Droit et SSI

Guillaume Piolle
guillaume.piolle@centralesupelec.fr
http://guillaume.piolle.fr/

CentraleSupélec – mastère Cybersécurité

15 février 2017

Plan

Les atteintes aux STAD

Atteintes aux systèmes de traitement automatisé de données (STAD)

Art. 323-1 à 323-8 du Code pénal (loi Godfrain du 5 janvier 1988, modifiés la LCENen 2004, la loi de 2012 sur la protection de l'identité, la LPM de 2013, la loi Renseignement de 2015...)

Violations de la loi informatique et libertés

Non-respect de la protection des données personnelles
5 ans de prison et 300 000 € d'amende (x5 pour les personnes morales)

Étude de 2006 (IBM/FBI) : la cybercriminalité représentait un coût annuel de 67 milliards de dollars aux États-Unis.

Étude de 2011 : 800 milliards de dollars.

Les atteintes aux STAD

Les comportements sanctionnés

- Accès/maintien frauduleux (2 ans et 60 k€, 3 ans et 100 k€ si modification) ;
- Entrave au fonctionnement (5 ans, 150 k€) ;
- Introduction/extraction/détention/transmission/suppression/modification frauduleuse de données (5 ans, 150 k€) ;
- Participation à un groupe visant à commettre ces délits, tentative de tous ces délits.

Majoration si la cible est un STA de données personnelles mis en œuvre par l'État (5-10 ans, 150-300 k€)

Peines complémentaires

Perte des droits civiques/civils/familiaux, interdiction de fonction publique ou de l'activité professionnelle visée, confiscations, fermeture d'établissements, exclusion des marchés publics, interdiction d'émettre des chèques, publication de la décision, + peines complémentaires « classiques » des personnes morales.

Atteintes aux STAD : l'exception « barbouzes »

art. 323-8 (loi sur le renseignement de 2015)

Le présent chapitre n'est pas applicable aux mesures mises en œuvre, par les agents habilités des services de l'Etat désignés par arrêté du Premier ministre parmi les services spécialisés de renseignement mentionnés à l'article L. 811-2 du code de la sécurité intérieure, pour assurer hors du territoire national la protection des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du même code.

`http://www.defense.gouv.fr/dgse/tout-le-site/nos-besoins-en-recrutement`

Atteintes aux STAD : exception sécu/recherche

art. 323-3-1 (LCEN, *modifié par la LPM en 2013)

*Le fait, sans motif légitime, **notamment de recherche ou de sécurité informatique***, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.*

Un délinquant célèbre : Kevin Mitnick

- **1979** (16 ans) : Intrusion informatique chez DEC ;
- **1980** (17 ans) : Intrusion physique dans un central téléphonique, puis détournement de lignes téléphoniques. Arrestation pour dégradation de données et vol : 3 mois en centre de redressement ;
- **1983** : Intrusion dans le réseau du Pentagone (6 mois dans un centre de détention pour jeunes) ;
- **1987** : Arrestation pour utilisation illégale de numéros de cartes téléphoniques et vol d'un logiciel (mise à l'épreuve) ;
- Trahi par son ancien complice, arrêté par le FBI (1 an de prison, 6 mois de programme anti-dépendance) ;
- **1992** : Intrusion à la Pacific Bell, nouvelle enquête du FBI, Mitnick fuit pendant deux ans et demi ;
- **1995** : Arrestation par le FBI, aidé par un ancien hacker victime de Mitnick (Shimomura), après des péripéties surmédiatisées (5 ans) ;
- Dirige actuellement la *Mitnick Security Consulting LLC*.

Un délinquant célèbre : Kevin Mitnick

Agissements confirmés

- Utilisation frauduleuse du réseau de bus de Los Angeles ;
- Obtention frauduleuse de droits admin sur un mini-ordinateur IBM du *Computer Learning Center* de L.A. pour gagner un pari ;
- Fuite face au FBI ;
- Intrusion dans les SI de DEC, Motorola, NEC, Nokia, Sun Microsystems, Fujitsu Siemens.

Agissements non confirmés mais ayant donné lieu à accusation officielle

- Vol de manuels à la Pacific Bell ;
- Lecture d'e-mails de responsables sécurité à MCI Communications et Digital ;
- Mise sur écoute du service des immatriculations de Californie ;
- Intrusion dans les SI de Santa Cruz Operation, Pacific Bell, FBI, Pentagone, University of Southern Cal., L.A. School District.

Plan

Infractions facilitées ou aggravées par l'informatique

- Atteintes aux mineurs ;
- Incitation au terrorisme, à la haine raciale, à d'autres crimes et délits ;
- Contrefaçon ;
- Escroquerie ;
- Délits de presse (injure, diffamation) ;
- ...

Usurpation d'identité : un moyen pour nuire, mais également un délit en soi (deux, même : art. 434-23 et 226-4-1 du Code pénal).

Rôle des hébergeurs et éditeurs web

Distinction entre hébergeur et éditeur

Formalisé par l'article 6 de la LCEN (2004-575), affiné par la jurisprudence.

- **Hébergeur** : mise à disposition du public de sites web (entre autres) conçus et gérés par des tiers, sans ingérence dans les contenus ;
- **Éditeur** : conception, organisation, choix éditoriaux sur les contenus publiés.

Hébergeurs et éditeurs peuvent être des personnes **physiques** ou **morales**.

Hébergeurs et éditeurs ont des niveaux de contrôle et d'implication différents sur les contenus publiés, et donc des niveaux de **responsabilité** différents.

Rôle des hébergeurs et éditeurs web

Éditeur de site web

Du fait de son rôle éditorial sur les contenus, il est normalement responsable, civilement et pénalement, de tous les contenus publiés sous son contrôle.
Obligation de mentions légales (art. 6, III-1) : objectif d'affichage de la responsabilité éditoriale et d'un moyen de contact physique (vers l'hébergeur pour les personnes physiques non professionnelles).

Et les commentaires ?

- Modérés a priori : l'éditeur est supposé avoir connaissance, et donc être responsable, de leur contenu ;
- Non modérés a priori : la responsabilité de l'éditeur ne peut être engagée qu'à partir du moment où un commentaire est directement porté à sa connaissance.

Moralité : modérez toujours a posteriori !

Rôle des hébergeurs et éditeurs web

Hébergeur de site web

Lié par le secret professionnel en ce qui concerne les informations d'identification de leurs clients (anonymat des éditeurs personnes physiques non professionnelles).

Responsabilités pénale et civile limitées : engagées uniquement à partir du moment où l'hébergeur a connaisance de données illicites et qu'il n'agit pas « promptement pour retirer ces données ou en rendre l'accès impossible ».

Absence explicite d'obligation de surveillance ou de recherche des activités illicites.

$\rightarrow$ grands efforts des acteurs du web pour être qualifiés d'hébergeurs plutôt que d'éditeurs en cas de procédure judiciaire.

Problème de la qualification pénale des contenus, dont l'hébergeur devient de fait responsable à la place du juge (cf. OVH/Wikileaks).

Rôle des hébergeurs et éditeurs web

Le droit de réponse

Introduit dans la loi de 1881 sur la liberté de la presse
Application confirmée pour tout site web dans l'article 6-IV de la LCEN (délai de trois mois à compter de la publication), réponse dans les trois jours, exclusion des zones éditables directement par les visiteurs.

Contenus manifestement illicites

Ils peuvent être signalés pour retrait.
Si le contenu n'est pas manifestement illicite, l'hébergeur ou l'éditeur doit refuser la demande pour préserver la liberté d'expression.
Le signalement abusif est sanctionné (1 an, 15 k€).

Procédures

Les demandes sont adressées à l'éditeur s'il n'est pas anonyme, sinon à l'hébergeur (qui est normalement connu et qui doit mettre en place un mécanisme de signalement). **Et sinon ?**

Auditabilité et journalisation

Obligations de journalisation

- 2001, Loi sur la Sécurité Quotidienne (LSQ) : les opérateurs télécom doivent conserver les données de connexion pendant un an (mesure temporaire, prolongée *ad vitam*) ;
- 2004, Loi sur la Confiance dans l'Économie Numérique (LCEN) : conservation des informations identifiant les personnes déposant des contenus en ligne (étendu à tous les fournisseurs d'accès) ;
- 2011, décret d'application de la LCEN : conservation des identifiants, peudonymes, mots de passe, données de paiement, coordonnées (étendu aux hébergeurs et éditeurs de sites web) ;
- Loi sur le Renseignement du 24 juillet 2015 : instauration des « boîtes noires » chez les opérateurs télécom par les services de renseignement.

En cas de journalisation insuffisante ?

[pas forcément à jour] Jusqu'à 375 k€ d'amende pour une société, 75 k€ et un an d'emprisonnement pour son dirigeant.

Auditabilité et journalisation

Qui peut accéder aux journaux ?

- La justice (commission rogatoire, décision en référé ou en instance) ;
- La police, sur réquisition simple (sans autorisation judiciaire), depuis la loi du 23 janvier 2006 sur la lutte contre le terrorisme ;
- Pour les opérateurs télécom : accès administratif (aucun contrôle judiciaire) par les agents de plusieurs ministères (LPM du 18 décembre 2013), services de renseignement (loi Renseignement de 2015) ;
- L'administrateur système/réseau, qui « est tenu d'une **obligation de confidentialité** » (même vis-à-vis de l'employeur, en tout cas en ce qui concerne les e-mails) et peut accéder aux données « dans le cadre de sa mission de sécurité du réseau informatique » (Cour de Cassation, 17 juin 2009).

Un risque opérationnel aggravé ?

À des fins de sécurité (lutte contre le terrorisme), on augmente le risque de dommages en cas d'intrusion et on fournit une incitation aux attaquants éventuels. *[Déportez la journalisation !]*

Conservation : vers une évolution au niveau européen ?

La Cour de Justice de l'Union Européenne (CJUE) a par deux fois posé des limites fortes aux obligations de conservation des données à des fins de sécurité publique.

Arrêt *Digital Rights Ireland Ltd*, 8 avril 2014

La CJUE **invalide la directive 2006/24/CE** sur la conservation des données :

> *Force est donc de constater que cette directive comporte une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire.*

Conservation : vers une évolution au niveau européen ?

Quelles conséquences pour la législation des États membres ?

Dans plusieurs pays (Autriche, Belgique, Bulgarie, Roumanie, Pays-Bas, Slovénie), les textes pris en application de la directive sont jugés invalides, inconstitutionnels ou en violation de la Charte des droits fondamentaux.

En France, le gouvernement considère que la législation, antérieure à la directive, n'est pas impactée par la décision de la CJUE.

Des recours en justice ont été tentés devant le Conseil d'État contre certains textes en particulier (LPM et décrets d'application, notamment), sans grand succès.

La législation française est-elle ou non conforme sur ce point au droit de l'Union ?

Pas très clair. . . En 2014, la section des études du Conseil d'État considérait qu'un encadrement plus clair de cette législation était nécessaire (et la section contentieux a visiblement considéré que la LPM jouait efficacement ce rôle).

Conservation : vers une évolution au niveau européen ?

Arrêt *Tele2 Sverige AB*, 21 décembre 2016

La CJUE, dans le contexte de l'application de la directive 2002/58/CE, considère qu'une législation nationale ne peut imposer une conservation **générale** des données (i.e. sans se limiter à des suspects de crimes graves, sous le contrôle d'une autorité judiciaire).

> *Eu égard à la gravité de l'ingérence dans les droits fondamentaux en cause que constitue une réglementation nationale prévoyant, aux fins de la lutte contre la criminalité, la conservation de données relatives au trafic et de données de localisation, seule la lutte contre la criminalité grave est susceptible de justifier une telle mesure.*

La législation française est-elle ou non conforme sur ce point au droit de l'Union ?

Probablement pas, mais il est probable que l'arrêt sera interprété de manière restrictive (uniquement pour les textes de transposition de la directive 02/58).

Plan

Recherche et divulgation de vulnérabilités

Une activité utile

Objectif : identifier les défauts de logiciels, de sites web. . . , prévenir les responsables et les cibles potentielles (utilisateurs) de sorte que les vulnérabilités soient comblées.

Problème

On alerte aussi les méchants pirates !

Recherche et divulgation de vulnérabilités

Stratégies de diffusion

- *Full disclosure* : publication immédiate et complète de la vulnérabilité ou de l'exploit ;
- *Responsible (limited) disclosure* : alerte de l'éditeur (avec les infos complètes), puis après correction ou après un certain délai, publication.

Variantes du *responsible disclosure* : publication d'une preuve d'exploit sans publier l'exploit ou la vulnérabilité eux-mêmes, « vente » de la vulnérabilité à l'éditeur.

Pourquoi le *Full Disclosure* peut faire « tiquer » : exemple

2011 : publication d'un chercheur français en sécurité informatique sur une vulnérabilité du réseau Tor, en prévenant les responsables à l'avance mais en refusant de donner les éléments techniques « en primeur ».

Problème : le réseau Tor est un mécanisme d'anonoymisation des connexions auquel certaines personnes (opposants politiques et dissidents dans les régimes totalitaires) confient leur sécurité physique.

En l'espèce l'attaque n'était pas facilement exploitable par n'importe qui, mais la question de fond de la responsabilité du chercheur dans ce type de cas demeure...

Même le *responsible disclosure* peut être risqué pour le chercheur !

L'affaire Kitetoa

- Kitetoa observe qu'en utilisant un simple navigateur, on peut accéder à des données confidentielles du site Tati.fr ;
- 13 février 2002 : Kitetoa est condamné pour accès frauduleux (amende limitée à 1000 €) ;
- 30 novembre 2002 : Relaxe en appel. L'avocate de Tati reconnaît que Kitetoa a fait « un travail de service public » mais demande sa condamnation quand même...

Même le *responsible disclosure* peut être risqué pour le chercheur !

Kitetoa : réquisitoire du parquet général de la Cour d'Appel de Paris

« Il semble inenvisageable d'instaurer une jurisprudence répressive dont il résulterait une véritable insécurité permanente, juridique et judiciaire, pour les internautes, certes avisés, mais de bonne foi, qui découvrent les failles de systèmes informatiques manifestement non sécurisés. »

Le parquet considère que l'infraction du prestataire de Tati.fr (défaut de sécurisation d'une base contenant des données personnelles) est plus grave que ce qui est reproché à Kitetoa. **Pourquoi pas de poursuites alors ?**

Responsible disclosure, suite : l'affaire Zataz

- Septembre 2008 : Damien Bancal (éditeur de Zataz.com) informe la société *Forever Living Products* d'une faille (serveur FTP acceptant les connexions anonymes). FLP corrige et **remercie** Damien Bancal ;
- Fin 2008 : D. Bancal publie un article sur la faille, sans divulguer de données confidentielles et en précisant qu'elle est corrigée ;
- 24 décembre 2008 : FLP l'assigne en justice au pénal (diffamation) et au civil (retrait de l'article) ;
- D. Bancal perd au civil en première instance (relaxe au pénal). Cependant, sa bonne foi est reconnue, ainsi que le caractère responsable de sa démarche. D. Bancal fait appel aux dons pour financer la procédure et reçoit beaucoup de soutien ;
- Les deux parties interjettent appel. Le retrait de l'article est confirmé mais FLP se désiste au pénal et s'engage à ne pas réclamer les sommes octroyées.

Coût de la procédure pour Damien Bancal : 14 196,21 €

« Affaire » Bluetouff

Septembre 2012 : O. Laurelli, alias *Bluetouff*, télécharge des documents sur le site de l'Anses (Agence nationale de sécuité sanitaire de l'alimentation, de l'environnement et du travail, OIV), qui considère qu'il y a intrusion et porte plainte après la mise en ligne d'un des documents (destiné à un usage interne).

Erreur de paramétrage du serveur : tous ces fichiers étaient accessibles en lecture.

Utilisation de deux VPN (une IP en Suède et une au Panama, pour un service de VPN publiquement opéré par le prévenu). Non retenu contre lui.
« recherche complexe » (`filetype:pdf...`) sur Google, arrive par erreur sur l'extranet, parcours de l'arborescence, constate la présence d'une authentification (inopérante donc).

« Affaire » Bluetouff

Relaxe en première instance

*Compte tenu de l'ensemble de ces éléments, même s'**il n'est pas nécessaire pour que l'infraction existe que l'accès soit limité par un dispositif de protection**, le maître du système, l'Anses, en raison de la défaillance technique, n'a pas manifesté clairement l'intention de restreindre l'accès aux données récupérées par Monsieur Olivier L. aux seules personnes autorisées.*
*Monsieur Olivier L. **a pu donc légitimement penser** que certaines données sur le site nécessitaient un code d'accès et un mot de passe mais **que les données informatiques qu'il a récupérées étaient en libre accès** et qu'il pouvait parfaitement se maintenir dans le système.*

+ Refus de retenir la qualification de *vol* de données, à cause de la non-rivalité de l'information (c'était avant l'introduction de la notion d'extraction dans 323-3).

« Affaire » Bluetouff

Appel (5 février 2014) : 3 000 € d'amende

La cour considère qu'il a *constaté la présence de contrôles d'accès et la nécessité d'une authentification par identifiant et mot de passe* et retient les chefs de *maintien frauduleux* et de *vol* de fichiers informatiques.

Cassation (20 mai 2015)

Rejet du pourvoi, le raisonnement de la cour d'appel est confirmé, y compris en ce qui concerne la qualification du vol de données. À défaut d'une qualification vraiment appropriée ? La notion d'*extraction* introduite depuis semble mieux adaptée.

Attention aux fantasmes...

On m'a dit qu'avec la LPM, on pouvait librement tester la sécurité d'un site web ?

C'est vrai si vous considérez, avec certains juristes en mal de sensationnalisme (ou de clients), qu'en ayant légitimement accès à un site web vous avez « le droit d'utiliser le logiciel » qui le fait tourner, ce qui vous donne le droit de « l'observer, de l'étudier ou de tester son fonctionnement ou sa sécurité », et que vous considérez que cette disposition vous autorise implicitement à le faire sur un site en prod que vous ne contrôlez pas (plutôt que de tester ce logiciel chez vous).

La LPM ne change rien : c'est le responsable du site web (le « maître du système » qui peut tester sa sécurité.

Attention aux fantasmes...

Ce que dit le CPI sur la rétro-ingénierie (art. L122-6-1 III. du Code de la Propriété intellectuelle)

La personne ayant le droit d'utiliser le logiciel peut sans l'autorisation de l'auteur ***observer***, ***étudier*** *ou* ***tester le fonctionnement ou la sécurité*** *de ce logiciel afin de déterminer les idées et principes qui sont à la base de n'importe quel élément du logiciel lorsqu'elle effectue toute opération de chargement, d'affichage, d'exécution, de transmission ou de stockage du logiciel qu'elle est en droit d'effectuer.*

+ Possibilité de reproduire le code ou de « traduire sa forme » (décompilation, désassemblage, etc.) aux seules fins d'interopérabilité (même pas pour la recherche ou l'évaluation de la sécurité).

La procédure de déclaration au CERT de l'ANSSI

Code de la défense, art. L2321-4 (loi « République numérique » de 2016, art. 47)

Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données.

L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée.

L'autorité peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace mentionnés au premier alinéa du présent article aux fins d'avertir l'hébergeur, l'opérateur ou le responsable du système d'information.

C'est quoi cet article 40 du CPP ?

L'obligation faite aux agents publics de signaler délits et crimes au procureur. . .

La procédure de déclaration au CERT de l'ANSSI

NB : on a échappé à pire, une version antérieure du texte prévoyait, pour le chercheur signalant une vulnérabilité, une **dispense de peine**...

Interface de signalement

`https://www.ssi.gouv.fr/en-cas-dincident/vous-souhaitez-declarer-une-faille-de-securite-ou-une-vulnerabilite/`

Et sur quoi va se fonder l'ANSSI pour juger si elle estime le chercheur « de bonne foi » ou pas ? Pourquoi ne pas avoir simplement demandé une absence d'intention de nuire ?

À quel point est-ce juridiquement risqué pour un chercheur de signaler une vulnérabilité à l'ANSSI ?

Cette procédure pourrait amener à préférer la valorisation dans le cadre d'un programme de *bug bounty* ou un signalement complètement anonyme.

Plan

Administrateurs

Une préoccupation constante

Possibles conflits entre impératifs de sécurité et obligations relatives à la vie privée.

Besoin d'auditabilité

Un impératif de la sécurité informatique : se donner les moyens de détecter les comportements malveillants ou erronés et de désigner les responsables.

Outil : conservation de **journaux** (logs) retraçant l'activité d'un système (logiciel, serveur web, etc.).

Huissiers de justice

Profession réglementée d'auxiliaire de justice, formation initiale exclusivement juridique.
Composante essentielle du métier : le **serment**, qui rend les déclarations et constatations de l'huissier incontestables.

Nombreuses missions

- Communication entre les parties (sommations de payer) ;
- Délivrance d'actes (assignations, citations, significations) ;
- Exécution des décisions de justice (injonctions, saisies. . .) ;
- **Établissement de constats**.

Peut constater, à la demande d'une partie, la présence d'un document ou d'une information sur un site web, un ordinateur, un smartphone (incluant notamment SMS, e-mails, tweets, etc.)

Collabore avec des **experts** lorsque cela est nécessaire.

Experts judiciaires

À la frontière entre deux mondes

L'expert est mandaté par un juge pour étudier un cas et remettre aux parties un rapport, dont le juge peut suivre ou non la conclusion.

- Expert dans son domaine d'activité (informatique ou autre) ;
- Formé à la procédure judiciaire et aux aspects du droit le concernant.

Serment de l'expert judiciaire

Je jure, d'apporter mon concours à la Justice, d'accomplir ma mission, de faire mon rapport, et de donner mon avis en mon honneur et ma conscience.

Les experts judiciaires sont attachés à une cour d'appel (ou à la Cour de cassation).

Les parties sont également libres de faire appel à des experts non inscrits, à leurs frais.

Experts judiciaires

L'expertise judiciaire au civil

L'expert peut être mandaté pour :

- Entendre les dires « techniques » des parties ;
- Effectuer des investigations sur les SI pour établir certains faits ;
- Évaluer des préjudices...

L'expertise judiciaire au pénal

L'expert est généralement mandaté pour explorer un support à la recherche d'informations sur une activité ou des relations, ou bien de documents constitutifs d'un délit/crime particulier.

Indirectement, l'expert peut être amené à participer à la qualification et à l'investigation, même si ce n'est pas à l'origine dans ses attributions.

Une partie significative des missions concerne la pédopornographie...

Tiers de confiance

Définition « informatique » d'un composant « de confiance »

Si un composant est dit « de confiance », c'est qu'il a la capacité de violer les règles. La sécurité du système repose donc sur la **confiance** que l'on a dans ce composant.

Tiers de confiance

Un tiers de confiance est une personne à qui l'on donne suffisamment d'informations pour qu'elle puisse causer des dommages si elle en faisait un usage illégitime. La sécurité d'un protocole repose sur la confiance que l'on peut avoir dans ce tiers, qui doit donc être **neutre** (non intéressé).

Tiers de confiance

Types de tiers de confiance

- PSCE : prestataire de services de certification électronique (tiers certificateur) ;
- PSHE : prestataire de services d'horodatage électronique (tiers horodateur) ;
- Tiers d'archivage ;
- Tiers de télétransmission ;
- ...

Les intermédiaires bancaires peuvent également être considérés comme des tiers de confiance suivant les applications.

Cadre juridique pour certaines de ces activités, référentiels sous forme de normes, de labels...

Auditabilité et preuve électronique

Problématiques

- Comment concevoir des systèmes d'information « expertise-friendly » ou « audit-friendly » ?
- Comment concevoir des SI ne nécessitant pas d'expertise ?
- Comment faciliter les attributions de responsabilités en cas de problème ?
- Comment concevoir des systèmes de journalisation suffisamment fiables pour la constitution automatique de preuve ?

Plan

Les différentes facettes de la propriété intellectuelle

- **Propriété littéraire et artistique :**
  - Droit d'auteur ;
  - Droits voisins ;
  - Droits des producteurs de bases de données ;
- **Propriété industrielle :**
  - Dessins et modèles ;
  - Brevets (+ COV, CCP...) ;
  - Marques.

Textes de référence

Code de la Propriété Intellectuelle (CPI, 1995)

Principes du droit d'auteur

Les œuvres protégées

Le droit d'auteur protège les **œuvres de l'esprit** qui sont des créations de **forme originale**.

Sources : art. L111-1 du Code de la Propriété Intellectuelle (CPI), jurisprudence, doctrine.

La forme

- L'œuvre doit avoir pris forme, être sortie de l'esprit de son concepteur ;
- Seule sa forme, sa représentation particulière sont protégées.

Les idées et les informations ne sont pas protégeables.

L'originalité

L'œuvre doit porter « l'empreinte de la personnalité de son auteur ».

Principes du droit d'auteur

Critères indifférents

- **Genre** (œuvres littéraires, picturales, musicales, audiovisuelles, spectacle vivant...) ;
- **Forme d'expression** (fixation ou non, sur n'importe quel support) ;
- **Mérite** (caractère « artistique » de l'œuvre, qualité).

Principes du droit d'auteur

Détail des droits

Droits moraux (incessibles, inaliénables, imprescriptibles) :

- Droit de paternité ;
- Droit de divulgation ;
- Droit au respect de l'œuvre ;
- Droit de repentir ou de retrait.

Droits patrimoniaux (70 ans *post mortem auctoris*) :

- Droit de représentation ;
- Droit de reproduction ;
- Droit de suite.

Nombreuses exceptions et limitations à ces droits.

Principes du droit d'auteur

Dispositions pénales : L335-2

Toute édition d'écrits, de composition musicale, de dessin, de peinture ou de toute autre production, imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une ***contrefaçon*** *et toute contrefaçon est un délit.*

La contrefaçon en France d'ouvrages publiés en France ou à l'étranger est punie de ***trois ans d'emprisonnement et de 300 000 € d'amende****.*

Seront punis des mêmes peines le débit, l'exportation et l'importation des ouvrages contrefaisants.

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 € d'amende.

Application du droit d'auteur à l'informatique

Un nouveau territoire de protection

Dans les années 80 s'est posée la question de la protection du logiciel. En France, il a été estimé que le droit d'auteur couvrait ce domaine (parce que non limité en termes de genre et de forme d'expression).

Par défaut, le logiciel est protégé par le droit d'auteur (ou par le *copyright* dans les pays correspondants).

Limitations

Attention : ce type de protection est limité par la nature même du droit d'auteur. On ne protège que des **œuvres de l'esprit** en ce qu'elles sont des créations de **forme originale**.

Application du droit d'auteur à l'informatique

Aspects protégés

- La **forme programmée** ;
- La **documentation** ;

pour peu qu'elles soient originales.
Les **éléments audiovisuels** sont protégés à part.

Aspects non protégés

- Les fonctionnalités ;
- L'utilisation d'un langage de programmation donné ;
- Les formats de fichiers utilisés.

cf. Décision de la CJUE du 02/05/2012

Application du droit d'auteur à l'informatique

Titularité des droits

Le droit d'auteur, pour le logiciel comme dans les autres domaines, naît sur la tête des **personnes physiques**.
Hors logiciel, il n'y a pas de transfert de propriété automatique vers l'employeur (sauf exceptions bien sûr, notamment pour les agents publics).

Cas spécifique du logiciel :

- Si l'auteur est un employé (y compris agent de l'État) agissant dans l'exercice de ses fonctions ou sur les directives de son employeur, les droits patrimoniaux sont transférés à ce dernier (L113-9) (en gros, l'auteur a juste le droit d'être mentionné comme tel) ;
- En cas de cession de droits (et sauf disposition contraire plus favorable à l'auteur), l'auteur ne peut s'opposer à une modification du logiciel par le cessionnaire, ni exercer son droit de repentir ou de retrait (L121-7).

Les licences logicielles

Notion de licence logicielle

Notion de droit U.S., inexistante en droit français : autorisation d'utiliser un bien.
Idée : on concède une **licence d'exploitation** d'un logiciel, qui fixe les conditions dans lesquelles il peut être utilisé (mécanique d'adhésion).

Possibilités standard d'interprétation en droit français :

- Cessions de droits (mais. . .) ;
- Contrats (mais. . .).

(La base restant une protection par le droit d'auteur)

EULA = *End User License Agreement*

Les licences logicielles

Les trois grands types de licences

- Licences propriétaires ou privatrices ;
- Licences de libre diffusion ;
- Licences libres.

Une licence peut être concédée à titre gratuite ou onéreux.

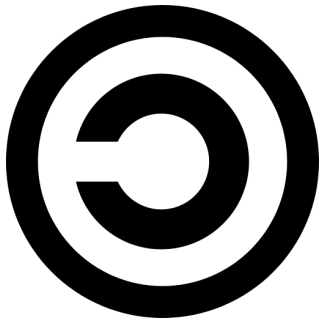
Les licences logicielles

Licences libres

Une licence libre confère quatre droits à toute personne, sans restriction (critère de la *Free Software Foundation*) :

- Droit d'**utiliser** l'œuvre pour tout usage (y compris commercial) ;
- Droit d'**étudier** l'œuvre (accès au code source) ;
- Droit de **redistribuer** des copies de l'œuvre ;
- Droit de **modifier** l'œuvre et de publier ses modifications.

Copyleft et licences contaminantes

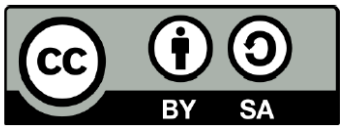


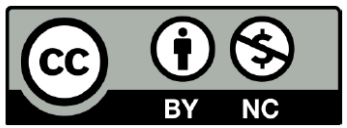
- **Licence libre non-copyleft** : les œuvres dérivées ne sont pas nécessairement sous licence libre (BSD, X11) ;
- **Copyleft simple** : les œuvres dérivées doivent être publiées sous une licence libre identique ou compatible (LGPL) ;
- **Copyleft fort** (licences « virales » ou « contaminantes ») : les œuvres dérivées ainsi que tous les composants associés doivent être publiés sous une licence libre identique ou compatible (GPL, CeCILL).

Licences Creative Commons

Composition d'une licence de base (CC-0, *Creative Commons Zero*) et de « modules » élémentaires :

- BY : Attribution ;
- SA : Share-Alike, redistribution à l'identique (copyleft) ;
- NC : Pas d'usage commercial (non libre) ;
- ND : Pas d'œuvres dérivées (non libre) ;





Le droit *sui generis* des bases de données

- Protection des **éléments de contenu** : tout l'arsenal de la PI ;
- Protection de la **base de données, indépendante :**
  - Droit d'auteur sur la forme de la base (notamment le caractère original de son indexation) ;
  - Droit *sui generis* (droit voisin du droit d'auteur) sur le contenu dans sa globalité.

Le droit *sui generis* des bases de données

Condition d'éligibilité pour la protection *sui generis*

La constitution de la base doit avoir fait l'objet d'un « investissement financier, matériel ou humain substantiel » (L341-1).

Effets de la protection *sui generis*

Le producteur peut interdire l'extraction et la réutilisation d'une partie « qualitativement ou quantitativement substantielle » du contenu de la base (L342-1).

Exceptions lorsque la base est mise à disposition du public (L342-3).

Le brevet d'invention

- Protège une **réalisation technique** (toujours pas une idée) présentant trois caractères :
  - Nouveauté ;
  - Inventivité ;
  - Applicabilité industrielle.
- Payant (dépôt et renouvellement), nécessite des formalités ;
- Limité en durée (généralement 20 ans) et en territoire ;
- Instaure un monopole d'exploitation de l'invention (fabrication, utilisation, importation, vente) ;
- Possible concession de licences d'exploitation (notion de *royalties*).

Question brûlante

Le brevet est-il adapté à la protection du logiciel ? En Europe : pas « en tant que tels », il faut qu'ils « puissent produire un effet technique » (association avec un autre système).

Sources et références

- Xavier Berne, *La CJUE s'oppose à l'obligation généralisée de conservation des données de connexion*, NextInpact, 21 décembre 2016 (`https://www.nextinpact.com/news/102607-la-cjue-s-oppose-a-obligation-generalisee-conservation-donnees-connexion.htm`) ;
- Guillaume Champeau, *L'arrêt Bluetouff de la cour d'appel de Paris*, Numerama, 7 février 2014 (`http://www.numerama.com/magazine/28335-l-arret-bluetouff-de-la-cour-d-appel-de-paris.html`) ;
- Cour de Cassation, chambre criminelle, *Arrêt 14-81.336 du 20 mai 2015* (`https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000030635061`) ;
- Cour de Justice de l'Union Européenne, *Arrêt de la Cour (grande chambre) du 8 avril 2014* (`http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=FR`) ;
- Cour de Justice de l'Union Européenne, *Arrêt de la Cour (grande chambre) du 21 décembre 2016* (`http://curia.europa.eu/juris/document/document.jsf?doclang=FR&docid=186492`) ;
- Aude Fredouelle, *Loi renseignement : « Accéder aux données de connexion nécessite de reconstituer le contenu du message »*, Journal du Net, 5 mai 2015 (`http://www.journaldunet.com/ebusiness/le-net/projet-de-loi-renseignement.shtml`) ;

Sources et références

- Legalis, *Pas d'accès frauduleux à un système non sécurisé : le prévenu est relaxé*, 22 mai 2013 (https://www.legalis.net/actualite/pas-dacces-frauduleux-a-un-systeme-non-securise-le-prevenu-est-relaxe/) ;
- Roseline Letteron, *L'accès administratif aux données de connexion*, Contrepoints, 30 juillet 2015 (https://www.contrepoints.org/2015/07/30/216153-lacces-administratif-aux-donnees-de-connexion) ;
- La Quadrature du Net, *Conservation des données : le Conseil d'État osera-t-il défier la CJUE ?*, 10 février 2016 (https://www.laquadrature.net/fr/conservation-donnees-conseil-etat) ;
- La Quadrature du Net, *Conservation des données : un coup porté à la surveillance de masse !*, 22 décembre 2016 (http://www.laquadrature.net/fr/allo-conseil-detat) ;
- Marc Rees, *Renseignement : pourquoi le Conseil d'État a sacralisé l'accès aux données de connexion*, NextInpact, 12 février 2016 (https://www.nextinpact.com/news/98491-renseignement-pourquoi-conseil-detat-a-sacralise-acces-aux-donnees-connexion.htm) ;
- Tribunal de Grande instance de Créteil, 11ème chambre correctionnelle, *Jugement du 23 avril 2013*, sur Legalis (https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-creteil-11eme-chambre-correctionnelle-jugement-du-23-avril-2013/).