Parlement européen

Background

# Q&R: Les nouvelles règles de l'UE sur la protection des données placent les citoyens aux commandes

[01-06-2016 - 14:19]

**La nouvelle législation européenne sur la protection des données vise à créer un ensemble de règles uniformes à travers l'UE adaptées à l'ère numérique, à améliorer la sécurité juridique et à renforcer la confiance des citoyens et entreprises dans le marché unique du numérique. Un consentement clair et positif au traitement des données, le droit à l'oubli et de lourdes amendes pour les entreprises enfreignant les règles sont quelques-unes des nouvelles fonctionnalités.**

Le Parlement européen a finalisé plus de quatre ans de négociations lorsque les députés ont adopté la législation en commission des libertés civiles le mardi 12 avril suivi d'un vote en plénière à Strasbourg le jeudi 14 avril.

La révision porte sur deux textes législatifs: un règlement général sur le traitement des données personnelles dans l'UE et une directive sur les données traitées par les autorités policières et judiciaires qui forment ensemble le paquet sur la protection des données.

Le règlement remplace la directive sur la protection des données de l'UE, qui date de 1995 alors qu'Internet était encore à ses débuts, et convertit le patchwork actuel des législations nationales en un ensemble unique de règles en vue de donner aux citoyens plus de contrôle sur leurs propres informations privées dans un monde numérique de téléphones intelligents, de médias sociaux, de services bancaires sur Internet et de transferts mondiaux. Cela permet également de créer la clarté juridique pour les entreprises afin de stimuler l'innovation et le développement futur du marché unique du numérique. Le règlement sur la protection des données renforce la confiance et fournit un niveau élevé de protection pour tous les citoyens de l'UE, quelles que soient les circonstances dans lesquelles leurs données personnelles sont traitées, sauf si elles le sont à des fins d'application de la loi (ce cas est couvert par la directive) et s'applique également à des entreprises hors Europe ciblant les consommateurs de l'UE.

La directive sur la protection des données couvre le traitement des données par le secteur de la police et de la justice pénale. Elle vise à assurer que les données des victimes, des témoins et des suspects de crimes soient dûment protégées dans le cadre d'une enquête pénale ou d'une action d'application de la loi. Dans le même temps, des législations plus harmonisées faciliteront également la coopération transfrontalière de la police ou des procureurs afin de lutter plus efficacement contre la criminalité et le terrorisme à travers l'Europe.

Après que le Conseil ait adopté officiellement l'ensemble du paquet sur la protection des données en première lecture le vendredi 8 avril, le Parlement a enfin pu conclure plus de quatre années de négociations qui ont débuté lorsque la Commission a présenté ses propositions en janvier 2012. Le Parlement a voté sa position en première lecture en mars 2014, mais a dû attendre plus d'un an pour que les États membres conviennent de leur position de négociation commune avant que les trilogues entre le Parlement, le Conseil et la Commission puissent commencer en juin 2015. Dans le cas de la directive, le Conseil a conclu un compromis sur son mandat de négociation en octobre 2015.

Un accord informel a été conclu le 15 décembre 2015 et adopté par le Parlement et le Conseil respectivement les 17 et 18 décembre. Depuis lors, le Parlement a demandé à plusieurs reprises au Conseil d'achever ses travaux sur les textes pour permettre une entrée en vigueur rapide des exigences plus strictes en matière de protection des données. En particulier, une majorité de députés ont toujours souligné la nécessité

urgente et indispensable de garantir un niveau suffisant de protection des données comme énoncé dans la directive sur la protection des données, avant de permettre la collecte massive de données relatives aux passagers de vol prévue par la directive européenne PNR, qui sera également votée lors de la session plénière d'avril 2016 à Strasbourg.

Le vote en plénière qui a eu lieu le jeudi 14 avril a marqué la dernière étape de la procédure législative. Le règlement sur la protection des données est entré en vigueur le 24 mai 2016, soit 20 jours après sa publication au Journal officiel de l'UE le 4 mai 2016. Ses dispositions sont directement applicables dans tous les États membres. Les États membres ont deux ans pour transposer les dispositions de la directive dans leur législation nationale, onc avant le 4 mai 2018.

**Contact**

**Rikke ULDALL**
BXL: (+32) 2 28 42976
STR: (+33) 3 881 72033
PORT: (+32) 498 98 32 57
EMAIL: libe-press@europarl.europa.eu
TWITTER: EP_Justice

## Qu'impliquent les dispositions du nouveau règlement sur la protection des données?

Le règlement met à jour et modernise les principes inscrits dans la directive de 1995 sur la protection des données afin de garantir le droit à la vie privée. Il se concentre sur les éléments suivants: renforcer les droits individuels et le marché intérieur de l'UE, garantir une mise en œuvre plus stricte des règles, faciliter les transferts internationaux de données à caractère personnel, et mettre en place des normes internationales de protection des données. La réforme représente une étape essentielle pour renforcer les droits fondamentaux des citoyens à l'ère numérique et pour faciliter les échanges commerciaux en simplifiant les règles pour les entreprises.

**Grâce aux nouvelles règles, les citoyens peuvent davantage contrôler leurs données personnelles de la manière suivante:**

**Le droit à l'oubli (article 17)**

Les personnes disposent du droit à l'oubli, c'est-à-dire l'effacement de leurs données personnelles lorsqu'elles ne souhaitent plus que leurs données soient traitées, à condition qu'il n'existe aucune raison légitime de les conserver.

Dans l'application de ce droit, si une personne demande à une entreprise Internet d'effacer ses données, cette entreprise devra également envoyer la demande à toute autre partie qui duplique les données. Cependant, ce droit serait limité dans certains cas, par exemple lorsque les données sont nécessaires à des fins historiques, statistiques ou de recherche scientifique, pour des raisons de santé publique, ou pour l'exercice du droit à la liberté d'expression. Le droit à l'oubli ne s'appliquerait pas non plus lorsque la détention des données à caractère personnel est nécessaire pour la conclusion d'un contrat ou lorsque la loi l'exige.

**Mieux contrôler les parties qui détiennent des données privées (article 7)**

La personne concernée (sujet des données) doit donner son **consentement clair et explicite** au traitement de ses données privées, c'est-à-dire que l'individu doit donner son consentement de manière active. Il doit par exemple cocher une case lors de la visite d'un site Internet ou effectuer une autre action ou faire une déclaration indiquant l'acceptation du traitement proposé des données personnelles. Le silence, des cases cochées par défaut ou l'inactivité ne constituent donc pas un consentement. À l'avenir, une personne peut également plus facilement revenir sur son consentement.

**Droit de transmettre les données personnelles d'un individu à un autre fournisseur de services (article 20)**

Conformément aux nouvelles règles, toute personne jouit du droit à la "portabilité des données" afin que les individus puissent transmettre plus facilement des données à caractère personnel entre fournisseurs de services. Ce droit permet par exemple à un utilisateur de changer de fournisseur de messagerie électronique sans perdre ses contacts ou ses courriels. Les individus peuvent ainsi mieux contrôler leurs données et la concurrence sur le marché numérique unique se voit également renforcée.

**Droit d'être informé dans un langage simple et clair (articles 12, 13 et 14)**

Les députés ont insisté pour que les nouvelles dispositions mettent un terme aux politiques de vie privée "en petits caractères". Avant la collecte des données, des informations doivent être fournies dans un langage clair et simple.

**Droit d'être informé en cas de piratage des données (articles 33 et 34)**

Les entreprises et organisations sont tenues d'informer sans délai l'autorité de surveillance nationale en cas de violation grave des données afin que les utilisateurs puissent prendre les mesures appropriées.

**Limitations claires au recours au profilage (article 21)**

Les nouvelles dispositions fixent des limites au profilage, une technique utilisée pour analyser ou prédire les performances d'une personne au travail, sa situation économique, sa localisation, sa santé, ses préférences, sa fiabilité ou son comportement grâce au traitement automatique de ses données personnelles.

Conformément au règlement, le profilage est, en règle générale, uniquement autorisé si la personne concernée donne son consentement, si la loi le permet et s'il est nécessaire à la conclusion d'un contrat. Les députés ont également précisé que le profilage ne devrait pas entraîner de discrimination ou se baser uniquement sur des données sensibles (telles que les données révélant, entre autres, l'origine ethnique, les opinions politiques, la religion, l'orientation sexuelle, les données génétiques ou biométriques, des sanctions administratives ou des suspicions).

De plus, le profilage ne devrait pas se baser uniquement sur le traitement automatique des données. Il doit comprendre une évaluation menée par l'homme, incluant une explication de la décision conclue après un tel examen. Ce système pourrait influer sur la manière dont la solvabilité est évaluée par exemple.

**Protection spéciale pour les enfants (article 8)**

Les nouvelles règles prévoient des garanties spéciales pour les enfants dans certains domaines, étant donné qu'ils peuvent être moins conscients des risques et conséquences liés au partage de leurs données personnelles. Ils bénéficient ainsi d'un droit à l'oubli plus clair.

Par ailleurs, les dispositions stipulent qu'en dessous d'un certain âge, les enfants doivent avoir la permission de leurs parents ("autorisation parentale") pour ouvrir un compte sur les réseaux sociaux, tels que Facebook, Instagram ou Snapchat, comme c'est déjà le cas avant dans la plupart des pays de l'UE. Il revient aux États membres de déterminer la limite d'âge qui devra être située entre 13 et 16 ans.

Ce seuil flexible est un compromis conclu pendant les négociations afin de permettre aux États membres de maintenir les règles déjà en place à l'heure actuelle. Le Parlement aurait préféré que la limite d'âge pour l'autorisation parentale soit fixée à 13 ans dans l'ensemble de l'UE (soit la même limite que celle proposée à l'origine par la Commission européenne).

L'objectif de cette disposition spécifique est de protéger les enfants contre la pression les poussant à partager leurs données personnelles sans en réaliser pleinement les conséquences. Cela n'empêchera pas les adolescents d'utiliser Internet pour obtenir des informations, des conseils, des formations, etc. De plus, les règles précisent que les enfants en dessous de la limite d'âge n'auront pas à demander à leurs parents la permission d'utiliser des services de conseil ou de prévention offerts directement à leur intention.

**Le respect de la vie privée comme norme**

Les entreprises doivent concevoir des fonctionnalités par défaut et des produits de sorte à collecter et traiter le moins possible de données à caractère personnel. La "protection de la vie privée dès la conception" et par défaut devient un principe essentiel et encourage les entreprises à innover et développer de nouvelles idées, méthodes et technologies pour la sécurité et la protection des données personnelles.

# Background

## En quoi consiste le "paquet sur la protection des données"?

Le paquet sur la réforme de la protection des données se compose de deux projets législatifs: un **règlement** général couvrant la majeure partie du traitement des données personnelles dans l'UE et une **directive** sur le traitement des données pour prévenir, enquêter, détecter ou poursuivre les infractions pénales ou appliquer des sanctions pénales.

Le règlement met à jour les principes énoncés dans une directive de 1995, de manière à suivre le rythme des changements majeurs apportés par Internet dans le traitement des données. Il couvre, par exemple, les données traitées sur Internet, comme pour les réseaux sociaux, les services commerciaux et bancaires en ligne et hors ligne, pour les registres des hôpitaux et des universités, les registres de clients des sociétés et des données personnelles à des fins de recherche. Le député en charge du projet de règlement est Jan Philipp Albrecht (Verts/ALE, DE).

La directive vise à remplacer une décision-cadre de 2008 (2008/977/JHA) sur le traitement des données transfrontalières pour la coopération policière et judiciaire. Elle est destinée à protéger les transferts de données à la fois nationaux et transfrontaliers. Elle définit également un niveau élevé de protection des données pour les citoyens. La députée en charge du projet de directive est Marju Lauristin (S&D, ET).

Le paquet sur la protection des données est un élément clé du marché unique du numérique et de l'agenda de l'UE sur la sécurité.

## Quels sont les avantages pour les entreprises?

La réforme prévoit la clarté et la cohérence des règles à appliquer en remplaçant l'actuelle mosaïque de lois nationales par une unique législation européenne. Les avantages sont estimés à 2,3 milliards d'euros par an, selon la Commission européenne.

Un nouveau **système centralisé** pour les entreprises signifie qu'elles n'ont à faire face qu'à une autorité de surveillance unique, pas 28, ce qui leur permettra de faire des affaires dans l'UE de manière plus simple et moins coûteuse. Dans le même temps, cela aura également un impact sur la surveillance des géants d'Internet avec des bureaux dans plusieurs pays de l'UE.

En outre, **les règles sont applicables à toutes les entreprises ciblant les consommateurs de l'UE**, indépendamment du fait qu'elles soient établies à l'intérieur ou à l'extérieur de l'UE. Le règlement énonce clairement que les entreprises basées en dehors de l'UE doivent respecter les mêmes normes que celles qui proposent des biens et des services sur le marché de l'UE. Cela contribue à créer une concurrence équitable pour toutes les entreprises opérant au sein de l'Union.

En disposant d'une règle au lieu de 28, la réforme de la protection des données de l'UE va également aider les **petites et moyennes entreprises** à pénétrer de nouveaux marchés. Dans un certain nombre de cas, les obligations des contrôleurs et processeurs de données sont adaptés à la taille de l'entreprise et / ou à la nature des données en cours de traitement pour éviter les formalités administratives et la création de charges disproportionnées pour les plus petites entreprises.

## Comment seront appliquées les nouvelles règles?

Pour assurer leur application correcte, les nouvelles règles de protection des données vont à la fois renforcer les pouvoirs des agents de protection des données et permettre des amendes importantes en cas de violations.

**Les entreprises devront désigner un responsable de la protection des données** si elles gèrent des quantités importantes de données sensibles ou surveillent le comportement de nombreux consommateurs. Les entreprises dont l'activité principale n'est pas le traitement de données seront exemptées de cette obligation afin d'éviter les procédures administratives.

**Des amendes allant jusqu'à 4% du chiffre d'affaires mondial des entreprises** devraient constituer un véritable moyen de dissuasion à enfreindre les règles.

## Quelles sont les implications de la nouvelle directive sur les échanges de données dans le secteur de l'application de la loi?

La directive sur les transferts de données à des fins policières et judiciaires fixe des normes élevées en matière de protection des données afin de garantir les droits et libertés des citoyens tout en permettant aux forces de police à travers l'Europe de coopérer de manière plus rapide et plus efficace pour lutter contre la criminalité grave et le terrorisme.

Elle applique aux services répressifs les mêmes dispositions sur la protection des données que celles prévues par le règlement, avec les adaptations nécessaires aux spécificités du secteur. Elle innove en harmonisant à grande échelle les diverses méthodes nationales présentes au sein de l'UE pour traiter les données à des fins d'application de la loi, et, pour la première fois, elle fixe des normes de protection minimales pour les transferts de données au sein de chaque État membre.

S'ils le souhaitent, les pays de l'UE peuvent prévoir des normes plus élevées que celles énoncées dans la directive.

**Comment les règles protègent-elles les citoyens?**

La directive protège les individus dont les données sont traitées à des fins de prévention et de détection d'infractions pénales, ainsi que d'enquêtes et de poursuites en la matière. Les garanties s'appliquent à tous, qu'il s'agisse de la victime, du criminel ou du témoin, et prévoient des droits clairs pour les individus. Tous les traitements de données liés à l'application de la loi dans l'UE doivent répondre aux principes de nécessité, de proportionnalité et de légalité, avec des garanties appropriées pour les individus. Les données à caractère personnel devraient être traitées de manière licite, loyale et seulement à des fins spécifiques. Un contrôle sera assuré par les autorités indépendantes nationales de protection des données disposant de pouvoirs d'exécution.

Les règles s'appliquent tant au niveau national dans les États membres que de manière transfrontalière au sein de l'UE. La décision-cadre, qui est maintenant remplacée, couvrait uniquement les échanges transfrontaliers de données. La directive prévoit aussi des règles strictes pour le transfert de données à caractère personnel vers les pays tiers et les organisations internationales, afin d'assurer un niveau élevé de protection des données lors de tels transferts.

**Quelles seront les conséquences des dispositions sur la coopération judiciaire pénale?**

Avoir la même législation dans l'UE facilitera la coopération des autorités répressives pénales dans l'échange d'informations, créant ainsi des conditions pour une lutte plus efficace contre la criminalité.

De plus, la directive complète les dispositions récentes sur le nouveau règlement d'Europol et sur la directive établissant un système de collecte des données des passagers aériens de l'UE (PNR) en imposant des normes élevées et uniformes en matière de transferts de données à des fins d'application de la loi.

## Faits et chiffres

Un nombre record de 3133 amendements à la proposition de règlement de la Commission européenne ont été déposés en commission des libertés civiles. Avec les amendements déposés dans les avis en commission de l'industrie (417), en commission du marché intérieur (226), en commission de l'emploi (27) et en commission des affaires juridiques (196), le nombre total d'amendements s'élève à **3999**. Il s'agit du plus grand nombre d'amendements jamais déposés pour **un seul dossier législatif** au Parlement.

Les groupes politiques du Parlement ont négocié 91 amendements de compromis, combinant les amendements déjà déposés, afin de faciliter le vote sur le règlement.

673 amendements à la proposition de directive ont été déposés en commission des libertés civiles. Avec les amendements déposés pour avis en commission des affaires juridiques (98), le nombre total d'amendements s'élève à 771.

Les groupes politiques du Parlement ont négocié 64 amendements de compromis, combinant les amendements déjà déposés, afin de faciliter le vote sur la directive.

La liste de vote pour le règlement compte 261 pages et celle pour la directive 57 (318 pages au total).

Au moment du vote en plénière en mars 2014, la réforme sur la protection des données avait été débattue pendant 20 mois. Les débats officiels en commission ont duré environ 30 heures. Les négociations informelles entre les groupes politiques ont duré 250 heures.

## Quels sont les principaux députés responsables de cette réforme?

- Jan Philipp Albrecht (Verts/ALE, DE) est le rapporteur pour le règlement.
- Marju Lauristin (S&D, ET) est la rapporteur pour la directive.

L'équipe de négociation du Parlement pour le **règlement** est composée de: Claude Moraes (S&D, UK), président de la commission des libertés civiles, Jan Philipp Albrecht (rapporteur), ainsi qu'Axel Voss (PPE, DE), Marju Lauristin, Timothy Kirkhope (ECR, UK), Sophia in't Veld (ADLE, NL), Cornelia Ernst (GUE/NGL, DE) et Kristina Winberg (EFDD, SV) en tant que rapporteurs fictifs. Les auteurs des avis en commission de l'industrie, Sean Kelly (PPE, IE), et en commission du marché intérieur, Lara COMI (PPE, IT), ont également participé aux trilogues.

L'équipe de négociation du Parlement pour la **directive** est composée de: Claude Moraes, président de la commission des libertés civiles, Marju Lauristin (rapporteur), ainsi qu'Axel Voss, Timothy Kirkhope, Sophia in't Veld, Cornelia Ernst, Jan Philipp Albrecht, et Kristina Winberg en tant que rapporteurs fictifs.

**Pour plus d'informations:**

Profil du rapporteur Jan Philipp Albrecht (Verts/ALE, DE) – règlement

http://www.europarl.europa.eu/meps/fr/96736/JAN+PHILIPP_ALBRECHT_home.html

Profil du rapporteur Marju Lauristin (S&D, ET) – directive

http://www.europarl.europa.eu/meps/fr/124698/MARJU_LAURISTIN_home.html

Profil du rapporteur pour avis Seán Kelly (PPE, IE) – commission de l'industrie

http://www.europarl.europa.eu/meps/fr/96668/SEAN_KELLY_home.html

Profil du rapporteur pour avis Lara Comi (PPE, IT) – commission du marché intérieur

http://www.europarl.europa.eu/meps/fr/96775/LARA_COMI_home.html

## Prochaines étapes

Le vote en plénière du 14 avril a marqué la fin de la procédure législative du règlement et de la directive sur la protection des données.

Le règlement est entré en vigueur le 24 mai 2016, soit 20 jours après sa publication au Journal officiel de l'UE le 4 mai 2016. Ses dispositions sont directement applicables dans tous les États membres.

Les pays de l'UE ont deux ans pour transposer les dispositions de la directive dans leur législation nationale.

En raison du statut spécial du Royaume-Uni et de l'Irlande pour les législations liées à la justice et aux affaires intérieures, les dispositions de la directive s'appliqueront dans ces pays de façon limitée, c'est-à-dire uniquement dans les domaines pour lesquels ces deux pays ont exprimé une option positive à d'autres législations en matière de coopération policière et judiciaire. En dehors de ces domaines, le Royaume-Uni et l'Irlande ne sont pas tenus par la directive.

Le Danemark peut décider dans un délai de six mois après l'adoption finale de la directive s'il souhaite la mettre en œuvre dans sa législation nationale.