BIG DATA
DONNEES PERSONNELLES

Quelle sécurité pour les données personnelles dans le contexte mondialisé des Big Data ?

– 15 octobre 2015 –

Dissémination de nos traces (1)

Les mouchards « classiques » ...

ORDINATEURS - SMARTPHONES

- Modèle / identité du poste
- Historiques et métadonnées liés aux sessions de navigation
- Clics, achats, transactions
- Historique des audios écoutées, des vidéos consultées
- Données personnelles stockées sur les sites marchands
- Messagerie
- Adresses mail, adresses IP
- Données de géolocalisation, déplacements
- Communications téléphoniques
- Échanges électroniques
- Discussions
- Cookies

APPLICATIONS

- Facebook
  Sexe, adresse e-mail, téléphone, études, métiers, villes d'origine et actuelle, photos, commentaires, liens de parenté, croyances religieuses, opinions politiques, vie amoureuse, liens partagés
- Google
  Historique des recherches
- Plates-formes vidéo
  Nos goûts, heures et durées de visionnage, durée des pauses
- Jeux
  Liste des contacts, adresses e-mail, numéros de téléphone
- Pass Navigo
  Mémoire des déplacements, dates, heures, lieux

LES « RATÉS »

- Déclarations d'impôts numérisées, avis d'imposition
- Bulletins de paie, relevés de comptes bancaires
- Factures, amendes
- Messageries
- Dossiers médicaux, constats d'accident
- Photos de vacances

Dissémination de nos traces (2)

Les objets connectés

Sport

- Âge
- Poids
- Taille
- Cardiofréquencemètre
- Calories brûlées
- Performances
- Capteurs d'images / vidéos, fonctions de partage sur les réseaux sociaux
- Mémorisation des géolocalisations
- Moniteur de sommeil

Santé

- Tension
- Electrocardiogramme
- Suivi du flux menstruel
- État de stress
- Suivi glycémique
- Auto-dépistage cancer du sein
- Scanner de la peau
- Clouds de santé
- IA / Traitement et croisement de dossiers patient à travers le monde

Domotique

- Qualité de l'air
- Caméras de surveillance (avec reconnaissance faciale et stockage des vidéos dans le cloud)
- Gestion de l'éclairage
- Contrôle à la voix et aux mouvements des objets connectés au sein du foyer
- Téléviseurs « entendants »
- Frigidaires intelligents

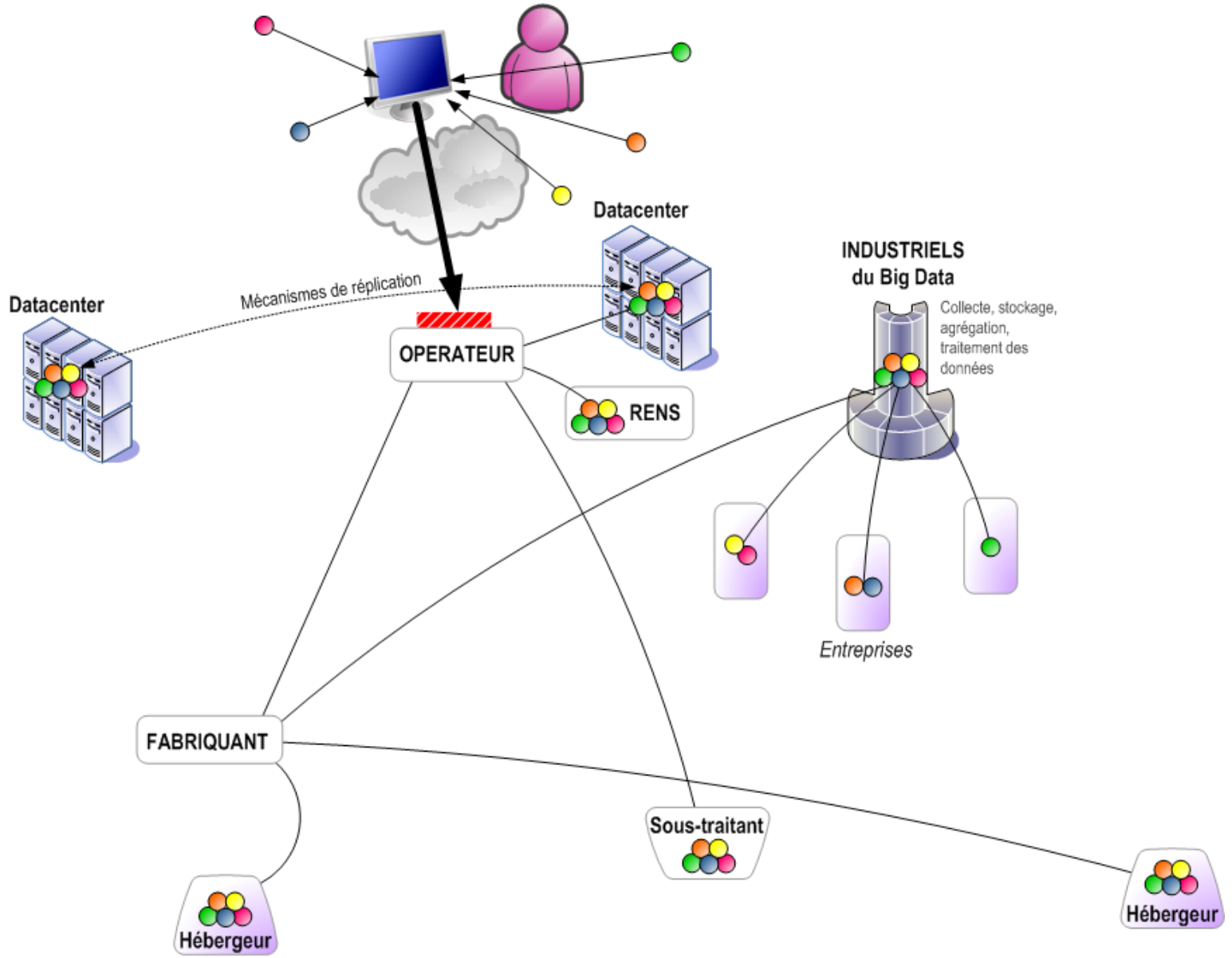
Auto - Moto

- Géolocalisation du véhicule
- État général, problèmes de maintenance
- Commande à distance
- Habitudes de conduite

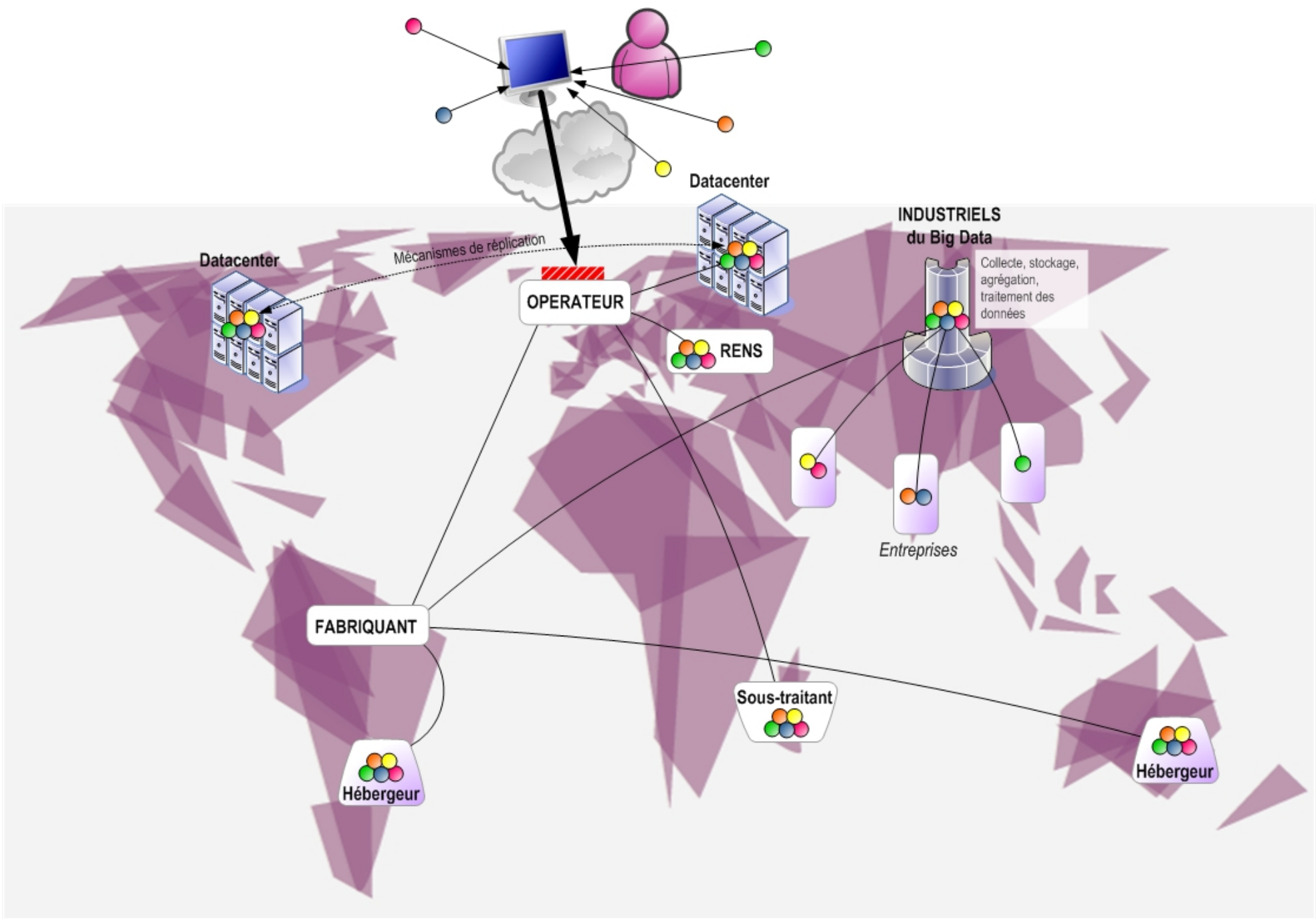
Loisirs

- Données de profil pour des conseils personnalisés en matière de protection solaire
- Empreintes digitales (valises)
- Capteurs de cuisson
- Touillettes pour cocktails
- Sex-toys, pratiques coquines via bluetooth

Localisation des données



Localisation des données

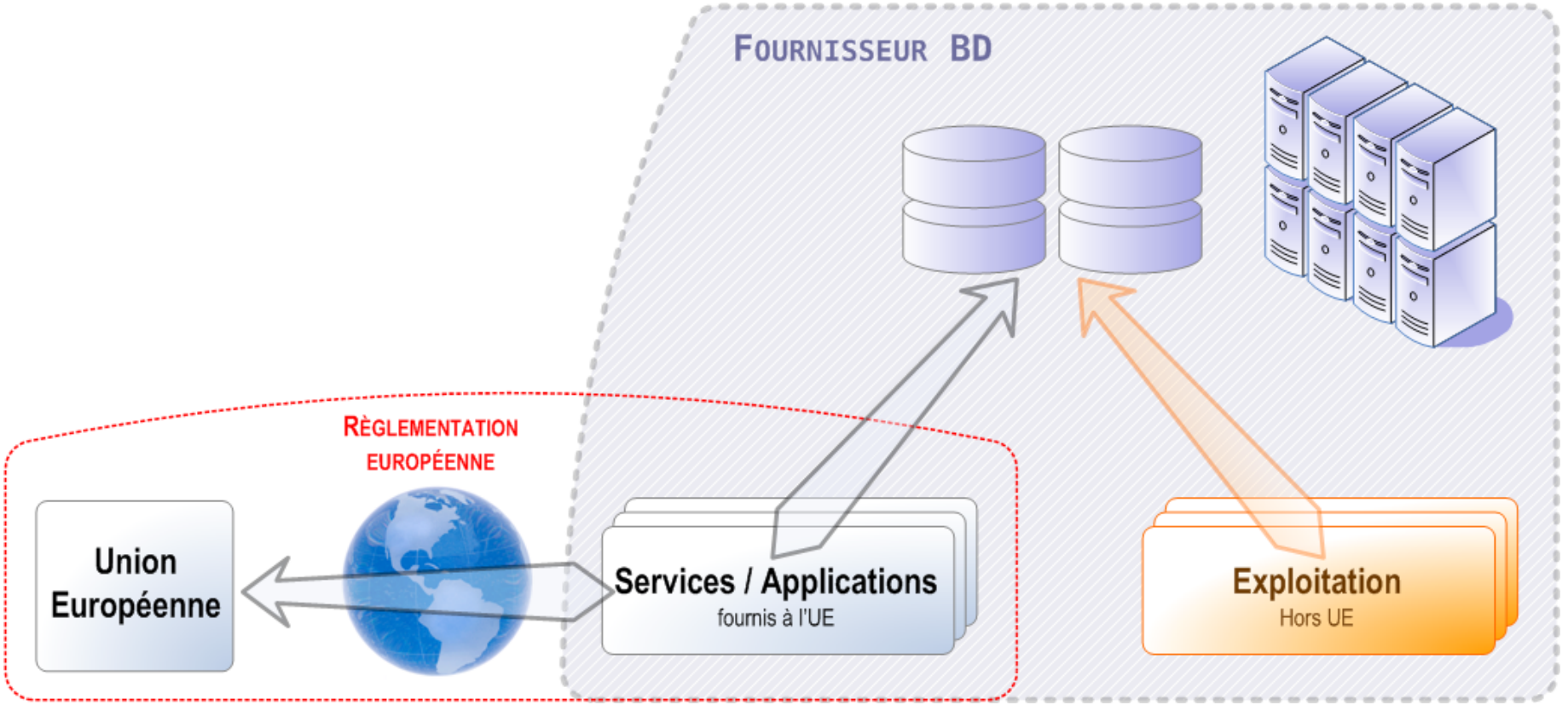


Un aspect de la sécurité : la protection juridique

- *France : CNIL*
- *EUROPE : projet de règlement européen*
- ***Limites***
  - Complexité de mise en conformité pour des acteurs non spécialistes
  - Complexité de mise en application des loi et règlement
    - Multiplicité des acteurs, diversité des données brutes
    - Capacité des technologies à donner un sens à partir de signaux faibles
    - Mise à jour des applications et traitements back-office
  - Les organisations à but « non bienveillant »
  - Les plates-formes ouvertes aux développeurs d'applications tierces
    - De toute bonne foi mais des maladresses dans le traitement des données
    - Intelligence économique
    - Espionnage

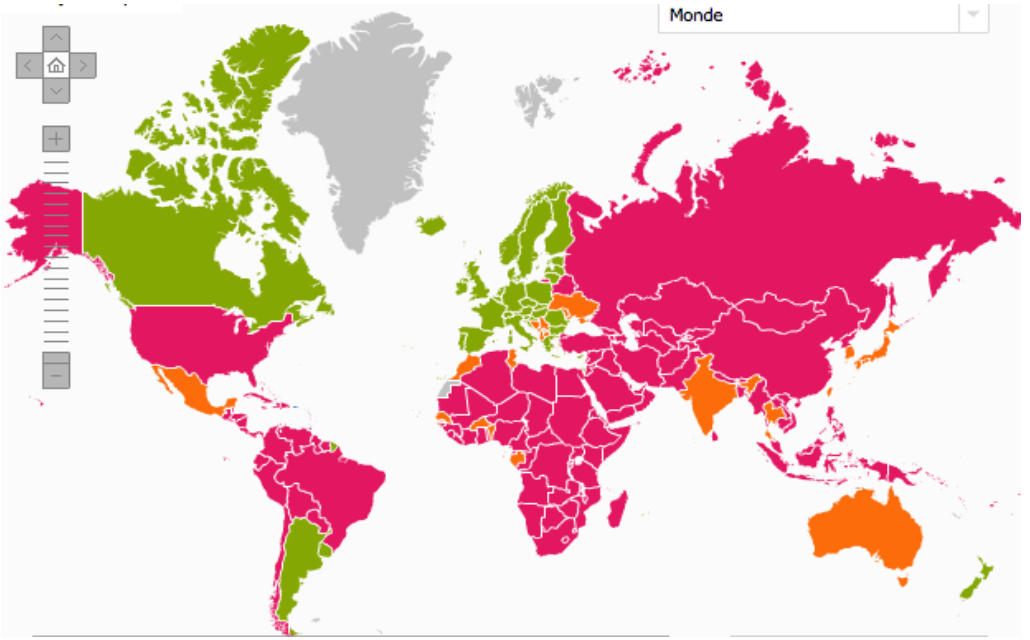
Quid de la protection juridique des datas hors UE ?

- *Règlement Européen applicable pour les produits et services fournis à l'UE*

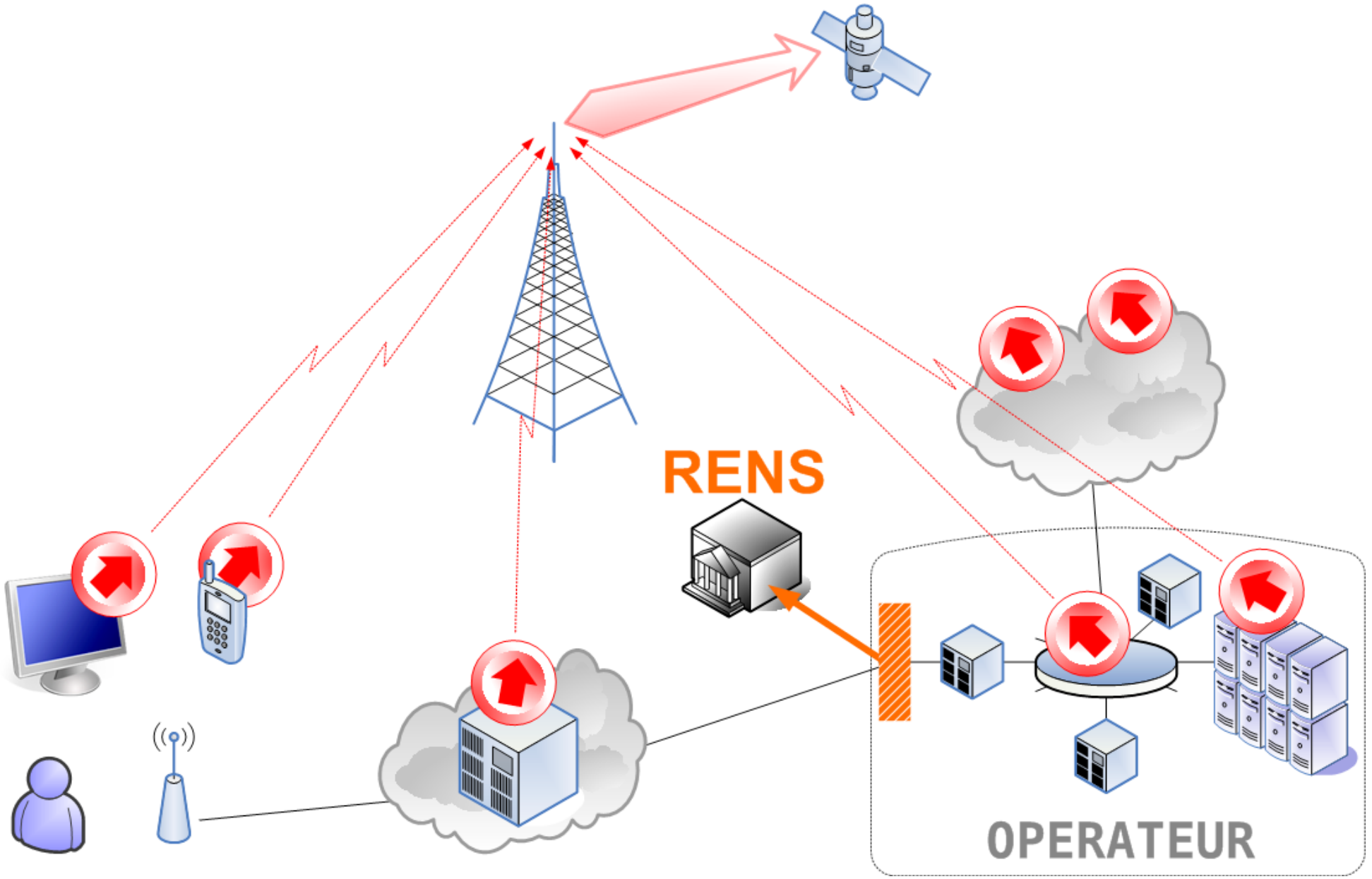


Quid de la protection juridique des datas hors UE ?

- *US : influences du 11 septembre (ex. Patriot Act)*
  - Ordonne la surveillance et la mise sur écoute globale et continue des citoyens américains
  - Exploitation massive des données recueillies à toutes fins utiles
- *Russie*
  - Loi fédérale N 242-FZ : la fin du cloud en dehors des frontières
  - Porte-parole du Kremlin, un message éloquent : « s'affranchir du principal administrateur d'internet »
- *Chine*
  - Sujet récent et encore incomplètement appréhendé
  - Des pratiques fortement orientées vers l'intelligence économique



La part des Anges...



Le risque informatique pour les données personnelles

- *Une sécurité limitée à celle des plates-formes informatiques*
  - Opérateurs de plates-formes BD, fournisseurs de messageries, hébergeurs, clouds, etc.
- *Les grands réseaux d'opérateurs eux-mêmes vulnérables (ex. SS7)*
- *Fuites « techniques » des constructeurs*
- *Vols massifs et récurrents de données personnelles*
  - Identités, n° cartes bancaires, mots de passe, n° téléphone
  - Comportements dans l'entreprise, entretiens d'évaluation, bilans médicaux, achats, adresses de livraison...
  - Photos / vidéos privées stockées sur le cloud
- *Accès illicites aux messageries, SMS, conversations téléphoniques*
- *Cyber-attaques classiques*

Incertitudes induites par les techniques du Big Data

- *Les erreurs dues aux algorithmes et processus d'analyse*
  - Corrélations multi-variables, énorme volume de données parfois bruitées, imprécises, non fiables. Risque : conclusions erronées
  - Nous ne maîtrisons pas les marqueurs d'activité suspectes
  - Le citoyen n'est pas au courant lorsqu'il entre dans la mauvaise case, il n'y aucune possibilité pour lui de contester
- *La fiabilité de certains modèles prédictifs encore trop aléatoire*
  - *« Si vous utilisez Firefox, vous êtes plus efficace que les utilisateurs de Safari »*
- *L'algorithme de plus en plus présent dans le processus de décision*
  - Bénéficie du sceau de l'objectivité
  - *« Contrairement à l'homme, l'algorithme est rationnel, objectif, non discriminant, neutre. Il est plus fiable qu'un recruteur »*

FRANCE : la loi sur le Renseignement (1)

- *« Garantir la sécurité intérieure »*
- *Généralisation des écoutes systématiques (boîtes noires opérateurs), surveillance automatisée*
  - « Accès permanent, complet, direct et immédiat aux informations ou documents collectés
  - « Le recueil en temps réel, sur les réseaux des opérateurs /.../ des informations ou documents /.../ relatifs à une personne préalablement identifiée comme présentant une menace »
- *Big Data : oui, on peut surveiller tout le monde*
- *Qualification d'un citoyen*
  - Rien d'illégal, mais... qu'est-ce qu'un comportement suspect ?
  - Il est aisé de procéder à des investigations plus poussées

FRANCE : la loi sur le Renseignement (2)

- *PNIJ*
- *Tendance générale au « Big Brother Data »*
  - Abrogation de la limite apposée par le législateur à la surveillance des populations
- *Une solution simple :*
  - Pas d'avis controversé, pas de critique, ne pas tromper son conjoint, pas de visite de sites politiquement incorrects...
  - *… La société de surveillance*

Scénarios d'attaque possibles

Coup de projecteur sur nos faiblesses
Jeu, addictions, rêves inaccessibles, turpitudes...

Exposition de la vie privée
Du fait d'acteurs tiers (photos, vidéos, données de tous types)

Identification de cibles potentielles
Projets sensibles ou stratégiques, intervenants généralement discrets

Terrain de jeu pour la cyber-criminalité
Nouveaux enjeux liés au développement du BD

Déstabilisation de hauts dirigeants
Jeter le discrédit sur un concurrent, pressions discrètes lors d'importantes négociations, éliminer un gêneur etc.

Surveillance des salariés d'une entreprise
La DG épie les activités et faits et gestes des salariés, y compris dans leur vie personnelle

Chantages, rançons
À destination d'une entreprise (ex. publication d'un fichier volumineux de données personnelles)
À destination d'un particulier (attitude «inappropriée »)

Surveillance étatique inappropriée
« Police de la pensée »
Risques de tomber par erreur sous les radars des services de renseignement

Dépôts de bilan d'entreprise
Perte de confiance suite à la divulgation massive de données personnelles

Présence agressive d'offres commerciales
« Politique de la pensée »
Personnalisation outrancière, offres inopportunes

Risques sur nos vies privées

- *Exposition très large de nos vies privées, bien au-delà de ce qu'aucun dictateur dans l'histoire n'aurait pu espérer*
- *Prédictions erronées de comportements déviants*
- *Pressions*
- *Subtilisation de données personnelles*
- *Le sentiment de devoir se justifier vis-à-vis d'un surveillant*

Solutions possibles

- *Culture « sécurité informatique »*
  - Sensibilisation de tout un chacun aux risques induits par la diffusion volontaire – ou semi-volontaire – d'informations personnelles
  - Actions de régulation au niveau du citoyen
- *Recherche européenne (ex. H2020)*
  - Techniques nouvelles pour l'évaluation du degré de confiance d'une application dans la manipulation des données personnelles
- *Encadrer les pratiques, pousser les acteurs à développer des actions de mise en conformité*
- *Encadrer l'exploitation des données par les services de renseignement*
  - Traces des accès
  - Contrôle des usages, audits périodiques par des cabinets indépendants

Merci de votre attention...

Plus de 20 ans d'expérience en SSI *sur les grands programmes informatiques, les systèmes de défense, de l'industrie et des Administrations*

Auditeurs agréés par l'**ANSSI** (certification RGS)
ISO 27001 Lead Auditors / Implementors

Contact :
Patrick LEGAND
Tel : +33 (0)6 07 81 61 68
Mail : plegand@xirius-informatique.fr

Xirius Informatique

11, Rue Fénelon – 75010 PARIS – Tel : +33 (0)1 82 09 34 74
e-mail : contact@xirius-informatique.fr – w.xirius-informatique.fr