Sécurité et numérique

François Pellegrini

université de BORDEAUX

Sécurité et numérique

Entre fantasmes d'efficacité et violations avérées des droits fondamentaux

François Pellegrini
Professeur, Université de Bordeaux
francois.pellegrini@u-bordeaux.fr

université de BORDEAUX

Sécurité et numérique

- L'ouverture des espaces numériques étend les problématiques sécuritaires au sein de ces nouveaux espaces
  - Sécurité des outils numériques proprement dits
    - « Cyber-sécurité »
    - Enjeu majeur de souveraineté et de protection des personnes et des biens
  - Usage des outils numériques pour la mise en œuvre des politiques sécuritaires
    - Surveillance ciblée ou de masse
    - Contrôle des individus ou des populations

Cyber-sécurité (1)

- Création de nouveaux délits sanctionnant les actions considérées comme répréhensibles
  - Loi « I&L » du 6 janvier 1978 (art. 34+, obligations)
  - Loi « Godfrain » du 5 janvier 1988 (répression)
- Répression des intrusions et manipulations / falsifications de données au sein des STAD
  - Pas de « propriété » sur les données
  - Pas de « vol » de données
    - Décisions récentes aberrantes

Cyber-sécurité (2)

- Protection récente des personnes informant les responsables de traitement et/ou les autorités des failles de sécurité découvertes
  - Art. L. 2321-4 CD
  - Nécessaire à la mobilisation de l'intelligence collective face à la complexité des systèmes informatiques
    - La robustesse d'une chaîne est celle de son maillon le plus faible

Surveillance numérique (1)

- La généralisation des outils numériques conduit à une explosion des traces numériques produites par les personnes
- Possibilité de collecte de ces traces :
  - A posteriori
    - Réquisitions auprès des responsables de traitement
  - Au vol
    - Fonctionnalités mises en œuvre par les responsables
    - Ex : géo-localisation par les opérateurs téléphoniques
  - Par des moyens spécifiques

Surveillance numérique (2)

- Nombreuses modalités de collecte de traces et d'informations autorisées pour des motifs sécuritaires :
  - Communication par les opérateurs des données ayant transité par les réseaux de communication (L. 851-1 CSI)
  - Communication en temps réel par les opérateurs des données transitant sur les réseaux (L. 851-2 CSI)
  - Communication en temps réel par l'opérateur de la géo-localisation des terminaux (L. 851-4 CSI)

Surveillance numérique (3)

- Dispositif d'interrogation de l'équipement destiné à obtenir ses caractéristiques et sa géo-localisation (L. 851-6 CSI)
- Espiongiciels d'interception de l'interaction d'une personne avec son terminal (706-102-1 CPP)
  - Frappes claviers (« *keyloggers* »), affichage, etc.
  - Vise à contourner la cryptographie de bout en bout
- Balises de géo-localisation (L. 851-5 CSI)

Surveillance numérique (4)

- Existence de dispositifs mettant en œuvre une surveillance de masse :
  - Analyseurs automatiques de trafic, dits « boîtes noires » (L. 851-3)
    - Analyse comportementale
  - Dispositifs de leurrage et d'interception de téléphonie mobile, dits « *IMSI catchers* » (L. 852-1)
    - Surveillance indiscriminée dans le périmètre du dispositif
    - Refus des garde-fous ayant pu permettre une utilisation ciblée du dispositif

Cryptographie (1)

- La cryptographie est une technologie essentielle au fonctionnement de l'ensemble de la société
- Structure l'ensemble de l'infrastructure informationnelle publique et privée
- Nécessité d'une loyauté absolue des briques cryptographiques

Cryptographie (2)

- Inanité d'obliger les acteurs à insérer des « portes dérobées » dans les protocoles et logiciels cryptographiques
  - Affaiblissement global de la sécurité en cas de découverte de la porte dérobée par des tiers
  - La protection par l'obscurité ne fonctionne pas
  - Échec commercial de la puce « Clipper »
  - Les dissidents utiliseront leurs propres outils
    - Développement des applications de sur-chiffrement sur les ordiphones

Cryptographie (3)

- Question de la surveillance globale
  - La surveillance automatisée de masse ne doit pas être facilitée

Extension du fichage (1)

- Il existe deux grandes catégories de fichiers :
  - Fichiers administratifs
  - Fichiers de police
- Encadrement différent de ces deux catégories
- Les fichiers de police sont considérés comme plus intrusifs
  - Contiennent des informations plus détaillées sur les personnes
  - Visent essentiellement à faciliter la détection et la punition de la récidive

Extension du fichage (2)

- Tendance manifeste des pouvoirs publics et de l'autorité judiciaire à, conjointement :
  - Constituer des fichiers administratifs les plus complets possibles sur tous les aspects de la vie des personnes
    - Documents administratifs, fiscalité, etc.
  - Autoriser l'exploitation de ces fichiers administratifs dans le cadre d'enquêtes de police
- Mise hors jeu de la CNIL en 2004
  - Avis consultatifs et non plus conformes

Le fichier TES (1)

- Fichier administratif des détenteurs de titres d'identité
  - Contient des informations biométriques sur les détenteurs : photo, empreintes, taille, yeux, etc.
  - Usage de la biométrie au prétexte de créer des titres « sécurisés »
- Les données biométriques sont extrêmement sensibles
  - Données non révocables

Le fichier TES (2)

- Deux fonctions à l'usage de la biométrie :
  - Authentification
  - Identification
- L'authentification ne nécessite pas de conserver des données biométriques en base centrale
  - Conservation des données uniquement sur le titre lui-même
  - TES conserve les données biométriques en base centrale
    - Pour « améliorer le service à l'usager »

Le fichier TES (3)

- Censure par le Conseil constitutionnel de la loi de mars 2012 relative « à la protection de l'identité »
  - Finalité d'identification rejetée
- Absence de censure de TES-2
  - Finalité d'identification non mentionnée explicitement
  - Mais possibilité de réquisitions judiciaires
    - Donc d'usage de la base à fin d'identification

Le FNAEG (1)

- Créé par la loi du 17 juin 1998 relative à la répression des infractions sexuelles et à la protection des mineurs
- Finalités : faciliter l'identification et la recherche :
  - Des auteurs d'infractions à l'aide de leur profil génétique
  - De personnes disparues à l'aide du profil génétique de leurs descendants ou ascendants

Le FNAEG (2)

- Extensions successives de son périmètre :
  - Principaux crimes d'atteintes aux personnes et aux biens
  - Simples délits : vol, tag, arrachage d'OGM, etc.
  - Inclusion de simples suspects
  - Facilitation de l'utilisation du fichier dans les enquêtes

Le FNAEG (3)

- En 2015, le FNAEG contenait :
  - 472 505 personnes condamnées (16%)
  - 2 280 448 personnes mises en cause (76%)
  - 254 038 traces de personnes inconnues (8%)
- Total : 3 006 991 profils génétiques
  - Soit près de 5% de la population
- Réserves du Conseil constitutionnel (et CEDH)
  - Taille et usages du fichier
  - N'a pas conduit à la remise en cause des pratiques

Le FNAEG (4)

- Utilisation de la recherche en parentèle au sein du FNAEG en 2011
  - Dans le cadre de l'affaire « Élodie Kulik »
  - Recherche « en aveugle »
    - Et non plus « *hit* / *no hit* » sur les personnes présentes
  - Recherche en parentèle directe
    - Ascendants et descendants directs
  - Sans que les textes ne la prévoient
    - Autorisée à posteriori par une loi du 3 juin 2016

Le FNAEG (5)

- Recherche en parentèle indirecte en aveugle mandatée en France en 2012
  - Alors que l'article 706-56-1-1 CPP n'autorise la recherche en parentèle qu'« aux fins de recherche de personnes pouvant être apparentées en ligne directe… »
- Pas de censure par la Cour de cassation
  - Au motif que les articles 81, 706-54 et suivants du CPP permettent au juge d'instruction d'ordonner toute expertise ayant pour objet l'identification et la recherche des crimes et délits

Le FNAEG (6)

- Transformation du FNAEG en fichier de « gens honnêtes »
  - Les personnes fichées n'ont pas commis le crime faisant l'objet de la recherche en parentèle
- Utilisé comme un fichier « de circonstance »
  - Parce qu'il est là et contient des « réprouvés »
- Permet déjà d'identifier la presque intégralité de la population
  - De par le nombre de personnes présentes
  - Sur-représentation des CSP-

Guerre de la biométrie

- Collecte massive par les États de données biométriques de leurs citoyens ou de tiers
  - Volonté de se doter de la capacité à identifier toute personne d'après ses traces
- Risque majeur de mésusage sur le temps long
- Nécessité de protéger la société
  - Refus de la conservation par l'État des données biométriques des citoyens
  - Nécessité de disposer d'un système d'identification contournable

Justice « prédictive »

- Systèmes fonctionnant selon la logique inductive
  - Intrinsèquement conservateurs
  - Relèvent de la prophétie auto-réalisatrice
  - Tendent à considérer comme suspects les personnes a-normales
- Biais systémiques majeurs
  - Lors de la définition du traitement
  - Lors de la collecte des données
  - Lors du fonctionnement de l'algorithme

Conclusion (1)

- La réglementation de l'usage des technologies numériques reste un défi pour le droit
- Le mirage sécuritaire dérègle la boussole des droits fondamentaux
  - Le peuple est considéré comme une menace
- La fascination technicienne fait exister ce qui est possible, pas ce qui est souhaitable
  - La vitesse du progrès dans le monde numérique empêche la prise du recul nécessaire
  - Manque de culture technique des décideurs

Conclusion (2)

- Risque majeur sur le temps long
  - Quelle Résistance possible dans un tel environnement ?
- Doit conduire à réactiver et renforcer le droit fondamental à la sûreté