SECURITE NUMERIQUE : FAIRE FACE AUX NOUVEAUX DEFIS !

CCI Haute Saône

30 janvier 2018

1. Analyse des risques

★ *Analyse des risques potentiels :* risques principaux identifiés :

- Atteintes à la vie privée (utilisation frauduleuse des données personnelles)
- Affaiblissement de la sécurité des réseaux (grand nombre de normes d'interopérabilité et de protocoles de réseau)
- Détournement de contenus au détriment des entreprises propriétaires (atteinte aux droits de PI)

Le niveau de criticité du risque dépend de la nature de l'objet connecté, de la nature des données traitées et de l'utilisateur final

2. Données personnelles

★ *De nouveaux défis pour la protection des données*

Un constat : Accroissement exponentiel des violations de données (+ 48% en 2014), toujours plus de (mauvaise) publicité dans les médias

- Ransomware « WANNACRY 2017» ➔ NIVEA, AUCHAN, ST GOBAIN, etc..
- Vols de données (2016) ➔ YAHOO: 500 millions de comptes, E BAY: 145, LINKEDIN: 115

POURQUOI?

- Manque d'intérêt pour la sécurité
- Mauvaises habitudes de sécurité
- Manque de sens de responsabilité des dirigeants d'entreprises
- Incapacité à évaluer, traiter et identifier les données collectées

2. Données personnelles

★ *Evolution du cadre règlementaire*

1970

Loi Informatique et Libertés (1978)

- Développement informatique dans les administrations
- Fichage public

1995

Directive 95/46/CE, loi IFL modifiée (2004)

- Développement informatique entreprises/Particuliers
- Fichage privé

2016

Règlement 2016/679/UE

(paquet européen relatif à la protection des données)

- Cloud computing
- Big data
- Profiling

2. Données personnelles

- ★ *Le paquet européen relatif à la protection des données* : Le règlement européen 2016/679 du 27/04/2016 constitue le 1° pilier de l'arsenal communautaire pour la protection des données des particuliers
- ★ *Objectif :* Etablir des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données
- ★ *Entrée en vigueur :* 25 mai 2018
- ★ *Principes :*
  - Renforcement du droit des personnes
  - Responsabilisation des responsables de traitement
  - Simplification, harmonisation et collaboration (interprétation homogène dans 28 Etats)
  - Application directe
  - Exceptions nationales possibles

2. Données personnelles

- ★ *Le paquet européen relatif à la protection des données* : Le règlement européen 2016/679 du 27/04/2016
- ★ *Evolutions règlementaires concernent* :
  - Définition des données personnelles
  - Responsable des traitements
  - Principe de sécurité renforcée
  - Collecte des données
  - Mentions obligatoires
  - Droits des personnes : portabilité/Oubli, etc..
  - Délégué à la protection des données
  - Traitements
  - Gestion des problèmes de sécurité
  - Transferts de données

2. Données personnelles

★ *Définition des données à caractère personnel*

Toute information se rapportant à une personne physique identifiée ou identifiable par référence à :

- Un numéro d'identification
- Une adresse email
- Une adresse IP
- Un cookie
- Etc..

★ Supprimer le caractère personnel par la « pseudonymisation » de la donnée (possibilité de rendre des DP illisible mais de façon réversibles) ex: dispositif de codage d'email permettant une lecture en clair au moment de l'envoi,

★ Obligation de sécurité à charge du responsable de traitement : Mette en œuvre des solutions pour répondre à l'obligation légale de présenter un niveau de sécurité du traitement adapté au risque encouru

2. Données personnelles

★ *Définition des données à caractère personnel sensibles:*

Il n'existe pas de définition, mais une liste (non exhaustive) :

- Origines raciales ou ethniques
- Opinions politiques, religieuses, philosophiques
- Appartenance syndicale
- Santé, vie sexuelle
- Données biométriques
- Données concernant l'emploi et l'organisation du travail
- Données génétiques
- Données relatives aux infractions et condamnations pénales

Loi informatique et libertés – Art. 8

RGPD

★ *Enjeu :* traitement spécifiquement encadré du fait d'un risque plus important pour les droits et libertés fondamentaux

2.a Données personnelles - Responsable de traitement

★ *Comment le déterminer?*
- Personne physique ou morale, publique ou privée
- Détermine les finalités du traitement
- Détermine les moyens techniques utilisés pour le traitement
- Peut être désigné par la loi

★ *Catégories de responsables de traitement*
- Exclusif
- Conjoints : plusieurs co-responsables unis par convention, responsabilité solidaire en cas de recours du titulaire des données
- Sous traitant : traite les données pour le compte du responsable de traitement, ex: hébergeur, intégrateur de logiciel, entreprise de sécurité informatique, etc.. ➔ Sont soumis à des obligations spécifiques

2.b Données personnelles - Principe de sécurité renforcée

- ★ *« Privacy by design » (protection de la vie privée dés la conception):* Chaque nouvelle technologie traitant des données personnelles ou permettant d'en traiter, doit garantir dès sa conception et lors de chaque utilisation, même si elle n'as pas été prévue à l'origine, le plus haut niveau possible de protection des données
- ★ *Objectif :* Protéger la donnée contre tout traitement illicite ou non autorisé et contre la perte et la destruction totale ou partielle survenue de façon accidentelle (ou pas), avec des mesures adaptées au risque

2.c Données personnelles - Collecte des données

★ *Conditions de la collecte pour que le futur traitement soit licite*

- Accord expresse du titulaire de la donnée (abandon de l'opt-out au profit de l'opt-in) :
  - Recueil de consentement ne doit pas être ambigu
  - Information obligatoire claire et compréhensible: identité du responsable et des finalités du traitement, possibilités de retrait du consentement
  - Possibilité de prouver que le consentement est univoque
- Dérogations : pas de consentement préalable exigé
  - Contrat ou mesures précontractuelles
  - Respect d'une obligation légale
  - Sauvegarde de la vie de la personne
  - Exécution d'une mission de service publique
  - Présence d'un intérêt légitime poursuivi par le responsable du traitement

★ Nature de la collecte : Directe ou indirecte

2.d Données personnelles - Mentions obligatoires

★ *Mentions obligatoires à transmettre au titulaire de la donnée lors de la collecte :*

- Identité du responsable du traitement ou de son représentant
- Coordonnées du DPD (le cas échéant)
- Nature des données concernées et finalités du traitement, ainsi que d'une éventuelle réutilisation ultérieure
- Description de l'intérêt légitime (si données sensibles)
- La destination de la donnée (qui réceptionne → Situation de sous-traitance)
- Décision de transférer les données vers un pays tiers (le cas échéant)
- Durée de conservation de la donnée
- Rappel du droit d'accès, de modification et d'effacement de la donnée (droit d'opposition)
- Rappel du droit de retirer le consentement à tout moment
- Rappel du droit d'effectuer une réclamation auprès de l'autorité de contrôle
- Rappel de l'exigence de fourniture de la donnée basée sur une obligation règlementaire ou contractuelle (le cas échéant)

2.e Données personnelles - Renforcement du droit des personnes

★ *De nouveaux droits pour les titulaires de données*

- Portabilité : Permet à une personne de récupérer les données qu'elle a fournies sous une forme aisément réutilisable, et, le cas échéant, de les transférer ensuite à un tiers. Il s'agit ici de redonner aux personnes la maîtrise de leurs données, et de compenser en partie l'asymétrie entre le responsable de traitement et la personne concernée,
- Mineurs : La législation européenne comporte des dispositions spécifiques pour les mineurs de moins de 16 ans. L'information sur les traitements de données les concernant doit être rédigée en des termes clairs et simples, que l'enfant peut aisément comprendre. Le consentement doit être recueilli auprès du titulaire de l'autorité parentale. Les États membres peuvent abaisser cet âge par la loi, sans toutefois qu'il puisse être inférieur à 13 ans. Devenu adulte, le consentement donné sur un traitement doit pouvoir être retiré et les données effacées.

2.e Données personnelles - Renforcement du droit des personnes

★ *De nouveaux droits pour les titulaires de données*

- Introduction du principe des actions collectives : Tout comme pour la législation relative à la protection des consommateurs, les associations actives dans le domaine de la protection des droits et libertés des personnes en matière de protection des données auront la possibilité d'introduire des recours collectifs en matière de protection des données
- Un droit à réparation des dommages matériel ou moral : Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du règlement, a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi

2.f Données personnelles - Délégué à la protection des données

★ *Le DPD*

- Définition : Personne dont le rôle consiste à veiller à ce que le responsable de traitement (ou le sous-traitant) protège convenablement les données à caractère personnel des individus, conformément à la législation en vigueur.
- Qui est-il ? Un salarié de la société ou un tiers
- Quand doit il être désigné (conditions alternatives)?
  - Traitement effectué par un organisme public
  - Traitements réguliers, systématiques et à grande échelle
  - Traitement à grande échelle de données sensibles
- Quelles missions?
  - Informer et conseiller le responsable de traitement, ses employés et sous-traitants
  - Contrôler le respect du cadre juridique
  - Gérer les études d'impact (données sensibles)
  - Coopérer avec l'autorité de contrôle et être le point de contact

2.g Données personnelles - Traitement des données

★ *Principe général : « Accountability » = Responsabilisation*

AVANT

Responsable de traitement : Déclaration (voir autorisation) préalable

APRES

Responsable de traitement : Soumis à autoévaluation (cf. nouvelle approche)= Responsabilité a priori

- Adoption de règles internes adaptées aux objectifs des traitements (**mesures techniques et organisationnelles**)
- Tenue d'un **registre des traitements**

2.g Données personnelles - Traitement des données

★ *Mesures générales techniques et organisationnelles (privacy by default):*
Il est nécessaire de prévoir dès la conception du traitement, les mesures techniques et organisationnelles qui vont permettre d'atteindre le plus haut niveau de protection possible

- Qui est responsable? Responsable de traitement, sous-traitant
- Quelles mesures mettre en œuvre?
  - Pseudonymisation et chiffrement
  - Moyens techniques de protection de la confidentialité, de l'intégrité et de la disponibilité des systèmes de traitement
  - Rétablissement dans des délais adaptés de l'accès des données en cas d'incident
  - Procédure de test et d'évaluation des procédures de sécurité
  - Si besoin, élaboration d'un code de conduite

2.g Données personnelles - Traitement des données

★ *Registre des activités de traitement :*

- Qui est concerné?
  - Responsables de traitement, sous-traitants, représentants dans l'UE d'entreprises étrangères
  - Entreprises ou organismes > 250 salariés

    Sauf si (conditions alternatives)
  - Réalise des traitements à risque pour les droits et libertés des personnes (ex: traitement permettant une discrimination liée à l'origine raciale)
  - Traitement habituel (ex: gestion fichier RH)
  - Traitement de données sensibles
  - Traitement de données judiciaires

2.g Données personnelles - Traitement des données

★ *Registre des activités de traitement :*

- Pourquoi?
  - Faciliter la surveillance et le contrôle des autorités
  - Faciliter le travail du sous-traitant, en phase avec la conformité du responsable du traitement
- Quel contenu?
  - Identité du responsable du traitement, de son représentant, du DPD
  - Finalités du traitement
  - Description des personnes et des données concernées par les traitements
  - Destinataire des données
  - Destination (si transferts hors UE)
  - Délais de conservation
  - Description des mesures de sécurité générale techniques et organisationnelles

2.g Données personnelles - Traitement des données

★ *Registre des activités de traitement :*

- Comment? Pas de forme contrainte
- Sanctions ? Registre inexistant ou non conforme :
  - 2 millions € ou 2% max. CA annuel mondial année N-1
  - L'autorité de contrôle dispose d'un panel de sanctions intermédiaires (avertissement, limitation temporaire ou définitive du traitement, retrait de la certification, etc..)

2.g Données personnelles - Traitement des données

★ *Traitement des données sensibles:*

Si un traitement (notamment du fait de l'utilisation de nouvelles technologies) présente un risque élevé d'atteintes aux droits des personnes physiques, le responsable de traitement doit :

- Réaliser une **étude d'impact**
- **Consulter préalablement l'autorité de contrôle** (CNIL)

2.g Données personnelles - Traitement des données

★ *Traitement des données sensibles:*

Si un traitement (notamment du fait de l'utilisation de nouvelles technologies) présente un risque élevé d'atteinte aux droits des personnes physiques, le responsable de traitement doit réaliser **une étude d'impact** relative à la protection des données, contenant:

- Une description du traitement et des finalités
- Une évaluation de la proportionnalité du traitement avec les finalités attendues
- Une évaluation des risques pour les droits et libertés des titulaires de données
- Une descriptions des mesures de préventions mises en œuvre pour prévenir le risque et des mécanismes de sécurité, qui permettront d'apporter la preuve du respect du cadre juridique

2.g Données personnelles - Traitement des données

★ *Traitement des données sensibles:*

Si l'analyse d'impact révèle un risque élevé concernent les atteintes aux droits et libertés en cas d'inaction du responsable de traitement, ce dernier doit réaliser **consultation préalable** de l'autorité de contrôle :

- Quel contenu ? Le responsable de traitement communique :
  - Les responsabilités respectives des acteurs du traitement (ex: responsable, sous-traitant, etc..)
  - Les finalités et moyens du traitement envisagé
  - Les mesures de protection et de garanties au bénéfice des droits et libertés
  - Les coordonnées du DPD
  - L'étude d'impact
  - Toute information exigée par l'autorité de contrôle

2.h Données personnelles - Violation des données personnelles

★ *Cas d'infraction à la sécurité des données:*

- Définition : Violation de la sécurité entrainant de manière accidentelle ou volontaire (mais illicite) une perte, altération, destruction ou une diffusion/Accès non autorisé de données personnelles
- Mesure curative : Notifications
  - A l'autorité de contrôle (sauf si absence de risque pour le droit des personnes)
  - A la personne concernée (idem)
- Délais : ASAP (si possible 72 heures)
- Informations fournies : Nature de la violation (chiffrage si possible), coordonnées du DPD, description de l'impact envisagé, description des mesures prophylactiques mises en œuvre

2.i Données personnelles - Transfert de données personnelles

★ *Conditions des transferts de données personnelles hors UE:*

- Principe : Interdiction.
- Dérogations possibles moyennant :
  - Un niveau de protection adéquat
  - Des garanties appropriées
  - Un consentement expresse
  - Un transfert unique
  - Sur la base d'une décision de justice issue d'un pays tiers (le cas échéant)

2.j Données personnelles - Sanctions

★ *Panel de sanctions sévères:*

- Sanctions administratives :
  - Mode de calcul :
    - Nature , gravité et durée de la violation
    - Caractère intentionnel ou négligent
    - Mesures curatives engagées par le responsable de traitement
    - Degré de responsabilité du responsable de traitement
    - Degré de coopération avec l'autorité de contrôle
  - Montants :
    - Absence de notification d'une violation de sécurité, absence ou brèche de protection dès la conception ou par défaut : 10M€ ou 2% CA global mondial exercice N-1
    - Non conformité du traitement, données sensibles non protégées, transfert frauduleux de données hors UE: 20M€ ou 4% CA

2.j Données personnelles - Sanctions

★ *Panel de sanctions sévères:*

- Sanctions pénales : Fixées par chaque Etats membres
- Montants :
  - Traitements frauduleux, absence de notification, etc.. : 300 000€, 5 ans de prison

3. Sécurité des réseaux

- ★ *Le paquet européen relatif à la protection des données* : le 2° pilier du paquet est la directive UE/2016/1148 du 06/07/2016,
- ★ *Objectif :* Augmenter le niveau de sécurité des réseaux numériques par la définition de normes de sécurité communes (lutte contre la cybercriminalité et les accidents techniques) et des procédures de notification
- ★ *Contenu :*
  - Création des CSIRT (computer security incident response team) : centres de réponse nationaux aux incidents de sécurité informatique chargés de mettre en oeuvre des réponses coordonnées
  - Deux catégories de professionnels directement visés :
    - Opérateurs de service essentiels : liste établie par les Etats qui regroupe les entités fournissant des services vitaux (ex : banques, fournisseurs d'énergie, transporteurs, hopitaux, fournisseurs d'eau potable, etc..)
    - Fournisseurs de service numérique : tout opérateur fournissant des services de place de marché, de moteurs de recherche, de service d'informatique en nuage

3. Sécurité des réseaux

- ★ *Le paquet européen relatif à la protection des données* : Le 2° pilier du paquet est la directive UE/2016/1148 du 06/07/2016,
- ★ *Obligations à la charge des deux catégories de professionnels :*
  - Opérateurs de services essentiels : Doivent mettre en œuvre les mesures techniques nécessaires pour prévenir les incidents et notifier dans un cadre normalisé, aux CSIRT et au grand public, les incidents constatés
  - Fournisseurs de service numérique : Obligations similaires. En cas de sous traitance, le sous traitant doit notifier le donneur d'ordre
  - Exclusion : Ces obligations ne s'appliquent pas aux micro et petites entreprises (selon la définition européenne), toutefois il est fortement recommandé à tout opérateur d'y souscrire volontairement dés lors que l'incident détecté peut avoir un impact significatif sur la continuité du service fourni.
- ★ Date d'application : 9 mai 2018

3.a Sécurité des réseaux – Les STAD

★ *La protection des réseaux en droit français :*

- Le concept de **STAD** (**Système de traitement automatisé de données**): Pas de définition légale : Ensemble composé d'éléments de nature diverse et protégé par des dispositifs de sécurité
- Sont des STAD : Téléphone mobile, réseau de paiement en ligne, ordinateur isolé, montre connectée, etc.,

3.a Sécurité des réseaux – Les STAD

★ *La protection des réseaux en droit français :*

Loi informatique et libertés :

Obligations à charge du responsable du système :

- Obligation d'assurer un niveau de protection adéquat (sécurité/confidentialité) en fonction de la nature des données (pas de RGS national).
- Politique de protection du système et procédures
  - Authentification (droits d'accès)
  - Sécurisation des informations et du système,
  - Sauvegarde
  - Contrôle de la bonne utilisation du système (charte informatique)
  - Gestion des incidents,
  - Recours à la sous-traitance

3.a Sécurité des réseaux – Les STAD

★ *La protection des réseaux en droit français :*

La protection des STAD en droit pénal :

- Art. 323-1 à 323-8 C.PEN. : Interdiction de toute atteinte frauduleuse aux systèmes de traitement automatique de données
  - Introduction dans le système
  - Modification des données
  - Altération du fonctionnement
  - Etc..

4. Atteintes aux droits de propriété intellectuelle

★ *Atteintes aux droits de propriété intellectuelle :*

- Question de la brevetabilité des logiciels
- Droits d'auteurs : Démonstration de l'antériorité nécessaire (constat d'huissier, enveloppe Soleau, etc..)
- Cadre juridique applicable : Le code de la propriété intellectuelle et la protection des logiciels par le droit d'auteur (Loi du 3 Juillet 1985)

5. Exemple : Objets connectés de santé

★ *Essai d'application du cadre juridique aux objets connectés de santé:*

Croisement de plusieurs régimes juridiques

★Gestion des données

- Traitement des données personnelles (cf. infra) : « *informations concernant tous les aspects tant physiques que psychiques de la santé d'une personnes* » (CJUE aff. 101/01 Linqvist)
- Interdiction de principe du traitement des données de santé (art. 8-1 loi informatique et liberté
- Hébergement par des tiers : RGPD , art. 28
- Responsabilité des hébergeurs de données de santé : art. L1111-8 CSP, interdiction de traitement des données qui leurs sont confiées, obligation de secret professionnel, interdiction de cession des données,..
- DPD obligatoire

5. Exemple : Objets connectés de santé

★ *Essai d'application du cadre juridique aux objets connectés de santé:*

Croisement de plusieurs régimes juridiques

- Cadre juridique des STAD
- Conformité du dispositif à la règlementation marquage CE : art. L5211-1 et s. CSP, *«On entend par dispositif médical tout instrument, appareil, équipement, matière, produit, à l'exception des produits d'origine humaine, ou autre article utilisé seul ou en association, y compris les accessoires et logiciels nécessaires au bon fonctionnement de celui-ci, destiné par le fabricant à être utilisé chez l'homme à des fins médicales.. »*
- Selon la jurisprudence communautaire, un logiciel peut être qualifié de dispositif médical

6. L'avenir : les chantiers juridiques de demain

★ *Problématique des modèles prédictifs:* utilisation des algorithmes d'aide à la décision appliqués sur des données collectées

- Problèmes d'éthique évidents
- Cadre juridique inexistant

Contacts

★Robert Guyon,
Responsable juridique

E-mail: r.guyon@bourgognefranchecomte.cci.fr
Tél : 03 80 60 40 61

enterprise europe network
L'Europe à la portée de votre entreprise.

Commission européenne

CCI BOURGOGNE FRANCHE-COMTÉ