Vent'anni di legislazione sulla protezione dei dati
Retrospettive e prospettive

Convegno pubblico
Bellinzona, 27 aprile 2012

L'evoluzione del diritto sulla protezione dei dati
Prospettive

Jean-Philippe Walter

Dott. iur., incaricato federale supplente della protezione dei dati e della trasparenza, presidente dell'Autorità comune di controllo Schengen dell'Unione europea

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Préposé fédéral à la protection des données et à la transparence
PFPDT

L'évolution du droit de la protection des données:

perspectives

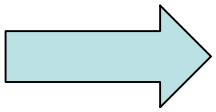
Jean-Philippe Walter, Dr en droit
Préposé fédéral suppléant

Sommaire

- Introduction
- Evaluation de la loi fédérale sur la protection des données
- Révision du cadre juridique européen
  - Union européenne
  - Conseil de l'Europe
- Perspectives suisses: vers une révision totale de la LPD ?
- Conclusion

Introduction

- 19 juin 1992:
  - Fin de l'affaire des « fiches »
  - Informatique (encore) dominée par grands centres de calcul, traitements (relativement) « maîtrisable »
- 2012:
  - Informatique pour tous, omniprésente
  - Internet, réseaux sociaux, smartphone, …
  - Globalisation
  - Ubiquité, multifonctionnalité, miniaturisation



Nécessité de réformes

Evaluation de la LPD

2010 – 2011: évaluation LPD par le bureau Vatter (…) :

- Analyser l'effectivité et efficacité LPD (limité à certains aspects)
- Connaissance de la loi
- Mécanismes de mise en œuvre
  - Exercice des droits des personnes concernées
  - Procédure et voies de droit
- Rôle, tâches et compétences du PFPDT

Conclusion évaluation

- LPD permet d'atteindre ses objectifs, mais
  - Augmentation des menaces sur le respect des droits et libertés fondamentales
  - Déficit au niveau de l'exercice des droits des personnes concernées (maîtrise insuffisante, manque de conscience sur les traitements, etc)
  - Evolution technologique, accroissement des traitements de données = défis pour individus, responsable de traitement, autorité de contrôle
  - PFPDT remplit son mandat de manière efficace compte tenu des ressources à disposition et du contexte actuel

Suite de l'évaluation

- Rapport du Conseil fédéral du 19 décembre 2012 aux chambres fédérales: nécessité d'adapter LPD
  - Mandat au DFJP d'examiner d'ici 2014 quelles mesures permettraient de:
    - Assurer la protection des données plus en amont
    - Sensibiliser davantage les personnes concernées
    - Améliorer la transparence
    - Améliorer le contrôle et la maîtrise des données
    - Protéger les mineurs

Développement au sein de l'Union européenne

- Traité de Lisbonne: extension des compétences communautaires, notamment au domaine de la police et de la justice

- Art. 8 Charte européenne : droit à la protection des données

- Art. 16 Traité de Lisbonne, fixer « les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les Etats membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données »

25 janvier 2012:

- Projet de règlement du Parlement européen et du Conseil relative à la protection des personnes physique à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données

- Projet de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales et à la libre circulation de ces données

Objectifs:

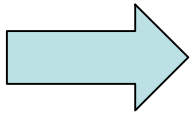
- Renforcer la protection des données en Europe
- Assurer une plus grande **cohérence** et **effectivité** des normes de la protection des données
- Répondre au défi du nouvel environnement numérique et globalisé
- Permettre aux personnes physiques d'exercer une maîtrise effective sur leurs données
- Faciliter la libre circulation des flux de données au sein de l'Union européenne
- Doter l'Europe de règles claires et uniformes
- Alléger les charges administratives pesant sur les responsables de traitement

Grandes lignes du règlement:

- Renforcement des droits des personnes concernées
- Renforcement de l'indépendance et des pouvoirs des autorités nationales de protection des données
- Renforcement des mesures de sécurité des données
- Accroissement de la responsabilité des personnes et organismes qui traitent des données
- Application cohérente et (si possible) uniforme des règles, notamment renforcement de la coopération entre APDs
- Maintien de l'exigence du niveau adéquat, mais assoupli (BCR)

Grandes lignes de la directive

- Garantir un niveau élevé et cohérent de protection des données en respectant les spécificités de la coopération policière et judiciaire
- Renforcer la confiance mutuelle entre les autorités policières et judiciaires des Etats membres
- Faciliter la libre circulation des données et renforcer l'efficacité de la coopération entre ces autorités



- Application des principes généraux de la protection des données à tout traitement de données personnelles (pas seulement aux échanges de données)
- Imposer des conditions et des critères harmonisés minima lorsque des limitations aux principes sont nécessaires
- Instaurer un régime spécial tenant compte de la nature particulière des activités répressives

Application du règlement et de la directive

- Règlement est d'application directe : une loi pour l'ensemble de l'Europe
- Directive doit être transposée par les Etats

- Règlement et Directive = acquis de Schengen

Convention 108

- Objectifs modernisation:
  - Gérer les défis de la vie privée résultant de l'utilisation des nouvelles technologies de l'information et des communications
  - Renforcer le droit à la protection des données
  - Concilier le droit à la protection des données avec les autres droits et libertés fondamentales
  - Renforcer les mécanismes de mise en œuvre et de suivi
  - Maintenir approche technologiquement neutre
  - Assurer la **cohérence** et la **compatibilité** avec UE
  - Préserver, réaffirmer, renforcer et promouvoir la **vocation universelle** et le **caractère ouvert** de la Convention

Grandes lignes du projet

- Objet et but : garantir à toute personne physique le droit à la protection des données à caractère personnel afin d'assurer le respect des autres droits et libertés fondamentales
- Champ d'application :
  - Couvre tous les traitements automatisés et non automatisés (dans la mesure où les données font partie d'un ensemble dont la structure permet de rechercher par personne concernée)
  - Exception pour les traitements « domestiques »
- Définitions:
  - Précision de la donnée à caractère personnel
  - Abandon des notions de fichier et de maître du fichier
  - Définition du responsable, sous-traitant et destinataire

Grandes lignes du projet (suite)

- Principes de base
  - Principes définis à l'article 5 complétés par
    - Principe de proportionnalité
    - Principe de minimisation des données
  - Motifs légitimant le traitement
    - Consentement
    - Droit interne + intérêt légitime prépondérant
    - Respect d'une obligation légale
    - Respect d'une obligation contractuelle

Grandes lignes (suite)

- Données sensibles :
  - Révision et extension du catalogue avec une classification selon:
    - Nature des données
    - Usage qui est fait des données
    - Risque grave pour les intérêts, droits et libertés fondamentales de la personne concernée,
  - maintien du principe de l'interdiction de traitement sauf si le droit interne prévoit des garanties appropriées.

- Sécurité des données: obligation d'annoncer les violations des données

Grandes Lignes (suite)

- Droits des personnes concernées:
  - Transparence: obligation d'information
  - Droit d'accès
    - Information sur l'origine des données
    - Connaissance du raisonnement qui sous-tend le traitement des données dont les résultats sont opposés à la personne concernée ou lui sont appliqués
  - Droit de ne pas être soumis à une décision automatisée sans pouvoir faire valoir son point de vue
  - Droit de s'opposer au traitement

    [restriction possible aux conditions de l'art. 9 de la convention]

Grandes lignes (suite)

- Obligation du responsable du traitement :
  - Responsable de la mise en œuvre des dispositions de protection des données
    - Choix des moyens utilisés: technologies de la vie privée
  - Obligation de procéder à des analyses d'impact
  - Mise en place de mécanismes internes permettant de démontrer la conformité des traitements avec les dispositions de protection des données
    - Nomination de chargés de la protection des données

Grandes lignes (suite)

- Flux transfrontières de données:
  - Exigence d'un niveau de protection des données adéquat
  - « Présomption » d'adéquation pour Parties à la Convention
  - Pays tiers:
    - Dispositions légales
    - Autres mesures juridiques: contractuelles, règles internes contraignantes, moyennant information des APDs
    - En l'absence d'un niveau adéquat, transfert dans des cas particuliers
      - Consentement
      - Intérêts spécifiques personne concernée
      - Intérêts légitimes protégés par la loi (art. 9)
  - Dérogations possibles pour garantir liberté d'expression et d'information

Grandes lignes (suite)

- Autorité de contrôle:
  - Compléter compétences et tâches
  - Renforcer indépendance
  - Renforcer coopération entre APDs, notamment investigation commune, échange d'information
  - Traitements effectués par les instances judiciaires dans l'exercice de leurs fonctions juridictionnelles pas soumis à compétence des APDs.

Mise en oeuvre

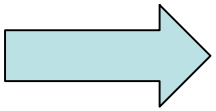
- Obligation des parties de prendre les mesures nécessaires pour donner effet aux principes de base pour la protection des données énoncés dans la Convention
  - Mesures prises avant la ratification ou l'adhésion
  - Examen par le comité conventionnel de la conformité des mesures prises avec les exigence de la convention
- Renforcement des compétences du comité conventionnel
  - Émettre des avis préalable à l'adhésion
  - Évaluation de conformité
  - Évaluation du normes juridiques régissant Ftd (adéquation)
  - Élaboration de modèles de mesures standardisées Ftd

Forme juridique et suite de la procédure

- Protocole d'amendement ?
- Adoption du projet par le comité consultatif en juin 2012
- Transmission au comité des Ministres
- Comité ad'hoc examine projet (automne 2012, début 2013)
- Adoption et ouverture à la signature par le CM dans le courant 2013

Perspectives suisses : vers une révision totale de la LPD ?

- Rapport d'évaluation
- Postulat Hodgers « Adapter la loi sur la protection des données aux nouvelles technologies » : renforcement du droit à la protection des données (privacy by design, audits externes)
- Postulat Graber « Atteintes à la sphère privée et menaces indirectes sur les libertés individuelles » : renforcement LPD eu égard à l'impact des technologies de surveillance
- Postulat Schwaab « opportunité d'ancrer et/ou de préciser dans la législation un droit à l'oubli numérique »
- Mandat du Conseil fédéral au DFJP
- Développement du droit européen



Réviser notre législation en matière de protection des données

Objectifs

- Ne pas affaiblir l'acquis
- Maintenir l'approche technologiquement neutre
- Rendre notre législation plus effective au bénéfice des droits et des libertés touchés par le traitement de données personnelles
- Créer les conditions nécessaires à ce que chacun et chacune d'entre-nous puissent recourir en toute confiance aux technologies de l'information et des communications
- Meilleure harmonisation avec le droit européen
- Collaboration – coordination entre APDs

Champ d'application

- Élargir le champ d'application et englober l'ensemble des traitements données, à l'exception des traitements « domestiques »
- même régime pour le secteur privé que pour le secteur public
- Application du droit matériel fédéral aux traitements des organes cantonaux et communaux (loi fédérale cadre), en réservant la surveillance aux APDs-cantonales

Définitions

- Meilleure cohérence avec la terminologie européenne, notamment Convention 108
  - Remplacer la notion de maître de fichier par celle de responsable de traitement
  - Introduction de la notion de sous-traitant

Principes de base

- Assurer cohérence avec droit européen sans toucher à l'essence des principes de base

- Introduction du principe de minimisation des données

Droits des personnes concernées

- Renforcement des droits pour assurer une plus grande maîtrise sur nos propres données : bénéficier des mêmes droits dans le monde numérique que dans le monde réel:
  - Renforcer la transparence des traitements:
    - obligation d'information lors de la collecte quelle que soit la nature des données collectées;
    - Information complète et accessible;
    - Délivrée de manière intelligible, en des termes clairs et simples, adaptés aux différents publics cibles;
  - Extension du catalogue des informations à fournir lors de l'exercice du droit d'accès (profilage, décision automatisée)

Droits des personnes concernées

- Droit à l'oubli: préciser et renforcer les droits existants en relation avec le droit d'opposition, de rectification et d'effacement, et la durée de conservation des données
- Droit de portabilité des données
- Droit de regard et de participation lors « décisions automatisées »
- Droit de s'opposer à la publication ou à l'indexation des données sur Internet
- Droit de surfer sans être observé et profilé
- Améliorer les voies de droit et les procédures en cas de conflit: droit d'action des associations, médiation
- Responsabilité objective du fait du traitement

Obligation des responsables de traitement

- Obligation de prendre en compte les principes de protection des données :
  - Durant toutes les phases du traitement
  - Dans l'organisation et le développement des systèmes d'information et des technologies (privacy by design, protection des données par défaut)
- Obligation de procéder à des évaluations des risques d'atteinte au droit à la protection des données / étude d'impact
- Obligation d'instaurer des chargés à la protection des données

Obligations (suite)

- Obligation d'annoncer les violations des données
- Obligation d'avoir un représentant en Suisse ou dans un pays de niveau adéquat
- Préciser les garanties qui doivent entourer le recours à des sous-traitant
- Obligation de documenter les traitements
- Introduction d'un contrôle préalable pour certaines types de traitement à risque élevé d'atteinte aux droits et libertés fondamentales
- Dans le cadre Ftd, soumettre règles internes à validation du PFPDT

Surveillance

Effectivité de la protection des données passe par l'existence d'autorités de surveillance (APD) dotées de compétences:

- Information – sensibilisation
- Conseil, notamment avis sur projets législatifs
- Surveillance : pouvoirs d'intervention et d'investigation:
  - Mener des enquêtes
  - Prendre des mesures conservatoires
  - Accèder aux locaux et aux traitements
  - Compétences décisionnelles et pouvoirs de sanctions
  - Agir en justice

Indépendance des APDs

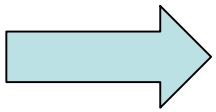
- APD doit exercer ses fonctions en toute indépendance
  - Institutionnelle
  - Fonctionnelle
  - Matérielle
- Critères de l'indépendance doivent préciser dans la loi
  - Nomination
  - Durée
  - Incompatibilité
  - Ressources
  - Financement

Coopération entre APDs

- Coopération, condition indispensable et incontournable pour assurer une meilleure effectivité et efficacité dans l'accomplissement des tâches
- Coopération à ancrer et préciser dans loi:
  - Partage des informations
  - Assistance mutuelle
  - Application cohérente des dispositions légales
  - Mener des activités de contrôle conjointes et coordonnées
  - Structure institutionnelle de collaboration
- 26 APDs cantonales + 1 APD fédérale, un luxe pour la Suisse nuisible à l'effectivité de la protection des données ?

Conclusion

- Principes LPD demeurent pertinents
- Révision nécessaire pour une meilleure effectivité et une meilleure maîtrise pour les personnes sur les données qui les concernent
- Revoir l'organisation des APDs
- Adoption d'un code suisse



Travaux doivent démarrer sans attendre;

APDs doivent se positionner