

Traitement de données à caractère personnel

Défis pour l'avenir



Question centrale

L'actuelle réglementation peut-elle résister aux défis de la société de l'information actuelle et future ?

Traitement de données à caractère personnel

- Avant : Web 0.0 (pas d'Internet) et Web 1.0
 - Traitement de données centralisé
 - Systèmes informatiques mainframe
 - Distinction claire contrôleur/sous-traitant
 - Traitement de données limité à quelques acteurs, flux de données maîtrisables
 - Le traitement local est la règle générale, le traitement réparti est l'exception
- Maintenant : Web 2.0
 - Traitement de données réparti, flux de données constants
 - Traitement de données peer-to-peer (réseaux sociaux)
 - Contenu généré par les usagers
 - Software as a Service (SaaS)
 - Informatique en nuages
- Futur : Web 3.0
 - Web sémantique
 - Informatique ubiquitaire
 - Réseaux de nouvelle génération

Nouveaux défis

- Augmentation énorme de la collecte de données
- Profilage détaillé des utilisateurs par accumulation et combinaison des banques de données et par les nouvelles technologies (p. ex. reconnaissance faciale)
- Données à caractère personnel conservées et traitées à des emplacements virtuels
- Augmentation énorme des contrôleurs : chaque citoyen devient contrôleur (P2P)
- Contrôle de ses propres données à caractère personnel devenu pratiquement impossible (le droit de disposer soi-même de ses données est une illusion)
- Décisions automatisées, de banal à crucial
- Le vol d'identité devient réel
- *"Personal data is the new oil of the Internet and the new currency of the digital world "*

Dix points importants

1. Champ d'application matériel
2. Champ d'application géographique
3. Formalités
4. Données sensibles
5. Obligations de transparence
6. Droits de la personne concernée
7. Mesures de sécurité
8. Délais de conservation
9. Coopération internationale
10. Rôle de la Commission vie privée et du Groupe 29

1. Champ d'application matériel



Donnée à caractère personnel

- *"Toute information concernant une personne physique identifiée ou identifiable"*
- La notion actuelle n'est-elle pas trop large ?
 - *"toute information"*
 - dessin d'enfant
 - données non structurées (p. ex. blog)
 - *"concernant"*
 - entreprise de taxis utilisant un système de positionnement par satellite
 - valeur d'une habitation
 - *"identifiable"*
 - concept absolu ou relatif ?
 - données de profilage "abstraites" ?
 - graffiti
- **Personne physique**
 - protection de la vie privée d'une personne morale ? (cf. Autriche/Italie)
 - protection d'une personne décédée ?

→ Retour à l'essentiel ?

Traitement

- *"Toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel"*
 - Tout traitement se fait actuellement au moyen de procédés automatisés
 - écrire une lettre sur un PC
 - visiter un site Internet
 - rédiger un e-mail
 - conserver un e-mail
 - blog
- L'objectif du législateur est-il de maintenir le champ d'application aussi large ?

Responsable ↔ sous-traitant

- Le critère combiné de "finalités et moyens" est souvent partiellement respecté par les différentes parties
 - P. ex. contexte de l'outsourcing
 - Description restreinte du "responsable"
 - Maison mère, filiales
 - Réseaux sociaux et autres applications P2P
 - Chacun devient responsable lorsqu'il publie des photos ou des blogs
- Vers une nouvelle définition des notions de responsable et de sous-traitant ?

2. Champ d'application géographique



Champ d'application géographique

- Principe de l'établissement
 - Interprétation différente par les États membres
 - Conséquence : application multiple de la législation relative à la vie privée au lieu du principe du passeport européen
 - Principe des moyens automatisés
 - Interprétation très large
 - Discussion sur l' "équipement" et les "moyens"
 - Cookies (⇒ utilisés par la majorité des sites Internet ...)
- Cette large application extraterritoriale de la législation relative à la vie privée est-elle opportune et réaliste ?

3. Formalités



Déclaration

- Vise à inciter à la réflexion, à créer la transparence et à permettre un contrôle. Toutefois :
 - La plupart des entreprises limitent leur obligation aux formalités (peu de réflexion)
 - Quels citoyens contrôlent la banque de données des déclarations ?
 - L'objectif est donc manqué
- Solutions alternatives ?
- Davantage/moins de formalités ?
 - Autoévaluation ?

4. Données sensibles



Données sensibles

- Concept
 - Donnée absolue ou relative (déterminé selon le contexte ou l'objectif) ?
 - Qu'en est-il des autres données sensibles ?
 - P. ex. données financières (comme la solvabilité), données biométriques, origine sociale, etc.
 - Pratiquement pas applicable dans le contexte en ligne
 - Facebook, Netlog, Twitter, blogs, etc.
 - Révision de l'affaire Lindqvist ?
- Comment trouver un équilibre réaliste entre une protection adéquate mais efficace ?

5. Obligations de transparence



Transparence

- Communications à la personne concernée souvent limitées à des politiques de protection de la vie privée interminables et souvent peu significatives
 - Opposabilité des politiques actuelles de protection de la vie privée ?
- Approche alternative ?
- Opter pour une combinaison de déclarations de vie privée et de politiques de vie privée ?
 - "Transparency Enhancing Technologies" ?

6. Droits de la personne concernée



Droits de la personne concernée

- Exercice des droits très difficile dans la pratique si le responsable est établi dans un autre État membre
- Attribuer de nouveaux droits ?
 - Droit à l'oubli ?
 - Droit de cessibilité des données ?

7. Mesures de sécurité



Mesures de sécurité

- Nécessité de directives de sécurité plus spécifiques
 - Normes (par secteur ou par type de données) ?
 - Mesure de sécurité en tant que norme en vertu de la directive 98/34 ?
- Nécessité d'une obligation générale de dénonciation de violation de sécurité ?

Pays tiers



Pays tiers

- La supposition que l'exportation est seulement exceptionnelle et peut donc être liée à des formalités importantes n'est plus exacte
 - L'exportation de données à caractère personnel vers des pays tiers est pratiquement toujours le cas en pratique
 - Applications Internet
 - Informatique en nuages
 - Outsourcing multiple
 - Application rigide des formalités
 - Le consentement de la personne concernée n'est en pratique pas demandé
 - Procédures différentes selon les États membres (contrats types, BCR)
 - Le "Data transfer paradox" entrave la compétitivité des entreprises européennes
 - Paradoxe : importation depuis des pays tiers non soumises à des conditions, exportation soumise à la législation européenne
- Nécessité de revoir la réglementation relative à l'exportation ?
- Black list au lieu de white list ?
 - Liste "Shaded grey"?

9. Conservation de données à caractère personnel



Conservation de données

- Différentes périodes de conservation dans les États membres
 - P. ex. surveillance par vidéosurveillance, fichiers "log", ...
 - Impossibilité d'agir en conformité pour les entreprises actives sur le marché interne
 - Confusion quant à savoir quelle réglementation s'applique

→ Besoin d'harmonisation ou de normes ?

10. Rôle de la Commission vie privée et du Groupe 29



Le rôle de la ou des Commission(s) vie²⁷ privée

- Limité à la loi vie privée ou plus large (vie privée en général)?
 - Poids suffisant sans moyen de sanction propre ?
 - Sollicitation trop importante de la Commission vie privée
 - P. ex. procédures d'autorisation
- Retour à l'essentiel ?
- Uniquement la loi vie privée
 - Plus de poids
 - Pas de tâches complémentaires

Rôle du Groupe 29

- Valeur juridique des avis ?
 - Cohérence du contenu des avis ?
 - Interprétation trop large de la législation ?
- Détermination plus claire du rôle dans la directive ?

Conclusion



Conclusion

- La directive actuelle n'est pas en mesure de relever efficacement les défis. Trop de citoyens et d'entreprises agissent (involontairement) en contradiction avec la loi, tandis que les véritables menaces en matière de vie privée restent dans l'ombre.
- Mesures pratiques
 - Intégration de la transparence dans les logiciels et le hardware ("*privacy by design*")
 - Développer des modèles
 - Politiques de vie privée multicouches
 - Développement de normes
- Mesures légistiques
 - Précision du cadre légal des notions
 - Suppression de l'obligation de déclaration, mais introduction d'une obligation générale de dénoncer les infractions
- Au niveau international
 - Convention vie privée (cf. convention sur la cybercriminalité) ?