Aspects juridiques de l'informatique

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

Supélec, équipe CIDre

ENS Cachan, antenne de Bretagne – Académie de Rennes
12 mars 2013

Avertissement

IANAL

I Am Not A Lawyer

Protection des données personnelles

Ce qui est privé est-il honteux ?

> *Si vous n'avez rien à vous reprocher, alors vous n'avez rien à cacher.*

Ce qui est privé est-il honteux ?

Si vous n'avez rien à vous reprocher, alors vous n'avez rien à cacher.

- Mais alors, pourquoi utiliser une enveloppe lorsque vous envoyez une lettre ?
- Ce n'est pas parce que vous n'avez « rien à cacher » que rien ne pourra vous être reproché ou que rien ne pourra vous blesser.

Ce qui est privé est-il honteux ?

Si vous n'avez rien à vous reprocher, alors vous n'avez rien à cacher.

- Mais alors, pourquoi utiliser une enveloppe lorsque vous envoyez une lettre ?
- Ce n'est pas parce que vous n'avez « rien à cacher » que rien ne pourra vous être reproché ou que rien ne pourra vous blesser.

Ce genre de déclaration est habituellement faite par un membre d'une « caste dominante » : un homme, blanc, hétérosexuel, si possible de plus de 45 ans.

Un exemple de risque : la brèche de vie privée

Formes principales

- Intrusion d'une personne dans vos affaires « privées » ;
- Révélation au public ou à un tiers d'une information « privée » que vous n'étiez pas prêt(e) à divulguer, et/ou qui est fausse ;
- Vol d'identité.

Un exemple de risque : la brèche de vie privée

Formes principales

- Intrusion d'une personne dans vos affaires « privées » ;
- Révélation au public ou à un tiers d'une information « privée » que vous n'étiez pas prêt(e) à divulguer, et/ou qui est fausse ;
- Vol d'identité.

Conséquences possibles

- Impact (plus ou moins grave) sur les relations sociales ;
- Risque de discrimination ;
- Risque de poursuites pénales ;
- ...

Un exemple de risque : la brèche de vie privée

Formes principales

- Intrusion d'une personne dans vos affaires « privées » ;
- Révélation au public ou à un tiers d'une information « privée » que vous n'étiez pas prêt(e) à divulguer, et/ou qui est fausse ;
- Vol d'identité.

Conséquences possibles

- Impact (plus ou moins grave) sur les relations sociales ;
- Risque de discrimination ;
- Risque de poursuites pénales ;
- ...

Et les personnes « publiques » ?

Les risques : Le vol d'identité

Symptômes (`identitytheft.org.uk`)

- Perte de papiers d'identité ;
- Les courriers (banque notamment) ne vous parviennent plus ;
- Opérations bancaires inhabituelles ;
- On vous informe que vous avez fait une demande de prêt, d'aide sociale ou gouvernementale ;
- Vous recevez des factures, injonctions de payer ou mises en demeures pour des biens ou services dont vous n'avez pas connaissance ;
- On vous refuse un crédit alors que vous avez un bon dossier ;
- Un contrat de téléphonie mobile a été souscrit en votre nom ;
- Vous êtes contactés par des organismes bancaires avec lesquels vous n'avez pas de contacts habituellement ;
- ...

La vie privée : une notion liée à la culture

En France

Droit fondamental, et même « fondamental fondamental », condition nécessaire à l'exercice des autres droits fondamentaux.
Dans le bloc constitutionnel depuis 1971.
Rôle central de l'État comme garant de ce droit.

La vie privée : une notion liée à la culture

En France

Droit fondamental, et même « fondamental fondamental », condition nécessaire à l'exercice des autres droits fondamentaux.
Dans le bloc constitutionnel depuis 1971.
Rôle central de l'État comme garant de ce droit.

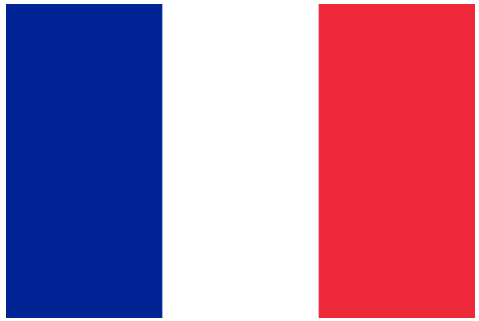
Aux États-Unis

Ne peut entrer en conflit avec la liberté d'expression, juridiquement supérieure (premier amendement).
Défiance envers l'État.
Rôle central du marché, de la libre entreprise.

Contexte international

- **ONU :**
  - 1948 - Déclaration universelle des droits de l'homme (art. 12) ;
  - 1966-1980 : Pactes à force contraignante (droits civils et politiques, droits économiques, sociaux et culturels).
- **Conseil de l'Europe :**
  - 1950 - Convention de sauvegarde des droits de l'homme et des libertés fondamentales (art. 8) ;
  - 1981 - **Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel** (en particulier préambule, art. 5).
- **Union européenne :**
  - 1992-2007 - Traité de l'Union européenne (inclut la CSDHLF) ;
  - 2000-2010 - Charte des droits fondamentaux de l'Union européenne ;
  - 1995 : **Directive 95/46/CE**
  - 2002 : Directive 2002/58/CE
  - ? - Projet de réglement européen en remplacement de 95/46.

Contexte national en France



- **Code civil**, article 9 ;
- **Loi n° 78-17 du 6 janvier 1978** relative à l'informatique, aux fichiers et aux libertés ;
- **Loi n° 2004-801 du 6 août 2004** relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

`http://www.legifrance.gouv.fr/`

Droit à la vie privée *vs* Protection des données personnelles

Droit à la vie privée

Droit « correctif »

Notion de préjudice et de réparation

Il faut démontrer le préjudice

Droit à la vie privée *vs* Protection des données personnelles

Droit à la vie privée

Droit « correctif »
Notion de préjudice et de réparation
Il faut démontrer le préjudice

Protection des données personnelles

Droit « préventif »
Règles visant à éviter les violations de la vie privée
La violation des règles constitue un préjudice en soi, par principe

Informatique et Libertés : Périmètre

Article 2 (extrait)

La présente loi s'applique aux **traitements automatisés de données à caractère personnel**, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles [...].

La loi Informatique et Libertés instaure la CNIL et crée (en 2004) les CIL (Correspondants Informatique et Libertés, futurs « délégués à la protection des données »).

Infractions à la loi Informatique et Libertés

délits sanctionnés de 5 ans de prison et 300 000 € d'amende ($\times$ 5 pour les personnes morales)

Informatique et Libertés : Périmètre

Donnée à caractère personnel (donnée personnelle)

Suite de l'article 2 :

Constitue une donnée à caractère personnel **toute information relative à une personne physique identifiée ou qui peut être identifiée**, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer **l'ensemble des moyens** en vue de permettre son identification dont dispose ou auxquels peut avoir accès **le responsable du traitement ou toute autre personne**.

Avant 2004 (cf directive 95/46), on parle d'*informations nominatives* ou *indirectement nominatives*.

Informatique et Libertés : Principes

- **Principe de légalité :** Les traitements sur certains types de données sont interdits (voir plus loin) ;
- **Principe de finalité :** On collecte des données en vue d'une finalité déterminée, et qui doit être respectée ;
- **Principe de légitimité :** La finalité poursuivie doit être légitime pour le responsable du traitement ;
- **Principe de proportionnalité :** La collecte doit être proportionnelle (nature, quantité et durée de conservation des données) à la finalité.

Informatique et Libertés : Principes

Données sensibles

Il est interdit de procéder à des traitements portant sur des données sensibles :

- Origines raciales ou ethniques ;
- Opinions politiques, philosophiques, religieuses ;
- Appartenance syndicale ;
- Santé et vie sexuelle.

Exceptions : consentement exprès, sauvegarde de la vie humaine, gestion des listes de membres, données déjà rendues publiques par la personne concernée, services de santé, statistiques officielles, recherche médicale, procédures judiciaires, « intérêt public » (strictement encadré).

Informatique et Libertés : Formalités préalables

Régime de déclaration

Cas par défaut (pas de données sensibles). Dispense de déclaration si présence d'un CIL dans l'organisation.

Régime d'autorisation (ou avis)

Traitements portant sur des données sensibles, génétiques, biométriques, relatives aux infractions ou condamnations, ou susceptibles de priver d'un droit, ou utilisant le numéro INSEE...

Informatique et Libertés : Droits et obligations

Droits des personnes concernées

- Obligation d'information sur le traitement, la collecte, la conservation, la transmission des données ;
- Droit d'accès et de rectification ;
- Droit d'opposition.

Obligations du responsable de traitement

Il doit garantir les principes de légalité, de finalité, de légitimité et de proportionnalité.
Il doit garantir les droits des personnes concernées (notamment via les « mentions obligatoires ») et est responsable de la confidentialité des données dont il a la garde.

Principes de conception et de gestion

Souveraineté des données

Faire en sorte que **l'utilisateur conserve le contrôle** sur les données personnelles le concernant :

- Stocker en priorité données et/ou clés sur ses terminaux personnels ;
- Contrôler étroitement usage et diffusion, en imposant des obligations (obligations de sécurité, notifications, suppression...).

Principes de conception et de gestion

Minimisation des données

cf. principe de proportionnalité

- Ne collecter que les données absolument nécessaires à la finalité ;
- Ne les transmettre/conserver que si c'est absolument nécessaire ;
- Détruire dès que possible les données non absolument nécessaires ;

Le tout dans les limites des obligations d'auditabilité des systèmes.

Le *Privacy by Design*

Principe

La protection de la vie privée, comme la sécurité, ne peut être efficace que si elle est pensée dès la conception du système. Les ajouts postérieurs ne peuvent pas espérer colmater des brèches de conception.

Le principe, de plus en plus mentionné dans les textes, doit concerner à la fois les intervenants techniques et non techniques, conjointement.

Exemples de mise en œuvre :

- Travail de spécification incluant experts techniques, juristes et décideurs ;
- Application de méthodes formelles de conception ;
- *Privacy impact assessments* ;
- Systèmes contraints par les politiques ;
- ...

Aspects pénaux

Infractions spécifiquement informatiques

Atteintes aux systèmes de traitement automatisé de données (STAD)

Art. 323-1 à 323-7 du Code pénal (loi Godfrain du 5 janvier 1988)

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.

Atteintes aux STAD

Les comportements sanctionnés

- Intrusion (2 ans, 30 k€, 3 ans et 45 k€ si modification) ;
- Entrave au fonctionnement (5 ans, 75 k€) ;
- Introduction frauduleuse de données (5 ans, 75 k€) ;
- Participation à un groupe visant à commettre ces délits ;
- Tentatives de tous ces délits.

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.

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.

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.

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 €

Infractions facilitées ou aggravées par l'informatique

- Atteintes à la protection de l'enfance ;
- Incitation au terrorisme, à la haine raciale, à d'autres crimes et délits ;
- Contrefaçon ;
- Escroqueries ;
- Délits de presse (injure, diffamation) ;
- ...

Hébergeurs et éditeurs

Distinction formalisée par l'article 6 de la LCEN (2004-575), affiné par la jurisprudence, pour attribuer des responsabilités différentes.

Hébergeur

Met à disposition du public des sites web conçus et gérés par des tiers, sans ingérence dans les contenus.

Responsabilité pénale et civile uniquement s'il a connaissance de données « manifestement illicites » et qu'il n'agit pas « promptement pour retirer ces données ou en rendre l'accès impossible ».

Éditeur

Conçoit, organise, effectue des choix éditoriaux sur les contenus publiés.

Normalement responsable, pénalement et civilement, de tous les contenus publiés sous son contrôle.

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...

Experts judiciaires

L'expert peut être un personne physique ou morale
Seules personnes morales inscrites en informatique : l'INPS et le LERTI (labo privé à Grenoble).

À lire/suivre pour creuser

`http://zythom.blogspot.com/`
Blog d'un expert judiciaire en informatique
Beaucoup de retours d'expérience, quelques protocoles et conseils techniques

À l'intersection entre droit et informatique

- Propriété intellectuelle (droit d'auteur, licences, mesures techniques de protection...) ;
- Responsabilités et obligations des administrateurs ;
- Responsabilités et obligations des intermédiaires techniques ;
- Rôle des tiers de confiance ;
- Domaine de l'informatique juridique ;
- ...

Merci !