5A A2S

Sécurité des Serveurs : Sécurité des SGBD

Année 2014/2015

B. Nguyen
benjamin.nguyen@insa-cvl.fr

Plan

- Menaces et législation
- Attaques
  - Injection
  - Buffer Overflow
  - Attaques Statistiques
- Contrôle d'accès *et d'usage*
  - Modèles DAC, MAC, RBAC*, UCON*
  - implémentation dans les BD relationnelles
- *Protection cryptographique des bases de données*
- *Protection matérielle des bases de données*
- Autres formes de protection des données
  - *Audit*
  - Anonymisation de données
  - *Tatouage de BD*

Les menaces

Où/par qui nos données sont-elles stockées ?

- Des données disséminées partout, parfois silencieusement
  - SI nationaux (Impôts, fichiers de police, BaseEcole, DMP …)
    - Les plus encadrés car focalisent toute l'attention
  - SI d'entreprise (employeurs, assurances, EDF …)
  - BD personnelles (factures, fichiers perso …)
  - BD "ambiantes" (Pass Navigo, Telco, télé-surveillance, log de requêtes Web …)
- Des données bien organisées
  - Données centralisées, structurées, cohérentes, à jour
  - Facilement accessibles, exploitables, croisables
  - donc intéressantes !
  - Et ce qui est intéressant pour le gestionnaire l'est pour l'attaquant

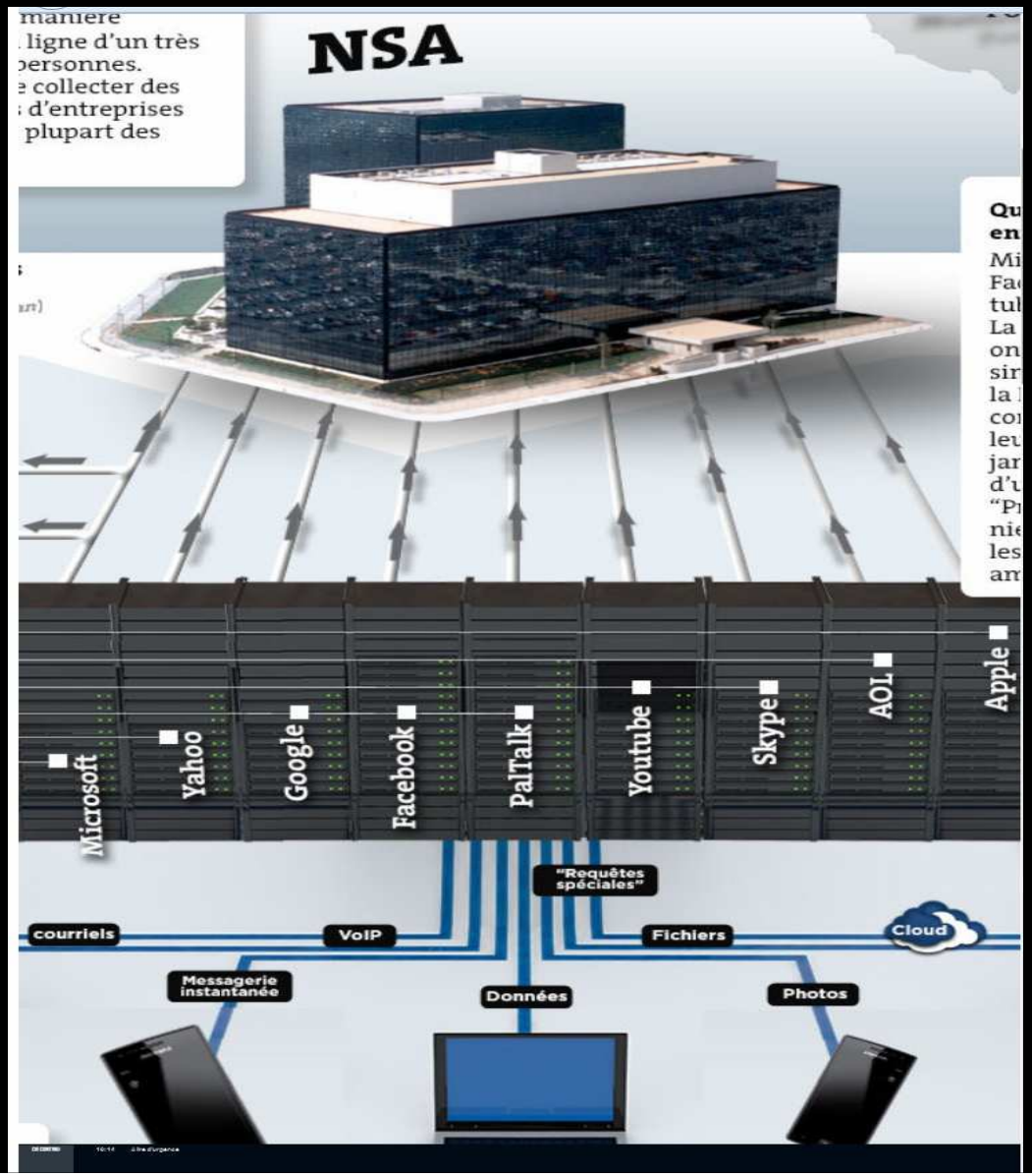
Sont-elles bien protégées ?

- La négligence à l'origine de nombreux trous de sécurité
  - 490.000 Bases de Données sans protection sur le Web (D. Litchfield, nov 07)
  - Données personnelles de 25 Millions de contribuables Anglais égarées (BBC, nov 07)
  - Données de 70 Millions de vétérans US égarées (DataLossDB, oct 09)
  - Achats d'or des clients du CIC (Canard enchaîné, déc 2011)
  - Playstation network hack : 77 million d'utilisateurs, infos perso et bancaires (2011)
  - LinkedIn (6.5 million de personnes, 2012)
  - eBay (145 millions de personnes, 2014)
  - Sites : Zataz.com, datalossdb.org, etc…
- Même les sites les plus sûrs sont piratés
  - FBI, NASA, Pentagone n'échappent pas à la règle
  - Rapport annuel CSI/FBI
    - Les SGBD constituent la 1ère cible des attaques
    - 45% des attaques sont internes

Existe-t-il une parade technique fiable ?

- Le côté 'Unbreakable' a attiré les Hackers (2002)
  - Les tentatives d’attaque sur Oracle ont augmenté de 30,000 per week.
- Quelques jours plus tard ….
  - 'When they say their software is unbreakable, they're lying.'
    -- Bruce Schneier
  - David Litchfield (chercheur anglais en sécurité) a montré qu’un buffer overflow existait dans le serveur Oracle.
  - http://www.theregister.co.uk/2002/02/07/how_to_hack_unbreakable_oracle/
  - N’existe plus depuis 2005 …

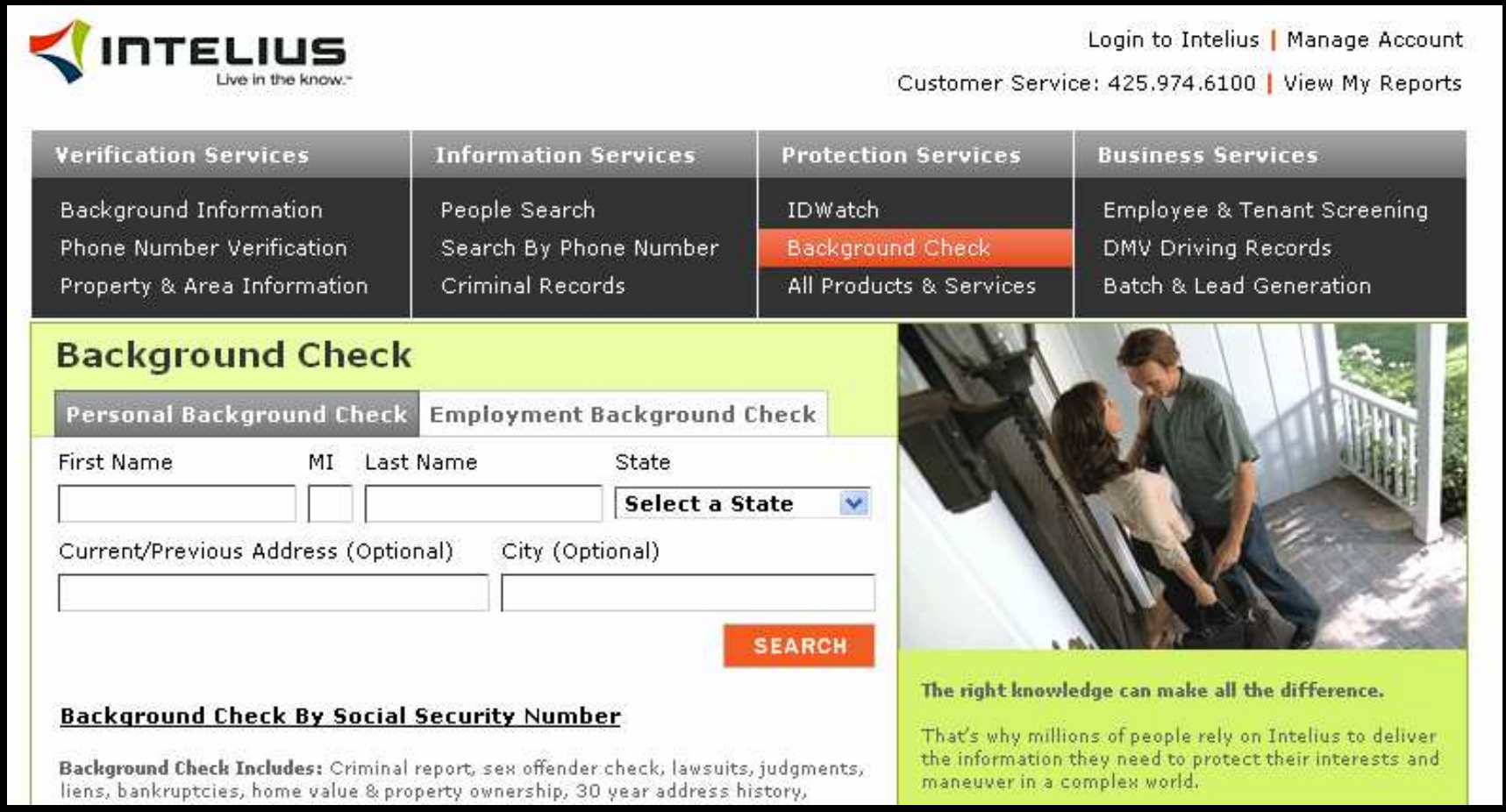
Et le problème est-il uniquement technique ?



Qui est responsable ?

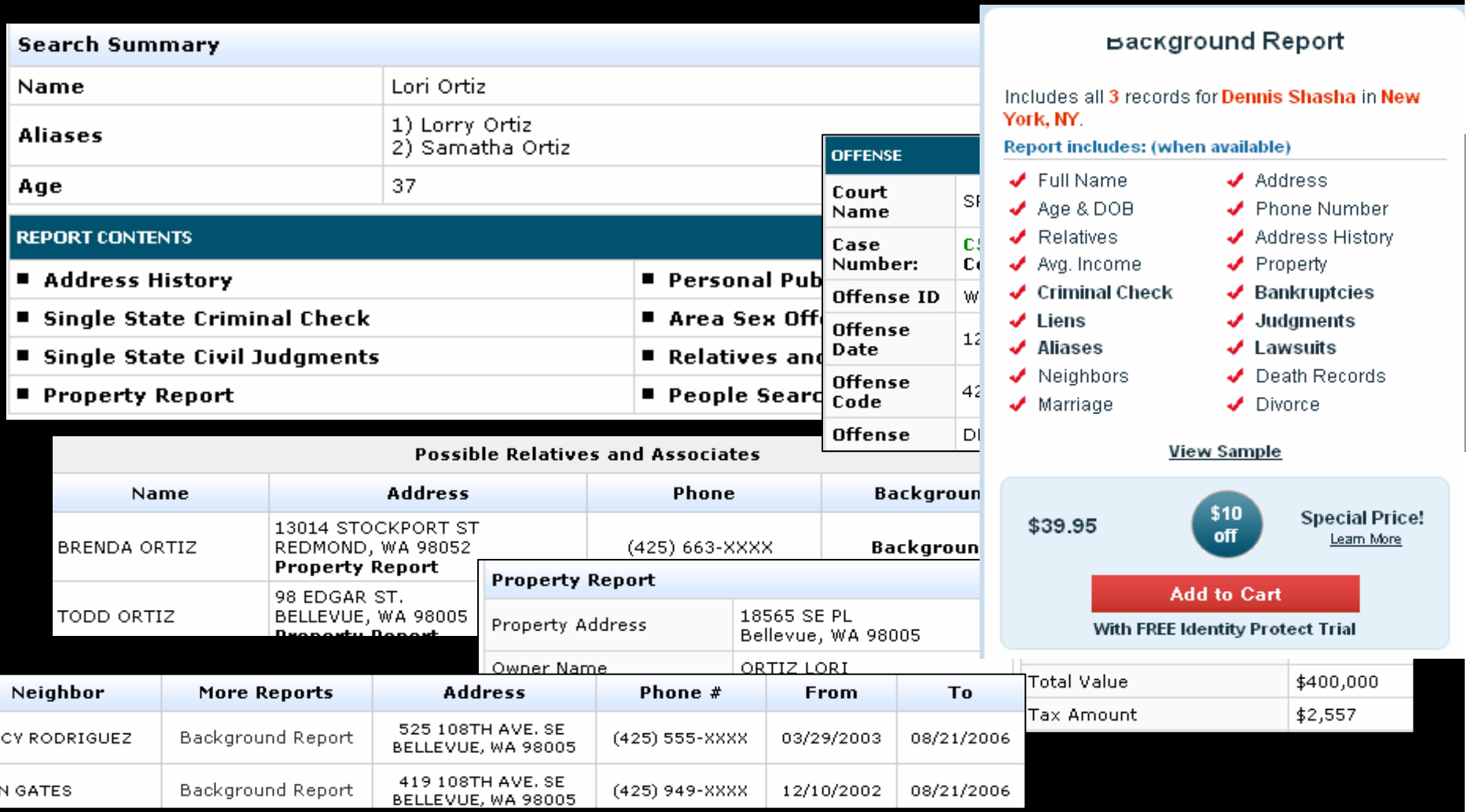
- Dilution des responsabilités
  - Hébergement de données: un modèle qui tend à s'imposer aux particuliers, aux entreprises, aux administrations
  - Vulnérabilité aux attaques internes
    - *Dossiers médicaux menacés de publication par l'employé d'un sous-traitant Pakistanais d'un hôpital Californien (San Francisco Chronicle)*
  - Quelle législation appliquer ?
  - Flou des chartes de confidentialité
    - *"We will not share your health data with individuals or third parties unless you explicitly tell us to do so or except in certain limited circumstances described in our privacy policy. "*
    - *"Certain features of Google Health can be used in conjunction with other Google products, and those features may share information to provide a better user experience and to improve the quality of our services. "*
  - Et aussi : rachat de sociétés, changement de législation, pressions gouvernementales

Mais qui s'intéresse à ces données ?
… Pourquoi des attaques ?



Que voulez-vous savoir sur vos amis, voisins, nourrice, employés, assurés …?

Le marché des données personnelles



Search Summary	
Name	Lori Ortiz
Aliases	1) Lorry Ortiz 2) Samatha Ortiz
Age	37

REPORT CONTENTS

- Address History
- Single State Criminal Check
- Single State Civil Judgments
- Property Report
- Personal Pub
- Area Sex Off
- Relatives and
- People Searc

OFFENSE	
Court Name	SF
Case Number:	C C
Offense ID	W
Offense Date	12
Offense Code	42
Offense	DI

Background Report

Includes all 3 records for Dennis Shasha in New York, NY.

Report includes: (when available)

- Full Name
- Age & DOB
- Relatives
- Avg. Income
- Criminal Check
- Liens
- Aliases
- Neighbors
- Marriage
- Address
- Phone Number
- Address History
- Property
- Bankruptcies
- Judgments
- Lawsuits
- Death Records
- Divorce

View Sample

$39.95 $10 off Special Price! Learn More

Add to Cart

With FREE Identity Protect Trial

Possible Relatives and Associates

Name	Address	Phone	Backgroun
BRENDA ORTIZ	13014 STOCKPORT ST REDMOND, WA 98052 Property Report	(425) 663-XXXX	Backgroun
TODD ORTIZ	98 EDGAR ST. BELLEVUE, WA 98005 Property Report		

Property Report	
Property Address	18565 SE PL Bellevue, WA 98005
Owner Name	ORTIZ LORI

Neighbor	More Reports	Address	Phone #	From	To
NANCY RODRIGUEZ	Background Report	525 108TH AVE. SE BELLEVUE, WA 98005	(425) 555-XXXX	03/29/2003	08/21/2006
JOHN GATES	Background Report	419 108TH AVE. SE BELLEVUE, WA 98005	(425) 949-XXXX	12/10/2002	08/21/2006

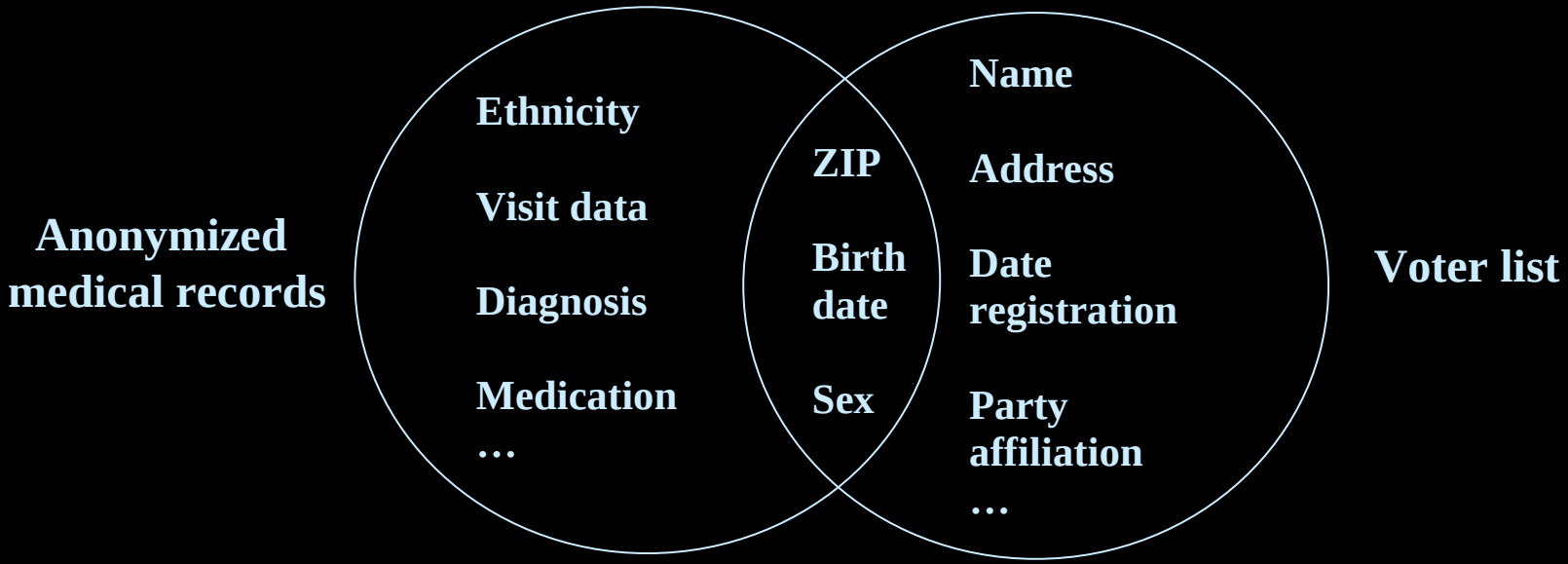
Total Value	$400,000
Tax Amount	$2,557

« The data within the report is compiled from thousands of different sources that include government, property, and other public record repositories. »

Et la parade (lucrative) s'organise => ORM (Online Reputation Manager) e.g. reputation.com

Un risque démultiplié par l'Open Data

- Anonymiser (pseudonymiser) les données ne suffit-il pas ?
- L'existence de quasi-identifiants permet de croiser des sources anonymisées avec d'autres qui ne le sont pas



- « 87% of the population in the US had characteristics that likely made them unique based only on {5-digit Zip, gender, date of birth} » [Sweeney, 2002]
- Antagonisme entre anonymisation et usage

Généralité du problème

- La préservation de la vie privée est un problème emblématique
- Quid de la protection des données industrielles, commerciales, artistiques, administratives, militaires, diplomatiques … ?
  - Se prémunir contre les fuites de confidentialité mais également contre la falsification, la destruction, la copie et plus généralement l'usage illicite
- Peut-on sécuriser efficacement ?
  - Pas de sécurité ultime
  - Une équation économique : Coût / Bénéfice de l'attaque
  - … et sociologique : risque législatif / Bénéfice de l'attaque

Que dit la législation ?

Nature des infractions de la cybercriminalité

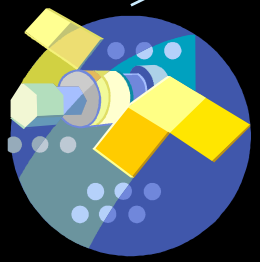
Cybercriminalité

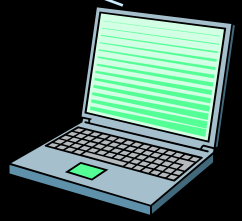
Infractions pour lesquelles les Technologies de l'Information et de la Communication (TIC) sont l'objet même du délit

Infractions pour lesquelles l'Internet est le moyen de commission

Caractéristiques : nature des technologies utilisées

Caractéristiques : criminalité de droit commun, de nature juridique traditionnelle





Infractions liées à la télécommunication

Infractions liées à la téléphonie cellulaire

Infractions informatiques

Infractions prévues par le code pénal

Infractions prévues par des textes spécifiques

Infractions pour lesquelles l'Internet est le moyen de commission

- Les atteintes aux libertés individuelles
  - Diffamation et injure
  - Atteintes à la vie privée
  - Haine raciale, négationnisme, révisionnisme
- Les atteintes aux biens
  - Escroquerie
  - Menace de commettre une destruction, une dégradation ou une détérioration
- Les atteintes à l'ordre public
  - Protection des mineurs
  - Terrorisme
  - Paris clandestins et Jeux d'argent
- Les infractions au code de la propriété intellectuelle
  - contrefaçon

Infractions pour lesquelles les TIC sont l'objet du délit : loi Godfrain, 5 janvier 1988

- Intrusion ou maintien frauduleux dans un système de traitement automatisé de données (STAD) == SGBD !
  - 1 an d'emprisonnement et 15 000 € d'amende
  - 2 ans d'emprisonnement et 30 000 € d'amende s'il y a dommage
- Supprimer, introduire ou modifier frauduleusement des données dans un STAD et/ou tenter d'entraver son fonctionnement
  - 3 ans d'emprisonnement et 45 000 € d'amende
- Détenir, offrir, céder ou mettre à disposition un équipement, programme informatique ou toute donnée en vue de commettre les infractions sus-citées
  - article 323-3-1 du code pénal (Loi sur l'économie numérique du 24 juillet 2003)
  - Peine en fonction de la nature de l'infraction
- Association de malfaiteurs
  - Article 323-4 du code pénal
  - Peine en fonction de la nature de l'infraction

Législation internationale concernant la protection des données à caractère personnel

- Situations très différentes selon les pays
- USA dotés d'une législation sectorielle
  - **Right to Financial Privacy Act, 1978**
  - **Health Insurance Portability and Accountability Act, 1996**
  - **Children's Online Privacy Protection Act, 1998**
  - **…**
- Union Européenne dotée d'une législation globale
  - **Data Protection Directive 95/46/EC, 1995**
  - **Nouvelle réglementation européenne (General Data Protection Regulation, encore en cours de réalisation…)**
  - **Agences nationales (ex: CNIL) imposant l'enregistrement des bases de données et la déclaration préalable des traitements**
- Principe de « Safe Harbor » permettant l'échange d'information avec des entités hors UE tout en offrant des garanties fondamentales de préservation de la confidentialité

Principes généraux de la directive 95/46/EC

- *Finalité*
  - les finalités des traitements doivent être légitimes, explicites et déterminées lors de la collecte des données. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les Etats membres prévoient des garanties appropriées. La période de conservation des données sous une forme permettant l'identification des personnes concernées ne doit pas excéder la réalisation des finalités pour lesquelles elles sont collectées.
- *Information et consentement*
  - La personne reçoit toutes les informations concernant la finalité de la collecte et le traitement ne peut être effectué que si elle donne son consentement explicite et éclairé.

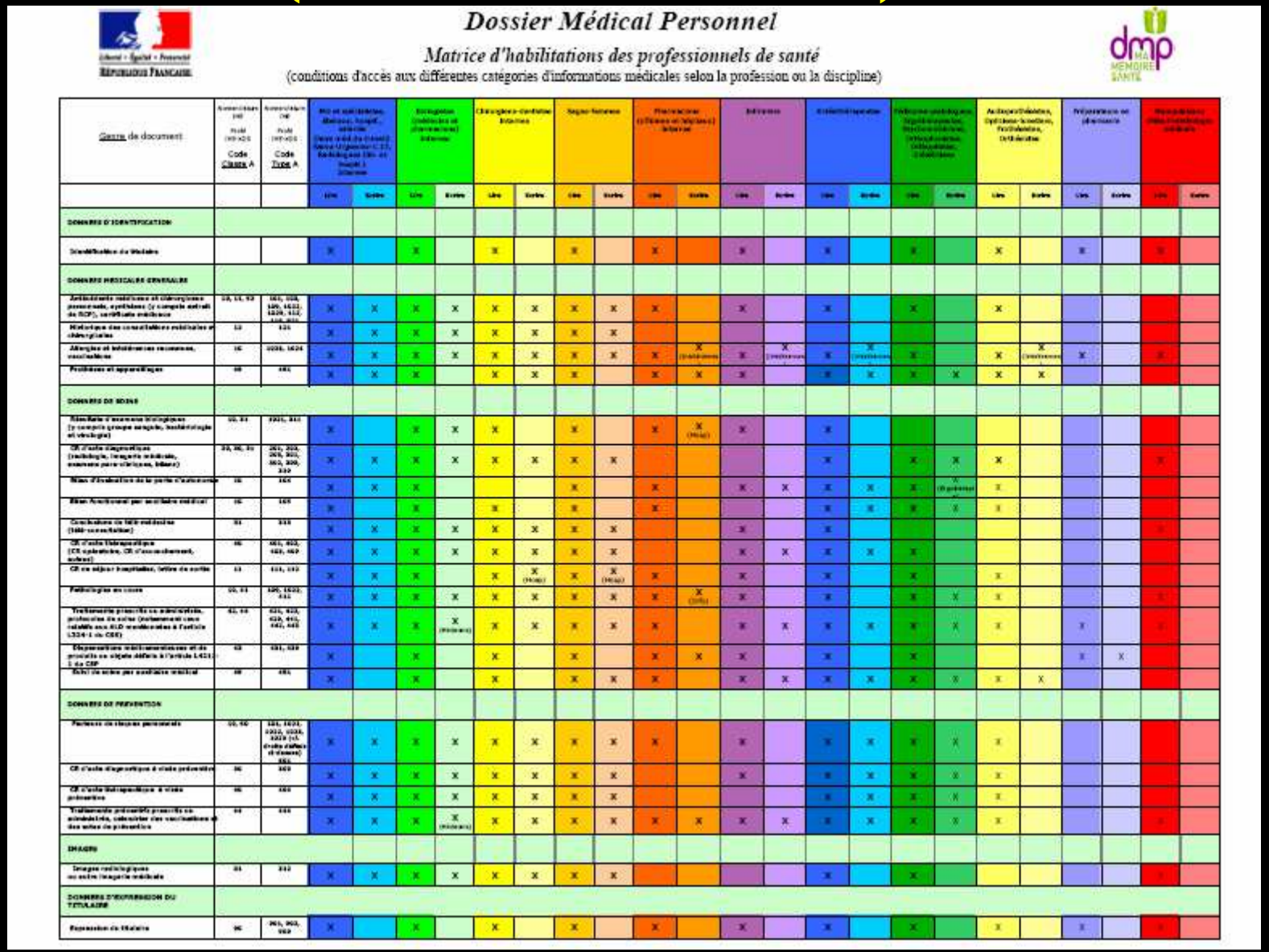
Principes généraux de la directive 95/46/EC

- *Droit d'accès*
  - la personne concernée a le droit d'obtenir la confirmation que ses données font, ou non, l'objet d'un traitement et peut demander la rectification, l'effacement et le verrouillage de données lorsque le traitement n'est pas conforme à la directive.
- *Exactitude*
  - Les données doivent être exactes, à jour et non excessives au regard des finalités pour lesquelles elles sont collectées.
- *Non discrimination*
  - Tout traitement portant sur des catégories particulières de données révèlant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale d'une personne sont interdits.

Principes généraux de la directive 95/46/EC

- *Sécurité*
  - le responsable de traitement doit assurer la sécurité des données contre toute destruction accidentelle et l'accès non autorisé.
- *Transfert vers des pays tiers*
  - Principe de Safe Harbor.
- *Dérogation*
  - Intérêts vitaux de la personne, intérêt public, sécurité nationale, recherche scientifique …
- *Champ d'application*
  - au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

La législation face à la réalité (ex 1 : droits d'accès)



Dossier Médical Personnel

Matrice d'habilitations des professionnels de santé

(conditions d'accès aux différentes catégories d'informations médicales selon la profession ou la discipline)

La législation face à la réalité (ex 2 : anonymisation des données)

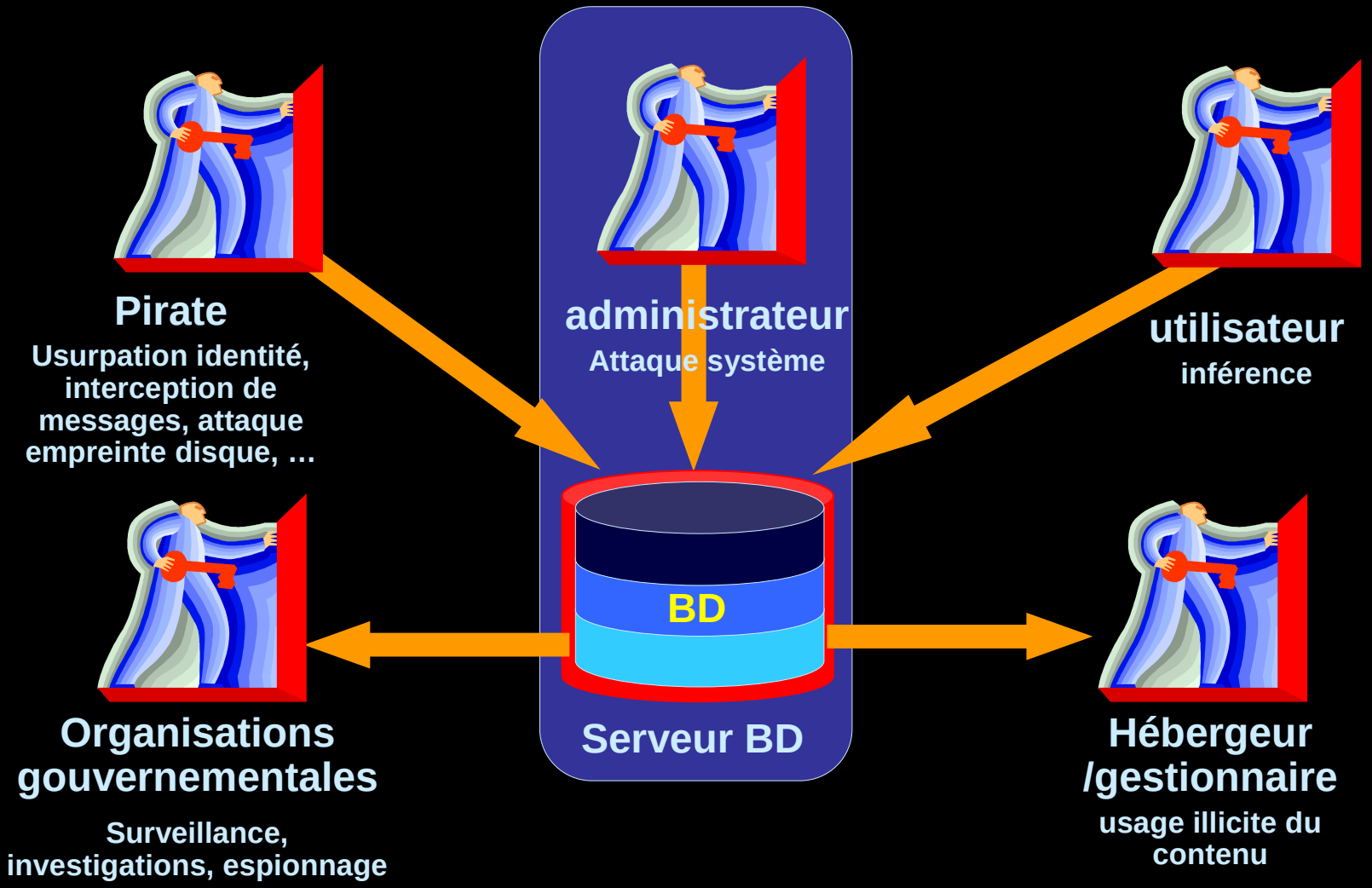
- Des règles plus permissives
  - L'exploitation de données anonymisées ne requiert plus le consentement de la personne dès lors que ce dernier a été donné pour l'objectif initial de la collecte
  - Plus de période limite de rétention
- Données concernées
  - directement nominatives (nom, prénom, date de naissance,..) ou indirectement nominatives (matricule, adresse, n° de téléphone, élément biométrique, adresse IP, les traces des données de connexion, etc)
- Préconisations de la CNIL
  - Ne collecter les données qu'au niveau de finesse strictement nécessaire
  - Ne pas fournir systématiquement un logiciel d'interrogation généraliste
  - Utiliser une fonction de hachage à sens unique (pseudonymisation)
  - Dans les requêtes d'interrogation, ne pas fournir de résultat de cardinalité inférieure à 10 ! (ou $k=5$, $l=3$)
  - …

Attaques et défenses informatiques

Principales classes d’attaques

- Difficile d’être exhaustif
- Principales classes d’attaques
  - Interception de signaux ou brouillage physique
  - Usurpation d'identité
  - Mystification (simulation d'un terminal ou d'un site web)
  - Rejeu de messages
  - Déni de service
  - Fouille du disque ou de la mémoire
  - Cryptanalyse
  - Cheval de Troie, Virus, Ver
  - Etc…

Principales classes d'attaquants



Sécurité des Systèmes d'Information : définition

Information Technology Security Evaluation Criteria *(ITSEC)*

- Confidentialité
  - Seules les personnes autorisées ont accès aux ressources du SI
  - *Ressources BD: données stockées dans la base ainsi que traitements activables sur ces données*
- Intégrité
  - Les ressources du SI ne sont pas corrompues
  - *BD: les données stockées et échangées doivent être protégées de toute modification illicite (destruction, altération, substitution, rejeu)*
- Disponibilité
  - L'accès aux ressources du SI est garanti de façon permanente
  - *BD: idem*
- *Et dans certains contextes*
  - *Auditabilité, imputabilité*

Principales défenses