

Traitement de données à caractère personnel – défis pour l'avenir

Évolution dans le traitement des données – L'époque des années nonante qui a précédé l'ère de l'Internet a été caractérisée par l'utilisation de systèmes informatiques mainframe, avec un traitement de données centralisé et local. Ces flux de données maîtrisables restaient en outre limités à quelques acteurs. La société de l'information actuelle est fortement déterminée par Internet, avec pour traits de caractère typiques un traitement de données réparti et des flux de données constants. Les réseaux sociaux, le contenu généré par les usagers, l'informatique en nuages et le "Software as a Service" constituent les tendances du Web 2.0 d'aujourd'hui. Le Web 3.0 du futur – avec le web sémantique et l'informatique ubiquitaire – poursuit le développement de ces tendances.

Nouveaux défis – Ces évolutions technologiques entraînent de nouveaux défis. La collecte de données croît considérablement, de même que les contrôleurs de données, les utilisateurs font l'objet d'un profilage détaillé, le contrôle de ses propres données à caractère personnel est souvent devenu une illusion, les données à caractère personnel sont fréquemment conservées et traitées à des emplacements virtuels et des décisions automatisées sont de plus en plus souvent prises sur la base de données à caractère personnel. Se pose alors la question de savoir si l'actuelle réglementation peut résister aux défis de la société de l'information actuelle et future. Dans ce cadre, les points suivants doivent être pris en considération.

1. Champ d'application matériel – *"Toute information concernant une personne physique identifiée ou identifiable"* est considérée comme une donnée à caractère personnel par la législation. Les différents éléments de cette définition sont souvent interprétés de manière très large. C'est en particulier au regard du concept "identifiable" que des discussions subsistent quant à la question de savoir si l'on doit utiliser un concept de données à caractère personnel absolu ou relatif. En ce qui concerne la définition de traitement, il se pose également la question de savoir si l'objectif du législateur est de maintenir le champ d'application aussi large. À l'heure actuelle, chaque traitement se fait en effet au moyen de procédés automatisés (traitement de texte, e-mail, blog, etc.). Enfin, de nombreuses difficultés se posent aussi dans l'application de la distinction entre les responsables et les sous-traitants. Le critère combiné de "finalités et moyens" est en effet souvent partiellement respecté par les différentes parties. En outre, l'interprétation restreinte du "responsable" pose des difficultés dans le contexte de filiales et chacun devient responsable dans le cadre d'applications P2P.

2. Champ d'application géographique – Ce qui importe dans la détermination du champ d'application géographique, ce sont d'une part le principe d'établissement et d'autre part le principe des moyens automatisés. L'interprétation différente de la notion d' "établissement" par les différents États membres de l'UE donne en effet souvent lieu à une application multiple de législations nationales en matière de vie privée. Par ailleurs, le concept de "moyens automatisés" est généralement interprété de manière très large. Les cookies sont par exemple utilisés en tant que moyens automatisés, impliquant que la majorité des sites Internet ayant des visiteurs européens entrent dans le champ d'application.

3. Formalités – L'obligation de déclaration pour les responsables vise actuellement à les inciter à la réflexion, à créer une transparence et à permettre un contrôle. Cet objectif est toutefois manqué du fait que les banques de données de déclarations ne sont que rarement voire jamais contrôlées activement par les citoyens et du fait que de nombreuses entreprises se limitent simplement à la formalité de déclaration sans s'interroger suffisamment sur leur traitement. L'on se demande s'il est souhaitable d'avoir davantage ou moins de formalités et quel rôle l'autoévaluation peut jouer dans ce contexte.

4. Données sensibles – L'interprétation actuelle du concept de "données sensibles" fait l'objet de discussions. Certaines données peuvent en effet être absolument sensibles, tandis que d'autres données sont relativement sensibles et ne deviennent par conséquent sensibles que dans un contexte donné. La définition actuelle exclut également certaines données que les personnes considèrent généralement comme fortement sensibles, comme les données financières. Aussi, le concept actuel se révèle souvent inapplicable dans un contexte en ligne, où des individus divulguent par exemple sur leur blog des données sensibles relatives à des tiers.

5. Transparence – Bien que les responsables du traitement aient une obligation de transparence à l'égard du titulaire des données, celle-ci reste généralement limitée à des clauses de vie privée interminables et vagues, truffées de jargon juridique, ce qui soulève la question de savoir si, et dans quelle mesure, ces clauses répondent aux obligations de transparence. On peut opter, à titre d'alternative, pour une combinaison de déclarations relatives à la vie privée et de clauses de vie privée, et l'on peut analyser plus avant les possibilités des Transparency Enhancing Technologies (TETs).

6. Droits de la personne concernée – D'une part, il est souvent difficile pour les personnes concernées d'exercer leurs droits étant donné que les responsables du traitement sont souvent établis dans d'autres États membres. D'autre part, il se pose la question de savoir si des droits complémentaires doivent être attribués à la personne concernée, comme par exemple le droit de cessibilité des données et le droit à l'oubli, même si le responsable a obtenu les données avec le consentement de la personne concernée et s'est réservé le droit de les utiliser ultérieurement.

7. Mesures de sécurité – Pour les responsables du traitement, il y a souvent une incertitude au sujet des mesures de sécurité qu'ils doivent prendre. Des directives de sécurité plus spécifiques sont dès lors nécessaires, lesquelles peuvent éventuellement prendre la forme de normes par secteur ou par type de données. Il convient à cet égard d'analyser plus en détail si, et dans quelle mesure, de telles directives de sécurité spécifiques doivent être considérées comme norme ou prescription technique en vertu de la Directive 98/34. Par ailleurs, une généralisation de l'obligation de déclaration en cas de violation de la sécurité (telle que reprise dans la directive e-privacy) est recommandée.

8. Délais de conservation – En ce qui concerne la période de conservation des données à caractère personnel, il existe pour certains traitements des délais de conservation maximaux imposés légalement dans les différents États membres (par exemple pour la vidéosurveillance, les fichiers "log", ...). Pour les entreprises actives sur le marché interne, il est quasiment impossible d'agir en conformité avec la réglementation locale. On ne sait en outre pas clairement quelle réglementation

s'applique en raison du caractère réparti du traitement de données. Une harmonisation des délais de conservation et l'utilisation de normes seraient dès lors recommandées.

9. Pays tiers – L'exportation de données à caractère personnel vers des pays tiers constitue à l'heure actuelle plus la règle que l'exception. L'application rigide des formalités rend souvent difficile l'exportation de données par les entreprises. Ainsi, les procédures de contrats types et les règles d'entreprise contraignantes sont par exemple différentes en fonction des États membres. En outre, le "data transfer paradox" entrave souvent la compétitivité des entreprises européennes. Il arrive en effet que des données à caractère personnel reçues de pays tiers et traitées en Europe ne puissent pas être renvoyées dans le pays d'origine, alors que ces données ont été collectées conformément au droit local.

10. Rôle de la Commission vie privée et du Groupe 29 – Concernant les commissions nationales de protection de la vie privée, la question se pose de savoir si leur fonctionnement peut concerner la vie privée en général ou s'il doit être limité au traitement de données à caractère personnel. L'absence d'un moyen de sanction propre a pour conséquence dans certains États membres (comme la Belgique) que la commission vie privée ne dispose pas suffisamment de poids pour agir à l'encontre d'infractions graves. En ce qui concerne le Groupe 29, la valeur juridique de ses avis est imprécise. De plus, le contenu des avis du Groupe 29 est parfois incohérent, ce qui donne lieu à un manque de clarté. En outre, on peut se demander si le Groupe 29 ne va pas trop loin dans son interprétation de la directive et si son rôle ne doit pas être défini plus clairement dans la directive.

Conclusion – La directive actuelle se révèle ne pas être en mesure de relever efficacement les défis actuels et futurs. Trop de citoyens et d'entreprises agissent (involontairement) en contradiction avec la loi, tandis que les véritables menaces en matière de vie privée restent souvent dans l'ombre. Au niveau pratique, l'intégration de la transparence dans les logiciels et le hardware, le développement de modèles, les politiques de vie privée multicouches et le développement de normes doivent être davantage stimulés. Complémentairement, une précision du cadre légal des notions s'impose et l'obligation de déclaration doit être remplacée par une obligation générale de déclaration en cas de violation de la sécurité. Au niveau international, on peut œuvrer davantage à une convention vie privée, afin de garantir un niveau de protection minimal dans le monde entier.