

4.1Délit d'usurpation d'identité.

128.Chaque année en France, plus de 210 000 personnes seraient confrontées à une usurpation d'identité numérique.

129.Conscient des lacunes présentées par le droit positif, le législateur vient d'instaurer un délit spécifique permettant de sanctionner l'usage malveillant d'éléments d'identité d'un tiers sur un réseau de communication électronique.

[12] Ce guide est accessible à l'adresse :
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_securite%20VD.pdf
[13] http://www.ssi.gouv.fr/IMG/pdf/securite_industrielle_GT_details_principales_mesures.pdf

130.La loi d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011 a crée un nouvel article 226-4-1 au sein de la partie du Code pénal consacrée aux atteintes à la personnalité et à la vie privée, rédigé ainsi :

> « *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*. »

131.Ce délit sanctionne l'usurpation de l'identité d'une personne physique, mais également l'usurpation de toutes les données permettant de l'identifier ce qui, en l'absence de définition clairement posées par la loi, pourrait notamment être le cas de :

- l'adresse électronique ;
- l'identifiant et le mot de passe ;
- un blog ;
- un avatar.

132.Pour que le délit soit constitué, trois conditions doivent être réunies :

- une utilisation
- de l'identité d'un autre
- mettant autrui en situation de risque juridique

133.La difficulté d'application à prévoir de ce texte vient du fait qu'il ne précise à aucun moment ce qu'est la tranquillité d'une personne. Cette indétermination de la notion a été vivement critiquée lors de la discussion du projet de loi en raison de l'interprétation extensive qui peut en être faite et qui peut, par là même, « générer une insécurité juridique préjudiciable à la liberté d'expression sur les réseaux de communication »[14].

134.Concernant l'usurpation d'identité en ligne réalisée en vue de porter atteinte à l'honneur ou à la considération de la personne dont l'identité a été usurpée, il conviendra de se reporter à la jurisprudence existante en matière de diffamation[15] pour appréhender ce que peuvent recouvrir ces notions.

4.2La captation des données informatiques

4.2.1Les accès antérieurement autorisés

4.2.1.1Collecte d'informations utiles à la manifestation de la vérité

135. La loi du 18 mars 2003 pour la sécurité intérieure (LSI) prévoit que sur demande de l'officier de police judiciaire, les organismes publics ou les personnes morales de droit privé à l'exception de ceux visés au deuxième alinéa de l'article 31 et à l'article 33 de la loi n°78-17 du 6 janvier 1978 relative à l'Informatique aux fichiers et aux libertés, mettent à sa disposition les informations utiles à la manifestation de la vérité, à l'exception de celles protégées par un secret prévu par la loi, contenues dans le ou les systèmes informatiques ou traitements de données nominatives qu'ils administrent.

136. Par conséquent, des informations contenues dans un système informatique doivent être mises à la disposition de la police judiciaire[16].

[14] Amendement présenté par MM. Braouezec, Vaxès, Mme Amiable, M. Asensi, Mme Billard, MM. Bocquet, Brard, Mme Buffet, MM. Candelier, Chassaigne, Dessalangre, Dolez, Mme Fraysse, MM. Gerin, Gosnat, Gremetz, Lecoq, Muzeau, Daniel Paul, Sandrier.
[15] Art. 29 de la loi du 29-7-1881 sur la liberté de la presse.

4.2.1.2Possibilité d'accéder à des données informatiques au cours d'une perquisition

137. L'article 17 de loi LSI a inséré dans le Code de procédure pénale un article 57-1 qui permet aux officiers de police judiciaire, au cours d'une perquisition d'accéder par un système informatique implanté sur les lieux où se déroule la perquisition, à des données intéressant l'enquête en cours et stocker dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.

138. Par ailleurs, les données auxquelles il aura été permis d'accéder peuvent être copiées sur tout support.

139. Les supports de stockage informatique peuvent être saisis et placés sous scellé.

4.2.2Les innovations de la LOPPSI 2

140.Afin de pouvoir mieux réprimer le comportement de certains criminels ne communiquant sur leurs activités qu'à travers des comptes mél ou à partir de cybercafés, la LOPPSI 2 a introduit de nouveaux articles au sein du Code de procédure pénale permettant aux enquêteurs de procéder à la captation à distance de données informatiques.

141.L'article 706-102-1 est rédigé comme suit :

> « Lorsque les nécessités de l'information concernant un crime ou un délit entrant dans le champ d'application de l'article 706-73 l'exigent, le juge d'instruction peut, après avis du procureur de la République, autoriser par ordonnance motivée les officiers et agents de police judiciaire commis sur commission rogatoire à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères. Ces opérations sont effectuées sous l'autorité et le contrôle du juge d'instruction ».

142.Ce dispositif pourra être autorisé pour une durée maximale de quatre mois, prorogeable une fois si les nécessités de l'enquête l'exigent.

143.Par ailleurs, le juge d'instruction devra préciser les infractions recherchées à peine de nullité. Toutefois, l'article 706-102-4 alinéa 2 précise que la découverte d'infractions autres que celles visées par le juge ne constitue par une cause de nullité des procédures incidentes.

144.Concernant l'installation du dispositif[17], trois cas doivent être distingués :

- Lorsque l'installation du dispositif ne nécessite pas une intervention physique dans des locaux, mais une simple transmission par un réseau de communication électronique, elle peut être autorisée par le juge d'instruction ;
- lorsqu'il faut installer le dispositif dans un lieu privé entre 21 h et 6h du matin, l'autorisation doit provenir du juge d'instruction ;
- lorsque le dispositif doit être installé dans un lieu d'habitation en dehors des heures légales de perquisition, l'autorisation doit être délivrée par le juge des libertés et de la détention.

145.Ne peuvent en principe faire l'objet d'une telle surveillance les entreprises de presse ou de communication audiovisuelle, les médecins, les notaires, les avoués, les huissiers, les députés, les sénateurs, les avocats ainsi que les magistrats.

[16] Art. 60-1 Code de procédure pénale.
[17] Art. 706-102-5 du Code de procédure pénale.

146.Les enregistrements des données informatiques seront placés sous scellés fermés et seront retranscrites dans un procès-verbal qui sera versé au dossier sans qu'aucune séquence relative à la vie privée étrangère aux infractions recherchées ne puisse y figurer.

147.Les dispositions précitées ont un champ d'application limité puisqu'elles ne peuvent concerner que la lutte contre la délinquance et la criminalité organisée.

148.Par conséquent, le risque que des entreprises soient concernées par ces dispositions est peu élevé, mais pas exclu.

149.En effet, si un salarié est soupçonné de se livrer à de telles activités en utilisant les moyens informatiques mis à sa disposition par son employeur, le système informatique de l'entreprise pourrait faire l'objet d'une telle captation informatique, sans que quiconque n'en soit informé.

150.Or, le risque majeur réside dans la découverte par les personnes chargées de la sécurité des systèmes informatiques au sein de l'entreprise de ce dispositif et sa neutralisation.

151. Une telle hypothèse n'a pas été traitée par les textes et on pourrait envisager une sanction sur le fondement de le 2° de l'article 434-4 du Code pénal qui punit de trois ans d'emprisonnement et de 45.000 € d'amende le fait, en vue de faire obstacle à la manifestation de la vérité, de détruire, soustraire, receler ou altérer un objet de nature à faciliter la découverte d'un crime ou d'un délit, la recherche des preuves ou la condamnation des coupables.

152.Cependant, pour que cette infraction soit constituée, faut-il encore démontrer son élément intentionnel ce qui semble peu probable dans la mesure où les responsables de la sécurité des systèmes n'étaient pas au courant du dispositif de surveillance.

5.Loi pour la programmation militaire 2014-2019

5.1Extension des périmètres de surveillance et d'interception

153.Depuis la loi relative à la lutte contre le terrorisme[18], un accès extrajudiciaire est prévu, dans le cadre de la prévention des actes terroristes, concernant les données d'identification des contributeurs (LCEN art 6 II bis) et les logs de connexion (article L 34-1-1 du Code des postes et des communications électroniques).

154. Ce dispositif anti-terroriste, initialement conçu pour être temporaire et expérimental, a été définitivement pérennisé par la loi de programmation militaire 2014-2019 qui consacre l'accès administratif aux données d'identification et de connexion.

155. Le décret n°2014-1575 du 24 décembre 2014, pris en application de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, encadre la collecte et le traitement des données de connexion par certains services du ministère de l'intérieur et de la justice, et notamment :
- les informations permettant d'identifier l'utilisateur ;
- les données relatives aux équipements terminaux de communication utilisés ;
- les caractéristiques techniques la date, l'horaire et la durée de chaque communication ;
- les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;
- les données permettant d'identifier le ou les destinataires de la communication.

[18]Loi n° 2006-64 du 23 01 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers

5.2Pérennisation de l'accès aux données d'identification

156. Ainsi, l'article L. 246-1 du Code de la sécurité intérieur autorise :

« *le recueil (…) des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications* ».

157. Par ailleurs, il convient de préciser que le champ d'application de l'article L. 246-1 est étendu au-delà du terrorisme aux quatre autres motifs prévu par l'article L 241-2 du CSI :

- sécurité nationale ;
- sauvegarde des éléments essentiels du potentiel scientifique et économique de la France ;
- prévention de la criminalité et de la délinquance organisées ;
- prévention de la reconstitution ou du maintien de groupements dissous en application de la loi de 1936 sur les groupes de combat et les milices privées.

6.Loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme

158.La Loi n°2014-1353 du 13 novembre 2014, adoptée pour renforcer la lutte contre le terrorisme sur Internet, vient modifier la loi Godfrain (Loi n°88-19 du 5 janvier 1988, première loi consacrée à la fraude informatique venant encadrer la protection du système d'information contre les intrusions, altérations et entraves (déni de service...)).

159.La loi ajoute de nouvelles infractions : l'extraction, la détention, la reproduction et la transmission des données issues d'un STAD (voir plus haut).

160.La loi créé une circonstance aggravante lorsque les atteintes sont commises en bande organisé à l'encontre d'un STAD mis en œuvre par l'Etat.

6.1Cyberpatrouille

161.Un arrêt de la Cour de cassation du 30 avril 2014[19] avait illustré la distinction entre la «provocation à la preuve » de l'infraction et la « provocation à la commission » de l'infraction, la preuve obtenue dans cette dernière hypothèse étant irrecevable.

162.Dans le cadre d'une enquête visant des sites spécialisés en matière de cybercriminalité, le FBI a mis en place un forum d'infiltration dénommé "Carderprofit", permettant aux utilisateurs d'échanger sur des sujets liés à la fraude à la carte bancaire et de communiquer des offres d'achat, de vente ou d'échange de biens et services liés à cette fraude. La Cour d'appel a constaté que puisque l'individu avait déjà manifesté, sur d'autres sites, son intérêt pour les techniques de fraude à la carte bancaire, il apparaissait que le forum d'infiltration en cause avait seulement permis de rassembler les preuves de la commission de fraudes à la carte bancaire et d'en identifier les auteurs. La Cour de cassation a estimé qu'il résultait de ces constatations qu'« il n'y avait pas eu, de la part des autorités américaines, de provocation à la commission d'infractions.

[19] Cass. crim 30 04 2014, aff. Forum de carding d'infiltration dénommé « carderprofit »

163.L'article 706-87-1 du Code pénal vient désormais élargir les attributions des agents ou officiers de police judiciaire dans le cadre de leurs enquêtes ou commissions rogatoires en matière de criminalité et délinquance organisées.

164.L'article dispose que « d*ans le but de constater les infractions mentionnées aux articles 706-72 et 706-73 et, lorsque celles-ci sont commises par un moyen de communication électronique, d'en rassembler les preuves et d'en rechercher les auteurs, les officiers ou agents de police judiciaire agissant au cours de l'enquête ou sur commission rogatoire peuvent, s'ils sont affectés dans un service spécialisé désigné par arrêté du ministre de l'intérieur et spécialement habilités à cette fin, procéder aux actes suivants sans en être pénalement responsables :*
1° Participer sous un pseudonyme aux échanges électroniques ;
2° Etre en contact par le moyen mentionné au 1° avec les personnes susceptibles d'être les auteurs de ces infractions ;
3° Extraire, acquérir ou conserver par ce moyen les éléments de preuve et les données sur les personnes susceptibles d'être les auteurs de ces infractions ;
4° Extraire, transmettre en réponse à une demande expresse, acquérir ou conserver des contenus illicites, dans des conditions fixées par décret.
A peine de nullité, ces actes ne peuvent constituer une incitation à commettre ces infractions. »

6.2Blocage de sites

165.Dans le cadre de la politique gouvernementale de renforcement des moyens de lutte contre le terrorisme, la loi du 13 novembre 2014 est venue modifier la loi pour la confiance en l'économie numérique en créant la possibilité, pour l'autorité administrative, de demander aux éditeurs et/ou hébergeurs de sites internet de retirer les contenus provoquant à des actes de terrorisme ou faisant l'apologie de tels actes, ainsi que ceux diffusant des images ou des représentations de mineurs à caractère pornographique.

166.En cas de non-conformité des éditeurs et/ou hébergeurs à cette demande (auquel cas ils s'exposent à des sanctions pénales), l'autorité administrative pourra alors demander aux fournisseurs d'accès à internet de bloquer l'accès à ces sites.

167.Le décret n°2015-125 du 5 février 2015 est venu préciser la procédure applicable pour ce blocage.

168.Cette procédure ne pourra être mise en œuvre que par un agent désigné par l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. Ce dernier communique aux fournisseurs d'accès à internet, par un mode de transmission sécurisé, la liste des adresses électroniques des sites contrevenants. Les fournisseurs d'accès à internet ont alors vingt-quatre heures pour bloquer l'accès à ces sites, par tout moyen approprié. De plus, ils devront mettre en place un renvoi de l'internaute vers une page d'information du ministère de l'intérieur expliquant les motifs du blocage.

169.Une vérification trimestrielle du contenu des sites bloqués sera effectuée par l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. Si ce contenu n'est plus considéré comme illicite, l'adresse électronique du site est retirée de la liste et les fournisseurs d'accès à internet auront alors vingt-quatre heures pour rétablir l'accès à ce site.

170.Un membre habilité de la CNIL est chargé du contrôle de la liste des adresses électroniques communiquées et de la régularité des demandes de blocage.

171.Enfin, il est prévu que les fournisseurs d'accès à internet recevront une compensation financière visant à couvrir les surcoûts engagés pour la mise en œuvre de ces blocages. Pour l'obtenir, les fournisseurs d'accès à internet devront adresser à l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication le détail de leurs interventions.

172.Les premiers cas de blocage ont été réalisés dès le le 15 mars 2015.

6.3 Déréférencement de sites

173.Le Décret n°2015-253 du 4 mars 2015 vise le déréférencement des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique auprès des moteurs de recherche ou d'annuaires.

174.Ce décret vient compléter celui du 5 février 2015 relatif au blocage de site.

175.Ce décret précise la permettant de demander aux exploitants de moteurs de recherche ou d'annuaires le déréférencement des sites incitant à la commission d'actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique.

176.Selon le décret, le déréférencement au sein des moteurs de recherche et annuaires s'effectuera en trois étapes :

- dans un premier temps, l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) transmettra aux exploitants de moteurs de recherche ou d'annuaires les adresses électroniques à déréférencer, selon un mode de transmission sécurisé ;
- ces adresses électroniques devront également être transmises « sans délai » et dans les mêmes conditions à la personnalité qualifiée désignée par la Cnil ;
- dans les 48 heures suivant cette notification, les exploitants des moteurs de recherche ou d'annuaires seront tenus de prendre « toute mesure utile destinée à faire cesser le référencement de ces adresses ».

177.En exécutant ce déréférencement, la confidentialité des données qui ont été communiquées doit être respectée et les adresses électronique ne doivent pas être modifiées « que ce soit par ajout, suppression ou altération ».

178.Le Décret met en place un contrôle postérieur au déréférencement**.** Une fois les sites déréférencés, l'OCLCTIC devra vérifier, « au moins chaque trimestre », que les adresses électroniques notifiées ont toujours un contenu présentant un caractère illicite. Dans le cas contraire, l'office devra notifier sans délai les adresses électroniques à la personne qualifiée de la Cnil et aux exploitants de moteurs de recherche ou d'annuaires afin que ces derniers puissent procéder, dans les 48 heures, au rétablissement de leur référencement.

179.La personne qualifiée désignée par la Cnil pourra « recommander » à l'OCLCTIC de mettre fin à une mesure de déréférencement en cas de constat d'une irrégularité. En cas d'opposition de l'OCLCTIC, l'intéressé aura la capacité de saisir la juridiction administrative compétente, en référé ou sur requête.