



## COMMUNIQUÉ DE PRESSE

EDPS/2013/06

Bruxelles, lundi 17 juin 2013

### Respect de la vie privée et confiance doivent être les fondements de toute stratégie de cybersécurité crédible en Europe

La cybersécurité ne peut servir de prétexte à la **surveillance illimitée** et l'analyse de données personnelles, annonce le Contrôleur européen de la protection des données (CEPD) dans son **avis rendu sur la stratégie de l'UE en matière de cybersécurité**. Bien qu'elle reconnaisse à juste titre l'importance des principes de protection des données pour une politique solide en matière de sécurité des réseaux et de l'information, **la stratégie n'est pas claire** sur la façon dont ces principes seront appliqués en pratique pour renforcer la sécurité des personnes, de l'industrie, des gouvernements et d'autres organisations.

Peter Hustinx, CEPD, déclare: "*La sécurité passe par la protection de la vie privée; je suis donc ravi que la stratégie de l'UE reconnaisse qu'il n'y a pas d'opposition entre respect de la vie privée et cybersécurité, et que les **principes de protection des données personnelles** servent plutôt que ne desservent. Toutefois ces ambitions légitimes ne se reflètent pas dans son implémentation pratique. Nous reconnaissons volontiers que les questions de cybersécurité doivent être abordées au niveau international au travers de normes internationales et la coopération, mais si l'UE veut coopérer sur la cybersécurité avec d'autres pays, dont les Etats-Unis, cela doit forcément passer par une **confiance mutuelle** et le **respect des droits fondamentaux**, prémisses qui paraissent actuellement compromises*".

L'objectif global de la stratégie de l'UE est de **rendre l'utilisation de l'Internet** et de tout réseau et système d'information connecté, **plus sûre** en permettant aux organisations dans les pays de l'UE de prévenir et réagir aux cyberattaques et perturbations. Le résultat vise à favoriser la confiance des personnes et organisations sur Internet. Toutefois, la communication de la Commission ne tient pas suffisamment compte du rôle du cadre légal de protection des données et des propositions actuelles, telles que le projet de règlement sur la protection des données et le règlement *eTrust*. Elle ne considère également pas l'importance de la prise en compte de la protection des données dès la création même d'un système de cybersécurité - **privacy by design** – pourtant garante de la confiance des utilisateurs. Le résultat en est que la stratégie n'est pas aussi efficace et complète que la Commission le souhaite.

Bien que des mesures pour assurer la cybersécurité peuvent nécessiter l'analyse de certaines données personnelles, notamment des adresses IP qui peuvent permettre d'identifier des individus spécifiques, la cybersécurité peut jouer un **rôle fondamental** pour assurer le respect de la vie privée et la protection des données personnelles en ligne, à condition que le traitement de ces données soit **proportionné, nécessaire et légitime**.

Les **autorités nationales de protection des données** jouent un **rôle significatif** pour assurer un niveau approprié de sécurité dans le traitement des données personnelles, y compris sur Internet, et dans les réseaux et systèmes d'information, et pour **sensibiliser** aux règles qui s'appliquent aux particuliers et organisations dans les pays de l'UE. Par ailleurs, elles doivent être informées de toute nouvelle opération impliquant le traitement de données personnelles et de toute violation de données. Les agences comme Europol, ENISA et autres énumérées dans la stratégie doivent également assurer la liaison avec elles dans l'exercice de leurs tâches. Bien que cela ne se reflète pas dans la stratégie, leur rôle en matière de cybersécurité doit être reconnu.

## **Informations générales**

Le 7 février 2013, la Commission et la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité ont adopté une communication conjointe pour le Parlement européen, le Conseil, le Comité économique et social européen et le Comité des régions sur la "**Stratégie de cybersécurité de l'Union européenne: un cyberspace ouvert, sûr et sécurisé**".

Le même jour, la Commission a adopté une proposition de **directive** du Parlement européen et du Conseil relative à des **mesures pour assurer un niveau commun élevé de sécurité des réseaux et de l'information à travers l'Union**. Cette proposition a été envoyée au CEPD pour consultation le 7 février 2013.

Le respect de la vie privée et la protection des données sont des droits fondamentaux dans l'UE. Dans le cadre du [règlement sur la protection des données \(CE\) n° 45/2001](#), l'une des fonctions du CEPD est de conseiller la Commission européenne, le Parlement européen et le Conseil sur les propositions de nouvelle législation et un large éventail d'autres questions qui ont un impact sur la protection des données. En outre, les institutions et organes de l'UE traitant des données personnelles qui présentent des risques particuliers pour les droits et les libertés des individus sont soumis à un contrôle préalable par le CEPD. Si, de l'avis du CEPD, le traitement notifié risque d'entraîner une violation d'une disposition du règlement, il doit faire des propositions afin d'éviter une telle violation.

**Données personnelles:** toute information concernant une personne physique identifiée ou identifiable. Les exemples sont le nom, la date de naissance, les photographies, les adresses e-mail et les numéros de téléphone. D'autres informations telles que les données de santé, les données utilisées à des fins d'évaluation et les données d'utilisation du téléphone, de l'e-mail ou de l'Internet sont également considérées comme des données personnelles.

**Respect de la vie privée:** droit d'un individu à être laissé seul et à contrôler l'information le concernant. Le droit à la vie privée est consacré par la Déclaration universelle des Droits de l'Homme (article 12), la Convention européenne des Droits de l'Homme (article 8) et la Charte européenne des Droits fondamentaux (article 7). La Charte contient également un droit explicite à la protection des données à caractère personnel (article 8).

**Privacy by design:** concept qui promeut l'intégration de la protection des données dès la conception et la définition de l'architecture des systèmes et technologies de l'information et de la communication, afin de se conformer aux principes de respect de la vie privée et de la protection des données.

**Limitation de la finalité:** les données personnelles ne peuvent être collectées qu'à des fins déterminées, explicites et légitimes. Une fois collectées, elles ne peuvent être traitées de manière incompatible avec ces finalités. Le principe est conçu pour protéger les individus en limitant l'utilisation de leurs données à des fins prédéfinies, sauf dans des conditions strictes et avec des garanties appropriées.

**Violation de données:** toutes données personnelles détenues par une organisation (généralement un fournisseur de télécommunications) qui sont (accidentellement ou délibérément) perdues, volées, détruites, modifiées, interceptées ou divulguées.

Le Contrôleur européen de la protection des données (CEPD) est une autorité de contrôle indépendante dont l'objectif est de protéger les données à caractère personnel et la vie privée et de promouvoir les bonnes pratiques dans les institutions et organes de l'UE. À cet effet, il remplit les tâches suivantes:

- contrôler les traitements de données à caractère personnel effectués par l'administration de l'UE;
- donner des conseils sur les politiques et les textes législatifs qui touchent à la vie privée;
- coopérer avec les autorités de même nature afin de garantir une protection des données qui soit cohérente.

---

[L'avis du CEPD](#) (EN) est disponible sur le site Internet. Pour plus d'informations: [press@edps.europa.eu](mailto:press@edps.europa.eu)

**CEPD - Le gardien européen de la protection des données**

[www.edps.europa.eu](http://www.edps.europa.eu)



Suivez-nous sur Twitter: [@EU\\_EDPS](https://twitter.com/EU_EDPS)