SCHÉMA
DROIT DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

NOTE D'ACTUALISATION DE LA VERSION 2015

Fédération des réseaux métier
d'Administrateurs Systèmes et Réseaux (ASR) dans le
milieu Enseignement Supérieur et Recherche

Table des matières

1. Préambule

1 La présente note vise à actualiser le schéma de synthèse des textes applicables au droit des systèmes d'information élaboré le 2 juin 2015 à la lumière des évolutions législatives et règlementaires françaises et européennes intervenue en 2016 et 2017.

2 Pour ce faire, les différentes thématiques du schéma seront successivement appréhendées et les évolutions intervenues ou à intervenir seront présentées. Les modifications proposées du schéma figureront en droit pour chaque thématique.

2. Cybercriminalité

3 S'agissant de cette thématique, le schéma dans sa version actuelle comporte deux axes :

- sur le fond, il présente les infractions d'atteinte à un système de traitement automatisé de données (STAD) telles qu'issues de la loi Godfrain du 5 janvier 1988 ;
- sur la forme, il envisage les spécificités procédurales existant relativement aux infractions commises par l'intermédiaire d'un réseau de communication électronique (cyberpatrouille et perquisition à distance).

4 En ce qui concerne les infractions relatives à un STAD, peut-être serait-il pertinent de mentionner la possibilité dégagée par la jurisprudence de caractériser un vol d'information intervenue dans l'hypothèse de l'atteinte à un STAD. D'après la Cour de cassation, le vol en effet peut être caractérisé si le prévenu « *s'est maintenu dans un système de traitement automatisé après avoir découvert que celui-ci était protégé et a soustrait des données qu'il a utilisées sans le consentement de leur propriétaire* »[1].

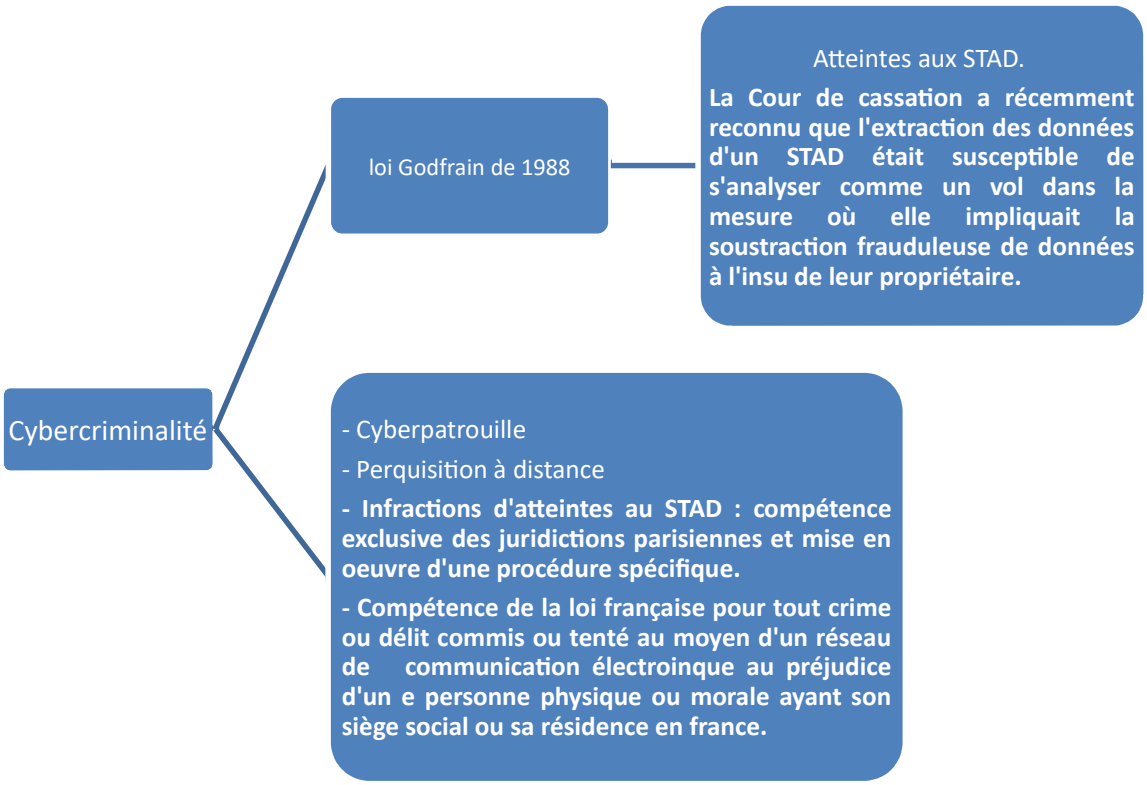
5 S'agissant de la procédure applicable, l'article 28 de la loi n°2016-731 du 3 juin 2016 relative au terrorisme et au crime organisé[2] concerne la cybercriminalité. Cette disposition modifie notamment les règles procédurales applicables aux infractions d'atteinte à un STAD :

- affirmation du principe selon lequel est assujetti au droit français tout crime ou délit commis ou tenté au moyen d'un réseau de communication électronique au préjudice d'une personne physique ou morale résidant ou ayant son siège social en France ;
- assujettissement des infractions d'atteinte à un STAD commises en bande organisée aux règles procédurales relatives à la surveillance et aux interceptions de correspondance émises par voie de communications électroniques et au recueil des données techniques de connexion ;
- prévision d'une compétence concurrente du procureur de la République, du pôle de l'instruction, du tribunal correctionnel et de la cour d'assises de Paris et possibilité pour de tels organes situés en province de se dessaisir à leur profit ;
- applicabilité de la procédure applicable aux infractions commises en bande organisée aux crimes et délits en matière de STAD commis en bande organisée.

6 Il conviendrait par conséquent d'apporter les modifications suivantes au schéma :

1Cass, crim, 20 mai 2015 n°14-81336 *Bluetouff*

2Loi n°2016-371 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties contre la procédure pénale



3. Sécurité intérieure

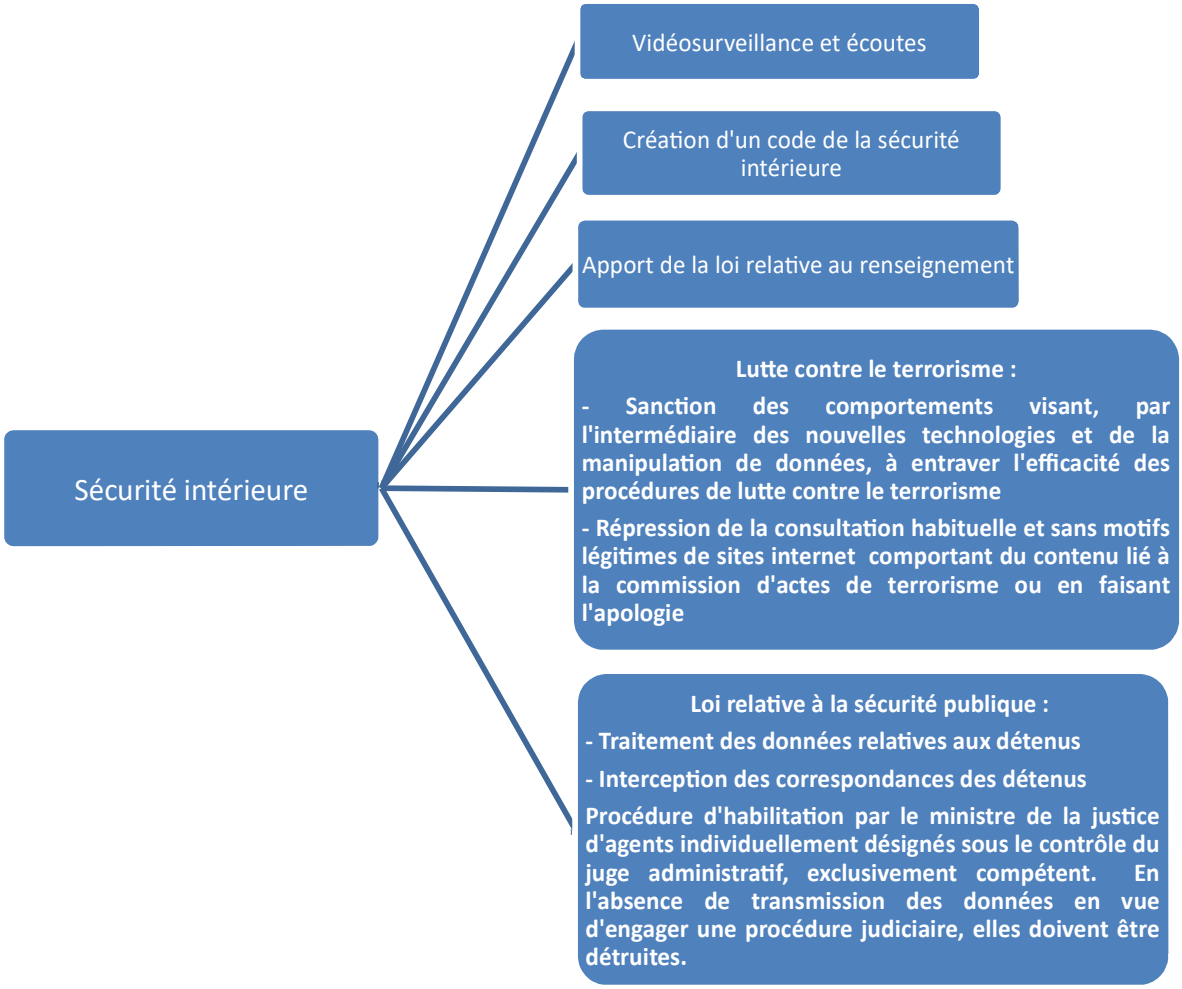
7 Compte tenu de l'actualité des trois dernières années et de la prééminence des attentats terroristes, la sécurité intérieure constitue aujourd'hui l'une des préoccupations fondamentales du législateur. Outre la loi relative au renseignement du 24 juillet 2015, deux textes peuvent être mentionnés, lesquels ont engendré des modifications majeures en matière de lutte contre le terrorisme, mais pas uniquement :

- la loi précitée du 3 juin 2016 a créé une infraction consistant à réprimer les comportements visant, par le biais des nouvelles technologies et de la manipulation de données, à entraver l'efficacité des procédures mises en œuvre aux fins de lutter contre le terrorisme ;

- la loi du 28 février 2017 relative à la sécurité publique[3] peut être citée à deux égards :
  - en premier lieu, elle consacre la nouvelle rédaction de l'infraction de consultation habituelle de site internet mettant en ligne du contenu lié à la commission d'actes de terrorisme ou en faisant l'apologie
  - en second lieu, elle règlemente l'usage des données relatives aux détenus en milieu carcéral. Elle autorise notamment le ministre de la justice à habiliter certains agents pénitentiaires afin qu'ils puissent accéder à de telles données et, si nécessaire, à intercepter les correspondances des détenus et conserver les données de connexion afférentes. En l'absence de transmission des données à l'autorité judiciaire, les données interceptées et conservées sont détruites. Tout litige en la matière relève de la compétence du juge administratif.

8 Ces deux textes pourraient justifier une modification du schéma existant selon les modalités suivantes :

3Loi n°2017-258 du 28 février 2017 relative à la sécurité publique



4. Internet

9 L'actualité de 2016 et 2017 a été marquée, s'agissant du droit du numérique, par l'adoption de la loi pour une République numérique le 7 octobre 2016[4]. Ce texte complète le dispositif jusqu'à présent applicable à Internet à plusieurs égards :

- instauration d'un principe de neutralité de l'Internet, selon lequel tout internaute doit avoir accès aux mêmes contenus quel que soit son fournisseur d'accès à Internet (FAI). Ce principe consiste ainsi à garantir l'accès à l'Internet ouvert tel qu'envisagé par le règlement européen du 25 novembre 2015 relatif à cette thématique[5]. Afin de mettre en œuvre ce principe, la loi précitée a édicté un certain nombre de règles, telles que l'interdiction de prévoir une limitation technique ou contractuelle à un service d'accès à Internet, l'obligation de prévoir une compatibilité des équipements terminaux avec la norme IPv6, etc.

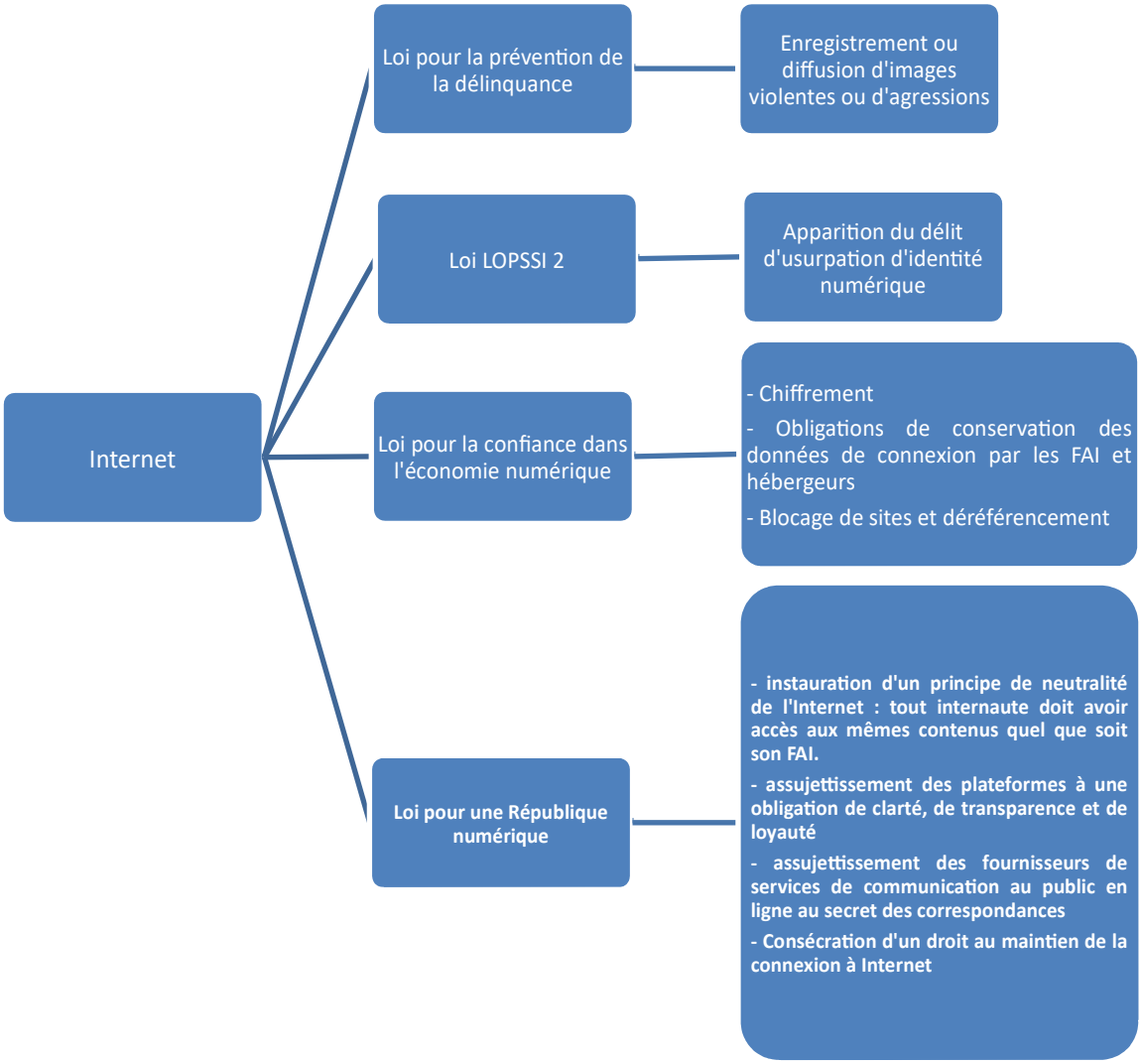
- création d'une règlementation applicable aux plateformes en ligne, définies par le texte comme un service de communication au public permettant le référencement ou le classement de contenus, biens ou services mis en ligne par des tiers et/ou la mise en relation entre plusieurs parties en vue d'une opération de vente, de prêt ou d'échange. Le texte assujettit les plateformes à une obligation de clarté, de loyauté et de transparence vis-à-vis des consommateurs.

4Loi n°2016-1321 du 7 octobre 2016 pour une République numérique
5Règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établissement des mesures relatives à l'accès à un internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) n°531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'union

- assujettissement des fournisseurs de services de communication au public en ligne au secret des correspondances dès lors qu'ils permettent à leurs utilisateurs d'échanger des correspondances. Le secret couvre le contenu des correspondances, l'identité des correspondants et, le cas échéant, l'intitulé du message et des documents joints à la correspondance. Le texte précise que cette obligation ne fait pas obstacle à la mise en œuvre de traitements automatisés d'analyse des correspondances ou de détection de contenus non sollicités ou de programmes malveillants.

- consécration d'un droit au maintien de la connexion à Internet au titre de la mise en œuvre du droit au logement. En cas de difficultés, la connexion peut être réduite mais doit rester maintenue s'agissant de certains sites et de l'accès aux messageries électroniques, et ce jusqu'à ce qu'il ait été statué sur une demande d'aide.

10 Outre les lois d'ores et déjà mentionnées, il conviendrait de mentionner dans le schéma les apports précités de la loi pour une République numérique s'agissant de la règlementation applicable à Internet.



5. Informatique et libertés

11 Le droit des données à caractère personnel a beaucoup évolué depuis juin 2015. En effet, le schéma dans sa version actuelle mentionne le projet de règlement européen du 25 janvier 2012. Celui-ci a donné lieu au Règlement général sur la protection des données (RGPD) du 27 avril 2016, qui entrera en vigueur le 25 mai 2018 sans nécessité de transposition. Un délai de deux ans a donc été laissé aux Etats membres afin qu'ils adaptent leur droit interne aux changements majeurs qu'il engendrera, qui peuvent être synthétisés comme suit :

- élargissement du champ d'application du droit européen des données à caractère personnel, applicable dès lors qu'un résident européen est substantiellement affecté par un traitement de données ;
- durcissement des sanctions applicables, lesquelles peuvent désormais atteindre 4% du chiffre d'affaires mondial de la société responsable de traitement ;
- consécration du principe d'*accountability*, définie comme l'obligation pour un responsable de traitement de rendre des comptes et de démontrer la mise en œuvre d'un processus permanent et dynamique de mise en conformité à la règlementation relative à la protection des données ;
- consécration du principe de *privacy by design / by default*, défini comme l'obligation pour un responsable de traitement d'appliquer les principes de protection des données à caractère personnel dès la création dudit traitement et tout au long de son développement ;
- désignation obligatoire d'un délégué à la protection des données (DPO) dans un certain nombre de cas énumérés par le règlement (traitement mis en œuvre par une autorité publique, particularités du traitement qui exigent un suivi régulier, etc.) ;
- suppression des formalités déclaratives au profit de la constitution et du suivi par le responsable du traitement et/ou le sous-traitant d'un registre des traitements mis en œuvre par ces derniers ;
- consécration d'un droit à la portabilité des données, qui permet à toute personne concernée de récupérer les données la concernant sous un format aisément réutilisable afin de les transférer ultérieurement à un tiers ;
- consécration d'un droit à l'oubli, qui permet d'obtenir du responsable du traitement l'effacement de l'ensemble des données concernant une personne, ainsi que la cessation de la diffusion de ses données ;
- renforcement de la transparence au profit des personnes concernées, ce qui se matérialise par un accroissement du nombre d'informations à transmettre et par des précisions quant aux modalités de communication ;

12 En droit français, la Cnil s'est fixé pour objectif d'impulser l'adoption d'une nouvelle loi Informatique et libertés, laquelle devra entrer en vigueur avant mai 2018. En effet, un certain nombre de dispositions deviennent désuètes ou incohérentes du fait du RGPD, qui effectue de nombreux renvois vers la législation nationale. Lors de la rédaction de ce nouveau texte, le législateur devra alors poursuivre trois objectifs :

- abroger les dispositions devenues incohérentes par rapport à celles du RGPD ;
- redéfinir certaines procédures applicables à la Cnil (exemple en matière répressive) ;
- régir les domaines au sujet desquels le RGPD renvoie au droit des Etats membres.

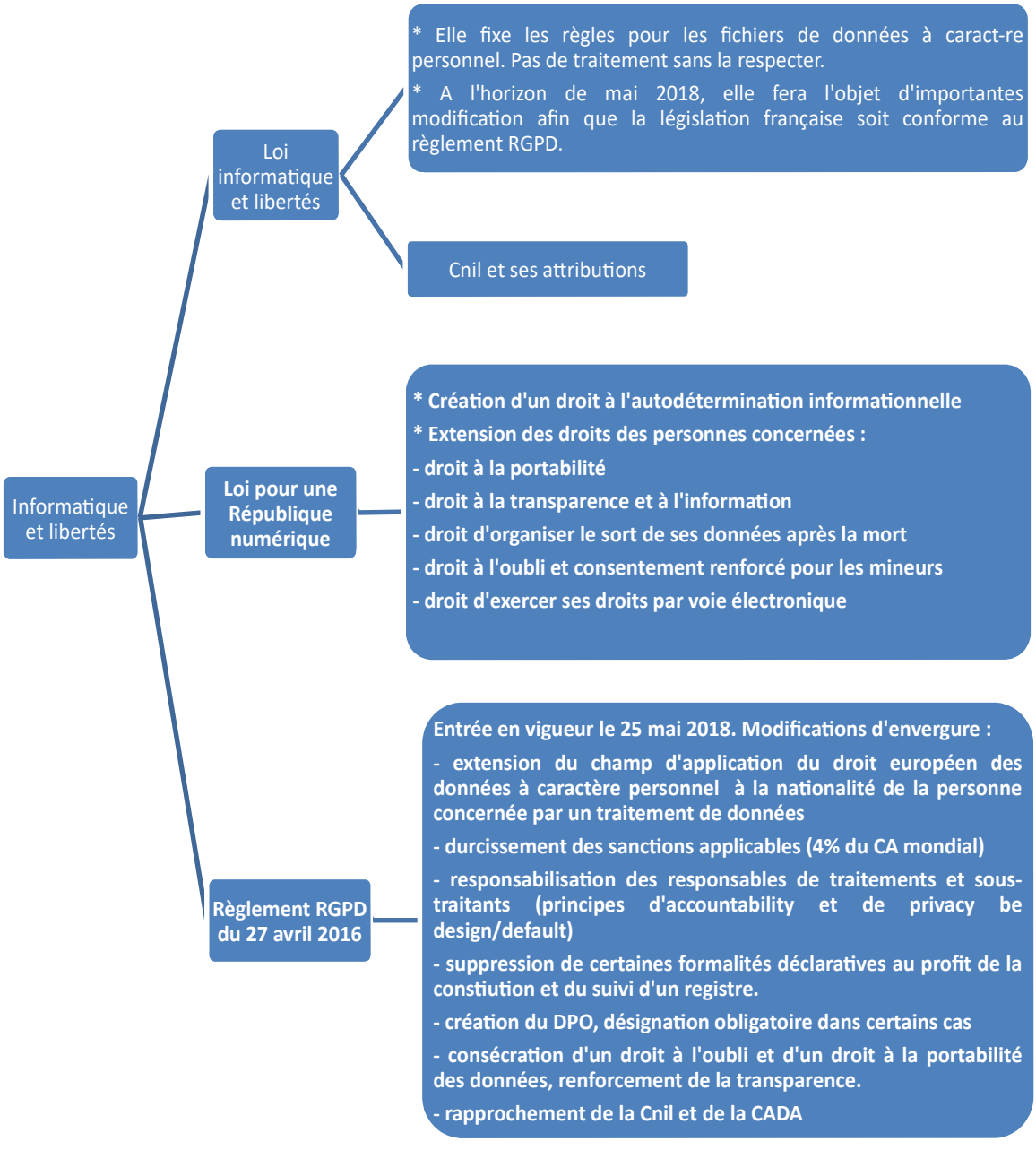
13 La loi pour une République numérique du 7 octobre 2016 a également prévu un certain nombre de dispositions relatives aux droits des personnes s'agissant de leurs données à caractère personnel. Elle consacre tout d'abord un droit à l'autodétermination

informationnelle, qui consiste en le droit pour quiconque de décider et contrôler les usages faits de ses données à caractère personnel. Elle reconnaît ainsi aux personnes :

- un droit à la portabilité de leurs données, ce qui rejoint le RGPD précité ;
- un droit d'organiser le sort de ses données à caractère personnel après sa mort ;
- un droit à l'oubli et un consentement renforcés pour les mineurs ;
- le droit de bénéficier d'une information et d'une transparence accrues ;
- la possibilité d'exercer leurs droits par voie électronique.

14 Par ailleurs, des modifications substantielles concernent la Cnil. Dans un premier temps, celle-ci est rapprochée de la CADA (Commission d'accès aux documents administratifs), avec laquelle elle peut se réunir pour former un collège unique autour de tout sujet d'intérêt commun. Dans un second temps, la Cnil voit son pouvoir de sanction précisé : la loi précitée crée une procédure accélérée en cas d'urgence et augmente le montant des sanctions pécuniaires, qui peuvent désormais atteindre 3 millions d'euros (ce qui n'a toutefois plus lieu d'être du fait du RGPD).

15 Compte tenu de ces modifications d'envergure, il convient de procéder à une modification d'ensemble de la partie Informatique et libertés du schéma :



6. Propriété littéraire et artistique

16 Deux textes ont fait évoluer la propriété littéraire et artistique au cours de l'année 2016 :

- La loi pour la liberté de création du 7 juillet 2016[6], qui dans son titre Ier consacre le principe de liberté de création artistique et incite à mener une politique en faveur de celle-ci, ne comporte pas de dispositions spécifiquement relatives au support numérique, aux créations numériques ou à Internet. Au contraire, le texte envisage la création au sens large ;

- La loi pour une République numérique susmentionnée du 7 octobre 2016 impulse quant à elle certains changements, parmi lesquels la création d'une nouvelle exception au droit d'auteur, dite de *Text Data Mining*. Elle permet d'effectuer des copies numériques à partir d'une source licite afin de consulter des textes et données de nature scientifique dans un but de recherche publique et sans finalité commerciale.

17 S'agissant de la lutte contre le téléchargement illégal, un décret du 9 mars 2017 prévoit le versement d'une compensation financière pour les fournisseurs d'accès internet (FAI) dans le cadre des activités menées en collaboration avec la Hadopi. En effet, dans cette hypothèse, les FAI prennent en charge un certain nombre de frais, parmi lesquels ceux liées à la procédure d'identification des internautes téléchargeant illégalement.

18 Les évolutions susmentionnées n'appellent pas, a priori, de modifications du schéma. Au contraire, elles concernent des points précis du droit d'auteur alors que ce dernier envisage de façon très générale la question du respect des droits d'auteur sur internet (téléchargement illégal et mesures techniques de protection).

7. Public

19 Le schéma dans sa version actuelle envisage les différents référentiels applicables au secteur public. S'il est vrai qu'aucun nouveau référentiel n'a été adopté depuis 2015, il pourrait être opportun d'ajouter au schéma une mention relative aux règles régissant les relations entre l'Administration et les administrés.

20 A En la matière, une ordonnance du 23 octobre 2015[7] et la loi pour une République numérique susmentionnée ont apporté des modifications significatives à plusieurs égards :

- ces deux textes consacrent le droit pour le citoyen de saisir l'administration en ligne. Pour ce faire, l'ordonnance précitée renforce les règles applicables aux téléservices mis en œuvre par l'administration afin de faciliter les démarches et formalités accomplies par les usagers. Le recours à un téléservice impose notamment à l'administration de délivrer à l'usager un accusé de réception électronique émis conformément au Référentiel général de sécurité.

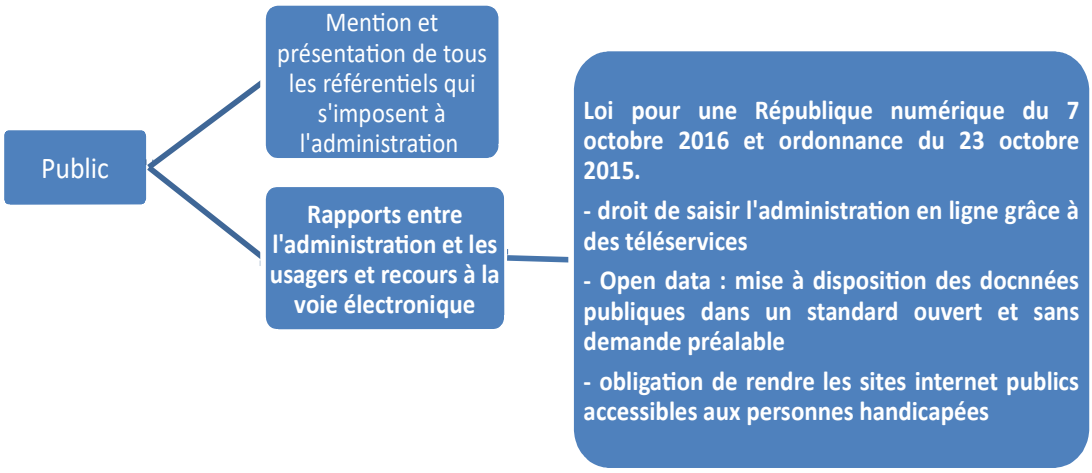
- la loi pour une République numérique prévoit une ouverture de l'accès aux données publiques (open data), soit la mise à disposition obligatoire dans un standard ouvert des documents administratifs et des données publiques qu'ils contiennent, ce indépendamment d'une quelconque demande de la part des personnes intéressées. Certains fichiers limitativement énumérés doivent ainsi systématiquement mis en ligne. Par ailleurs, la CADA est dotée par le texte de

6Loi n°2016-925 du 7 juillet 2016 relative à la liberté de la création, à l'architecture et au patrimoine
7Ordonnance n°2015-1341 du 23 octobre 2015 relative aux dispositions législatives du code des relations entre le public et l'administration

compétences accrues s'agissant du contrôle de la communication par l'administration de ses documents.

- la loi pour une République numérique a créé une obligation de rendre les sites internet publics accessibles aux personnes handicapées. Cette application vaut pour tous supports : sites internet, intranet, extranet, applications mobiles, progiciels et mobilier urbain numérique, etc. L'absence de mise en conformité à cette obligation expose les personnes concernées à une amende administrative d'un montant maximum de 5.000 euros.

21 Ces modifications exposées, il est proposé de modifier le schéma comme suit :



8. Santé

22 Le schéma envisage la question de l'hébergement des données de santé. Il importe à cet égard de mentionner la création récente du système national des données de santé, un traitement de données à caractère personnel créé par une loi du 26 janvier 2016[8] et dont les modalités ont été prévues par un décret du 26 décembre 2016[9] rendu après avis de la Cnil[10].

23 Ce fichier rassemble les bases de données déjà existantes, ce qui permettra d'effectuer diverses études médicales portant sur un nombre significatif de personnes. Ce fichier repose sur une procédure de pseudonymisation : chaque personne y est inscrite par l'intermédiaire d'un code, aucune donnée la concernant ne permettant de l'identifier. Il est accessible en permanence par certains services ou organismes publics, et sur autorisation de la Cnil pour d'autres structures. Les données y sont conservées pendant 20 ans maximum puis font l'objet d'un archivage pendant une durée de 10 ans[11].

24 Il serait opportun, compte tenu de son importance, de mentionner l'existence de ce fichier dans la partie du schéma relative à la thématique de la santé.

8Loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé
9Décret n°2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé »
10Délibération n°2016-316 du 13 octobre 2016 portant avis sur un projet de décret en Conseil d'Etat relatif au système national des données de santé (demande d'avis n°16018114)
11https://www.cnil.fr/fr/creation-du-systeme-national-des-donnees-de-sante-snds-quels-usages-avec-quelles-garanties

9. Industrie

25 Bien que de nombreuses voix s'élèvent pour dénoncer la vulnérabilité des systèmes de contrôle industriels SCADA face aux actes de piratage informatique, aucune norme récente n'a été adoptée en la matière. Par conséquent, aucune modification ne doit être apportée au schéma s'agissant de cette thématique.

10. OIV (Opérateur d'Importance Vitale)

26 Les premiers arrêtés ministériels relatifs à la sécurisation des systèmes d'OIV et pris en application des recommandations de l'ANSSI sont entrés en vigueur au 1er juillet 2016. Une seconde vague est intervenue au cours du mois d'août 2016. Outre ces derniers, la règlementation des OIV n'a pas fait l'objet d'évolutions significatives depuis la réalisation du schéma.

27 Toutefois, peut-être serait-il opportun, à des fins d'exhaustivité, de faire mention dans cette partie du schéma du Code de la défense, dans la mesure où ce dernier constitue le cadre légal de référence qui définit les OIV et les secteurs d'activité d'importance vitale.

11. Banque

28 Les évolutions législatives et règlementaires qui ont impacté le secteur bancaire depuis 2016 ne concernent pas le droit des systèmes d'information. Par conséquent, aucune modification du présent schéma n'est nécessaire s'agissant de l'encadré « banque ».

12.Défense

29 Comme pour l'OIV, aucune actualité notable ne nécessite la modification du schéma. Il serait cependant envisageable de mentionner dans l'encadré « défense » la loi de programmation militaire pour les années 2014 et 2019, qui concerne cette thématique.