GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

WP227

DECLARATION COMMUNE DES AUTORITES EUROPEENNES DE PROTECTION DES DONNEES REUNIES AU SEIN DU GROUPE DE L'ARTICLE 29

Adopté le 26 novembre 2014

Introduction

Notre vie quotidienne est numérique. En moins d'une décennie, nos activités professionnelles, économiques, privées ont migré vers le monde numérique. Cette évolution a ouvert un monde d'opportunités nouvelles. Elle permet le développement de biens et de services extraordinairement innovants, qui satisfont à des demandes tant individuelles que collectives. Les données à caractère personnel constituent la particule élémentaire de ce monde numérique.

Le fonctionnement de l'environnement numérique repose sur des infrastructures informationnelles complexes que des acteurs privés ont développées pour leurs besoins propres. Ceux-ci amassent des quantités gigantesques de données personnelles que certains d'entre eux stockent, traitent et partagent souvent sans laisser à l'individu un niveau de contrôle suffisant et sans être soumis à une supervision effective. Par ailleurs, comme les révélations d'Edward Snowden l'ont récemment dévoilé, des autorités publiques et des services de renseignement ont exigé d'avoir un accès massif à ces infrastructures de données pour d'autres finalités, notamment celle de sécurité nationale.

Le caractère massif et routinier de cet accès a choqué le monde entier. Désormais, le défi consiste à remédier à la crise de confiance que ces révélations ont générée envers les gouvernements (nationaux et étrangers) et les services de renseignement et de surveillance. Il s'agit également de régler la question sous-jacente du contrôle de l'accès à ces quantités gigantesques de données personnelles. Comment construire un cadre qui permette à la fois aux entreprises privées et aux organisations d'innover, d'offrir des produits et services qui répondent aux demandes des consommateurs et aux besoins publics, aux services de surveillance et de renseignement de remplir leurs missions dans le cadre de la loi, et de ne pas sombrer pour autant dans une société de surveillance ?

Du fait de son histoire et de sa culture communes, l'Europe doit faire entendre sa voix sur les moyens d'assurer le respect des droits fondamentaux, parmi eux la protection de la vie privée et la protection des données à caractère personnel, sans faire obstacle ni à l'innovation, ni au besoin d'assurer la sécurité de nos sociétés. Les autorités indépendantes de protection des données de l'Union européenne, rassemblées au sein de leur groupe de coordination, dit « Groupe de l'Article 29 », ont souhaité faire connaître plusieurs messages essentiels quant à la manière d'atteindre un tel objectif.

C'est pourquoi le Groupe de l'Article 29, lors de sa séance plénière du 25 novembre 2014, a adopté la Déclaration suivante :

Valeurs européennes

1. **La protection des données à caractère personnel est un droit fondamental.** Les données à caractère personnel (y compris les métadonnées de communication) ne peuvent être traitées comme un seul objet de commerce, un actif économique ou un bien de consommation.

2. **Les droits des personnes au regard de la protection de leurs données doivent être combinés avec les autres droits fondamentaux,** notamment la prohibition de toute discrimination et la liberté d'expression, qui sont de valeur égale dans toute société démocratique. Ils doivent également être articulés avec l'impératif de sécurité.

3. **La technologie est un moyen qui doit demeurer au service de l'homme.** Le fait qu'un traitement de données soit techniquement faisable, qu'il puisse parfois révéler des informations utiles au renseignement ou permettre le développement de nouveaux services n'implique pas qu'il soit de ce fait acceptable sur les plans social et éthique, ni qu'il soit raisonnable ou conforme à la loi.

4. **La confiance du public dans les produits et services de l'économie numérique** dépend en grande partie du respect des règles de protection des données par l'industrie. Le respect de ces règles constitue un facteur concurrentiel fondamental pour les acteurs numériques ; il assurera la durabilité du développement de l'industrie numérique, au bénéfice de celle-ci comme de celui des consommateurs.

5. **La prise de conscience et les droits des personnes** doivent être renforcés pour permettre à celles-ci de limiter leur exposition à un risque de surveillance excessive par les acteurs publics ou privés. L'amélioration de l'éducation au numérique, y compris à la protection des données, et la faculté d'initier des actions judiciaires collectives permettant de dénoncer des violations généralisées des données personnelles constituent des mesures clés dans cette perspective.

Surveillance à des fins de sécurité

6. **La surveillance secrète, massive et indiscriminée** de personnes en Europe, que ce soit pas des acteurs publics ou privés, qu'ils agissent au sein des Etats membres de l'Union ou ailleurs, n'est pas conforme aux Traités et législation européens. Elle est inacceptable sur le plan éthique.

7. **L'accès à des données à caractère personnel aux fins de sécurité n'est pas acceptable dans une société démocratique dès lors qu'il est massif et sans condition**. La conservation, l'accès et l'utilisation de données par les autorités nationales compétentes doivent être limitées à ce qui est strictement nécessaire et proportionné dans une société démocratique. Elles doivent être soumises à des garanties substantielles et effectives.

8. **Le traitement de données personnelles dans le cadre d'activités de surveillance** ne peut avoir lieu que dans le cadre de garanties appropriées définies par la loi, conformément à l'article 8 de la Charte européenne des droits fondamentaux. Parmi ces garanties, figure l'exigence d'un **contrôle indépendant et effectif**, auquel les autorités de protection des données doivent être associées selon leurs compétences.

9. L'autorité publique d'un Etat non membre de l'Union ne peut par principe **accéder directement à des données personnelles couvertes par les règles européennes**, quelles que soient les conditions de cet accès ou la localisation de ces données. D'éventuels conflits de juridiction ne pourront être résolus que sous certaines conditions – telles que l'autorisation préalable d'une autorité publique de l'Union ou l'application d'un traité d'entraide judiciaire, concernant respectivement l'accès d'autorités étrangères à des données transférées depuis l'Union ou à des données stockées dans l'Union. Des demandes d'accès émanant de l'étranger ne peuvent être adressées directement aux sociétés soumises au droit de l'Union.

10. Aucune des dispositions figurant dans les **instruments européens visant à encadrer les transferts internationaux de données** entre parties privées ne peut servir de base légale à des transferts de données vers les autorités de pays tiers pour des finalités de surveillance massive et indiscriminée - que ce soit celles de la Sphère de sécurité (« Safe Harbor »), de règles d'entreprise contraignantes (« BCR ») ou des clauses contractuelles types.

11. Dès lors que des entités publiques ou privées collectent des quantités massives de données fournissant des informations très précises sur les vies privées des personnes dont les données sont conservées, elles doivent organiser le stockage de ces données de manière à permettre le contrôle par une autorité européenne indépendante, du respect des exigences de protection des données. Le **stockage de ces données sur le territoire de l'Union** est un moyen effectif de faciliter l'exercice de ce contrôle**.**

Influence européenne

12. **Les projets européens de règlement et de directive relatifs à la protection des données doivent être adoptés en 2015**. Outre contribuer à l'unification du marché numérique européen, ces textes doivent assurer un haut niveau de protection des données aux personnes, conforme aux valeurs et droits fondamentaux de l'Europe.

13. Le niveau européen de protection des données ne peut être érodé, en tout ou partie, par des accords bilatéraux ou internationaux**, y compris des accords commerciaux** sur les biens et services à conclure avec des pays tiers.

14. Les règles de protection des données de l'Union sont nécessaires à la sauvegarde de la situation politique, sociale and économique de l'Union et de ceux qui sont soumis à la législation de l'Union. Elles doivent être considérées comme des principes internationaux impératifs en **droit international public et privé**. Des lois étrangères ou des accords internationaux ne peuvent leur passer outre et les organisations ne peuvent y déroger par contrat.

15. L'équilibre à établir entre protection des données, innovation et surveillance n'implique **ni de reconstruire les frontières internes de l'Union ni de fermer les portes de l'Europe** à des partenariats étrangers. Il exige de respecter le haut niveau de protection découlant de l'héritage européen de protection des données que consacrent la Convention 108 du Conseil de l'Europe et les règles de protection des données de l'Union.

Suivi de la Déclaration

16. Le Groupe de l'article 29 ouvre cette Déclaration aux commentaires **de toute partie intéressée**, qu'elle soit de statut public ou privé. Ces commentaires peuvent lui être adressés par l'intermédiaire du site Web disponible à l'adresse www.europeandatagovernance-forum.com. Le Groupe tiendra compte de ces commentaires dans ses activités de l'année 2015.