ISSN 1977-9135

LE CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES

Newsletter du CEPD

N° 42 | Juillet 2014

DANS CE NUMÉRO

FAITS MARQUANTS

Protection de la vie privée: procédures de gel des avoirs au Conseil

Le gel des avoirs fait partie des mesures pouvant être adoptées dans le cadre d'enquêtes sur des individus suspectés de certains crimes graves, comme des activités terroristes ou des violations des droits de l'homme commises par des personnes liées aux régimes de certains pays tiers. Sur recommandation des États membres, le Conseil européen publie au Journal officiel de l'Union européenne des listes d'individus dont les actifs doivent être gelés, ainsi que les raisons pour lesquelles ils doivent l'être. Les institutions financières sont alors contraintes de bloquer ces comptes sur la base de ces listes.

Le CEPD avait pour mission d'évaluer les implications de ce processus en matière de protection des données et, le 7 mai 2014, nous avons publié notre avis. Conformément à l'approche que nous avons adoptée dans un précédent *avis*, qui portait sur la procédure de gel des avoirs suivie par la Commission européenne, nous avons recommandé au Conseil de limiter la quantité d'informations publiées dans ces listes. Autrement dit, seules les informations réellement nécessaires à l'identification des individus concernés devraient être publiées. Plus précisément, nous avons exprimé nos doutes quant à la nécessité réelle de publier les raisons qui ont conduit à inclure un individu dans ces listes.

Il arrive parfois qu'une personne figure à tort sur ces listes, généralement en raison d'une erreur ou parce que les motifs de son inclusion sur ces listes ne sont plus d'actualité. Cela pose un problème puisque, même si le Conseil retire des listes ceux qui s'y trouvent à tort, le fait qu'ils se soient un jour retrouvés sur ces listes reste mentionné dans les archives publiques du Journal officiel. Pour résoudre ce problème, nous avons recommandé au Conseil non seulement de corriger les listes sans délai et à intervalles réguliers, mais aussi de prendre des mesures supplémentaires pour effacer les noms de ceux qui se sont retrouvés sur ces listes par erreur. Pour ce faire, on peut par exemple expliquer les raisons pour lesquelles ces noms sont effacés dans l'acte modificatif, qui est publié au Journal officiel, ou dans une lettre adressée à la personne concernée. Cette procédure devrait permettre aux personnes concernées de débloquer leurs comptes et de minimiser les atteintes à leur réputation.

Avis du CEPD

Vie privée et compétitivité à l'ère de la collecte de données massives

La collecte et le contrôle d'une très grande quantité de données personnelles constituent une source importante de pouvoir pour les principaux acteurs du marché mondial des services Internet, a déclaré le Contrôleur européen de la protection des données (CEPD) après la publication de notre avis préliminaire sur la *vie privée et* [la] *compétitivité à l'ère de la collecte de données massives: l'interaction entre le droit à la protection des données, le droit de la concurrence et la protection des consommateurs dans l'économie numérique*. Les données personnelles fonctionnent désormais comme une sorte de monnaie d'échange permettant de payer des services en ligne soi-disant gratuits et constituent un bien immatériel de grande valeur pour un nombre croissant d'entreprises actives sur le marché européen. Ceci montre bien la nécessité d'une meilleure concertation entre les différents régulateurs.

L'évolution de la collecte de données massives a révélé des failles dans les règles européennes de la concurrence, de la protection des consommateurs et de la protection des données qui semblent ne pas s'être adaptées à ce développement. Des interactions plus judicieuses entre ces différents domaines de politique publique qui se chevauchent partiellement permettront de soutenir la croissance et l'innovation et d'atténuer d'éventuels dommages pour les consommateurs. Le CEPD se réjouit de faciliter les discussions entre les régulateurs et les experts dans ces domaines.

Peter Hustinx, CEPD

Avis du CEPD

SUPERVISION

Vos courriers électroniques professionnels, vos données personnelles?

Après qu'un ancien membre du personnel de l'UE a déposé une plainte auprès du CEPD concernant l'accès à sa messagerie électronique professionnelle, nous avons eu l'opportunité de définir avec précision ce que recouvre le concept de «données à caractère personnel» dans ce contexte.

Notre évaluation a suivi l'approche adoptée dans le *document du groupe de travail «Article 29»* relatif au concept de «données personnelles». Sur cette base, l'adresse e-mail, le nom du membre du personnel mentionné dans les courriers électroniques et pièces jointes et les informations afférentes sur le trafic des données indiquant le moment où un courrier électronique a été envoyé ou reçu par un membre du personnel sont considérés comme étant des données personnelles de la personne concernée. Toutefois, le contenu des courriers électroniques et des pièces jointes trouvés sur un compte de messagerie électronique ne devrait être considéré comme les données personnelles d'un membre du personnel que si celui-ci en est l'objet direct. Par exemple, ceci pourrait inclure des courriers électroniques relatifs à une évaluation, à des questions liées à un contrat de travail et à des enquêtes ou procédures internes concernant le membre du personnel, ainsi qu'à l'évaluation individuelle du membre du personnel portant sur certaines situations ou certains comportements.

Cependant, le seul fait qu'une personne ait un droit d'accès à des données personnelles ne signifie pas qu'elle a automatiquement le droit de recevoir des copies de l'intégralité des documents ou courriers électroniques. Les mesures à prendre dépendront des circonstances: il sera parfois nécessaire de remettre une copie de certains documents, mais, dans d'autres situations, il sera plus approprié, par exemple, de fournir un accès direct à ces documents dans les locaux de l'institution ou de l'organe de l'UE – ce qui est qualifié par le *règlement* de l'UE sur la protection des données de *«communication sous une forme intelligible»*.

Définir le concept de «données personnelles»

Sur le même sujet, nous avons adopté une décision dans le cadre d'une plainte contre l'Office européen de lutte antifraude (OLAF). Le plaignant prétendait, entre autres choses, que l'OLAF n'avait pas pleinement respecté son droit d'accès.

Dans ses relations avec le plaignant, l'OLAF a appliqué une interprétation restreinte de l'article 2 du *règlement n° 45/2001*. Cependant, le CEPD considère que le concept de données à caractère personnel défini dans l'article 2 du règlement est bien plus large. En effet, conformément à l'article 2, point a), du règlement, les données à caractère personnel concernent «toute information concernant une personne physique identifiée ou identifiable».

Cette définition fait clairement référence à quelque chose de plus large que le simple nom d'un individu. Une fois encore, nous nous sommes appuyés sur l'approche adoptée par le *groupe de travail «Article 29»* pour justifier notre décision. Le groupe de travail «Article 29» établit que les informations «concernant» un individu, au sens de l'article 2, point a), incluent les informations concernant l'identité, les caractéristiques ou le comportement de cet individu; les informations utilisées pour déterminer ou influencer la façon dont cet individu est traité ou évalué; et les données qui, si elles sont utilisées, sont susceptibles d'avoir un impact sur les droits et intérêts de cet individu. À la lumière de cette définition des données personnelles, le CEPD a dès lors demandé que l'OLAF reconsidère la réponse qu'il avait d'abord donnée à la demande d'accès du plaignant.

Principes de protection des données vs. conservation des données

Alors qu'ils menaient une enquête interne auprès d'une autre institution européenne, les enquêteurs de l'Office européen de lutte antifraude (OLAF) ont demandé les enregistrements des conversations téléphoniques professionnelles réalisées depuis le téléphone portable professionnel de l'individu faisant l'objet de l'enquête. Il apparaît que plusieurs années de données étaient disponibles. Cependant, conformément au *règlement* de l'UE sur la protection des données, le stockage de telles données pour une durée supérieure à six mois n'est pas autorisé, à moins que cela soit demandé dans le cadre d'une affaire juridique qui est déjà en cours à la fin de cette période de six mois.

Dans le cadre de cette consultation, nous avons été interrogés sur la possibilité pour l'OLAF de consulter ces enregistrements. La conservation de ces documents étant illégale, nous avons conseillé de ne pas remettre les enregistrements aux enquêteurs et de les détruire, tout comme l'ensemble des enregistrements de communications que l'institution aurait conservés pendant plus de six mois. Nous avons également conseillé à cette institution de mettre en place un système qui garantira à l'avenir le respect de cette période de conservation. L'institution a par la suite mis ces deux recommandations en œuvre.

CONSULTATION

L'UE doit garantir que les droits des individus sont au cœur de son espace de liberté, de sécurité et de justice

Le CEPD a appelé le Conseil européen à placer les droits des individus au cœur de ses politiques de justice et de sécurité pour les années à venir. L'intention du Conseil européen de définir des orientations stratégiques dans le cadre des traités actuels, pour une nouvelle programmation législative et opérationnelle dans l'espace de liberté, de sécurité et de justice, est l'occasion de revitaliser l'approche européenne dans ces domaines et de remédier à la perte de confiance née des révélations sur la surveillance de masse. L'avis du CEPD sur le développement futur de l'espace de liberté, de sécurité et de justice, publié aujourd'hui, souligne la nécessité d'une plus grande intégration de la protection de la vie privée et des données dans les activités de toutes les institutions de l'UE.

> ***L'annulation récente par la Cour de justice européenne de la directive sur la conservation des données pour violation excessive des droits des individus à la protection de leurs données personnelles devrait retentir comme une sonnette d'alarme. Les décideurs politiques européens doivent imposer des limites et des garanties appropriées, de façon plus éclairée et systématique, lors de la mise en place de propositions qui ont un impact significatif sur les droits fondamentaux.»***
>
> Peter Hustinx, CEPD

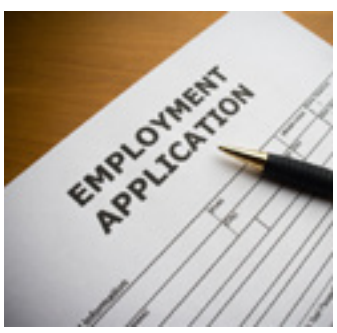
Avis du CEPD

Simplification de la recherche d'emploi (et respect de la vie privée)

Le portail EURES sur la mobilité de l'emploi fournit des informations, des conseils et des services de recrutement aux demandeurs d'emploi à travers toute l'UE. D'une part, les demandeurs d'emploi peuvent télécharger leur CV dans la base de données EURES, chercher un emploi et postuler; d'autre part, les employeurs peuvent rechercher des CV qui correspondent aux postes à pourvoir. Le portail EURES subit actuellement des changements qui augmenteront sa capacité à mettre en relation, de façon automatique, les postes à pourvoir et les demandes d'emploi. Si cette amélioration est positive pour les demandeurs d'emploi, elle comporte néanmoins un plus grand risque pour la protection de la vie privée. C'est pourquoi la Commission européenne a proposé un nouveau règlement visant à mettre à jour le cadre légal du portail et à mieux protéger les données des demandeurs d'emploi.

Dans notre avis du 3 avril 2014, nous nous sommes félicités que la proposition de la Commission nécessite le consentement explicite des travailleurs concernés et tienne dûment compte de leur droit d'accès et de modification de leurs données. Cependant, nous pensons également que la proposition devrait spécifier plus clairement qui peut avoir accès à la base de données, quelles mesures de protection ont été prises pour éviter les abus du système et de quelle manière fonctionne la mise en correspondance automatisée. Nous avons également suggéré que le règlement prévoie que les personnes faisant des recherches sur le portail EURES ne disposent pas d'un accès direct aux noms, aux CV ni à aucune autre donnée à caractère personnel directement identifiable des candidats, à moins que celui-ci ne choisisse de rendre l'intégralité de son CV disponible sur EURES. Nous avons recommandé que la finalité de tout traitement et la liste des utilisations acceptables des données stockées sur EURES soient clairement spécifiées.

Avis du CEPD



Une stratégie pour protéger les secrets d'affaires

Dans ses efforts pour encourager la croissance économique, créer un marché du travail compétitif et fournir des produits et services de haute qualité au sein de l'UE, la Commission européenne a lancé en 2011 sa stratégie de marché unique des droits de propriété intellectuelle. Dans ce contexte, la Commission a adopté à la fin de l'année 2013 une proposition de directive sur la protection des secrets d'affaires contre l'obtention, l'utilisation et la divulgation illicites, pour laquelle le CEPD a été consulté.

Dans cette proposition, le concept de secrets d'affaires ou d'«informations commerciales» est décrit comme quelque chose qui va «au-delà des connaissances technologiques, [et qui comprend] par exemple les informations relatives aux clients et aux fournisseurs», ce qui inclut des données personnelles.

La proposition de la Commission se concentre sur les droits de la personne qui détient ce secret d'affaires. Elle vise à établir un niveau suffisant et comparable de recours sur le marché intérieur, afin de contrer la mauvaise utilisation qui est faite des informations commerciales secrètes, tout en fournissant des protections suffisantes contre les abus. Ce faisant, la proposition entend attirer et retenir les investisseurs et accroître la confiance en la compétitivité des entreprises européennes. Pour respecter cette directive, les États membres doivent mettre en place certaines mesures visant à protéger les informations secrètes qui sont détenues légalement par des personnes physiques ou morales.

Dans notre avis du 12 mars 2014, nous nous sommes concentrés sur les obligations d'un détenteur de secret d'affaires qui est responsable du traitement d'informations personnelles (contrôleur de données) envers des individus dont il détient les données (personnes concernées), dont il est responsable. Entre autres choses, nous recommandons que:

- soit définie la relation entre les données personnelles et le concept du secret d'affaires;
- soient clairement distingués les secrets d'affaires et les secrets commerciaux;
- soit ultérieurement clarifiée l'application d'une autre législation de l'UE; et que
- les droits des citoyen de l'Union, en particulier leur droit d'accès aux données traitées, ne puissent en aucun cas être enfreints par la proposition de directive.

Avis du CEPD

Recherche d'un équilibre entre respect de la vie privée et sécurité internationale

Le programme de surveillance du financement du terrorisme (TFTP) conclu entre l'UE et les États-Unis est utilisé pour collecter des renseignements et prévenir des attaques terroristes par le biais d'un partage d'informations sur les transactions financières entre l'UE et les États-Unis. *L'article 11 du TFTP conclu entre l'UE et les États-Unis* engage la Commission européenne à réaliser une étude sur la possible introduction au sein de l'UE d'un système équivalent au TFTP, le SSFT (système européen de surveillance du financement du terrorisme), qui permettrait un transfert de données plus ciblé de l'UE vers les États-Unis. Avec ce système, l'UE disposerait d'un contrôle accru sur les données de ses citoyens, par rapport à l'accord actuel, considéré par beaucoup comme dangereux pour les données des citoyens de l'Union.

L'étude d'impact menée par la Commission sur la création du SSFT (un cadre légal et technique pour l'extraction de données sur le territoire de l'UE) contient une analyse basée sur les principes de nécessité, de proportionnalité, de rentabilité et de protection des droits fondamentaux. En tenant compte de tout cela, la Commission a conclu que «peu d'arguments plaident, à ce stade, en faveur de la présentation d'une proposition portant création d'un SSFT de l'UE».

Dans nos observations formelles du 17 avril 2014, nous avons salué cette conclusion et le raisonnement qui la sous-tend. Cependant, nous avons attiré l'attention sur le fait que la Commission aurait dû utiliser la même analyse que lorsqu'elle a évalué la nécessité de poursuivre, de modifier ou de mettre fin à l'accord TFTP conclu entre l'UE et les États-Unis. En outre, nous avons souligné la nécessité d'une analyse complète. Cela est d'autant plus important à la suite des révélations de l'an dernier en matière de surveillance, qui ont poussé de nombreuses personnes à remettre en question, une fois encore, la fiabilité et la sécurité de l'accord TFTP, et à la lumière des récentes décisions de la Cour de justice de l'Union européenne portant sur la conservation des données (affaires jointes C-293/12 et C-594/12 concernant *Digital Rights Ireland*) qui a invalidé la directive 2006/24/CE.

Pour ce qui est de l'étude d'impact, nous déplorons que cette analyse n'ait pas cherché davantage à proposer d'autres choix que le SSFT pour l'UE. Elle n'a pris en considération ni les conclusions des rapports de l'*autorité de contrôle commune (ACC)* d'Europol sur ses inspections concernant la mise en œuvre de l'accord, ni l'analyse du *groupe de travail «Article 29»* sur la nature massive des transferts de données financières de l'UE vers les États-Unis et sur les limites des réparations judiciaires et administratives efficaces. Il est essentiel de traiter ces questions si l'UE souhaite développer une meilleure approche.

Observations du CEPD

Le CEPD exhorte l'ICANN à limiter la collecte et la conservation des données personnelles

L'Internet Corporation for Assigned Names and Numbers (*ICANN*) a lancé une consultation publique sur la collecte et la conservation des données dans le contexte de son contrat d'opérateur de registre de 2013. Ce contrat est destiné à encourager la prise de responsabilités et la transparence dans l'industrie des noms de domaine et constitue un accord signé entre l'ICANN et ses agents, qui sont propriétaires des noms de domaine.

Dans notre réponse du 17 avril 2014, nous avons encouragé l'ICANN à prendre les devants pour garantir que, dès leur conception, les nouveaux outils, instruments ou politiques Internet intègrent par défaut la vie privée et la protection des données (privacy by design) pour le bien de tous les utilisateurs d'Internet, pas seulement des Européens. Nous avons conseillé à l'ICANN d'inclure par défaut dans le contrat d'agent l'obligation de ne collecter que les données personnelles qui sont véritablement nécessaires à l'exécution du contrat entre l'agent et le déclarant – comme pour la facturation – ou à toute autre finalité compatible, comme la lutte contre la fraude liée à l'enregistrement d'un nom de domaine. De plus, ces données ne devraient pas être conservées plus longtemps que nécessaire, ni à ces fins, ni à d'autres, comme l'application de la loi ou du droit d'auteur.

Observations du CEPD

Nouvelle orientation pour les services d'informations sur la circulation

Entre décembre 2013 et mars 2014, la Commission européenne a mené une consultation publique sur la mise à disposition, dans l'ensemble de l'Union, de services d'informations en temps réel sur la circulation. Ces services fournissent aux usagers de la route des informations utiles et opportunes sur des sujets tels que le code de la route, les itinéraires, les temps de trajet estimés et les retards potentiels au cours d'un trajet. La consultation publique visait à rassembler les avis des parties prenantes pour tenter de répertorier les problèmes liés aux services actuels, d'identifier les opportunités d'amélioration et de préparer les spécifications et normes relatives à la future fourniture de ces services.

Dans nos observations officielles du 12 mars 2014, nous avons souligné que la collecte et l'utilisation d'informations routières en temps réel peuvent impliquer le traitement de données à caractère personnel. Cette remarque est particulièrement pertinente en cas d'interaction avec des équipements comme la plateforme eCall ou les GPS qui collectent des informations relatives aux utilisateurs. Nous avons donc recommandé à la Commission de prendre pleinement en considération la législation européenne sur la protection des données lors de la mise en œuvre des spécifications ou lois futures dans ce domaine, en particulier les directives 95/46/CE et 2002/58/CE. Pour ce faire, la Commission doit garantir l'intégration du concept de protection de la vie privée dans les infrastructures informatiques et les logiciels dès leur conception (respect de la vie privée dès la conception). Des mécanismes de protection appropriés régissant la collecte et la réutilisation des données de localisation doivent également être mis en place, et nous avons rappelé à la Commission que le CEPD devait être consulté avant l'adoption de toute nouvelle spécification dans ce domaine.

Observations du CEPD

Un modèle moderne de gouvernance de l'internet se doit d'être universel et respectueux des libertés fondamentales

Les efforts mis en œuvre par l'UE pour mettre en place un modèle intégré de gouvernance de l'internet et de protection des données devraient être complétés par une réforme effective du cadre légal de l'UE et par une adoption rapide du Règlement Général sur la Protection des Données, a affirmé le CEPD à la suite de la publication de son Avis sur la Communication de la Commission intitulée Politique et Gouvernance de l'internet – le rôle de l'Europe à l'avenir.

Avis du CEPD

Communiqué de presse du CEPD

Les 10 ans du CEPD: notre rôle et les institutions de l'UE

Le CEPD a rédigé un nouveau document politique expliquant de quelle manière nous conseillons les institutions de l'Union européenne en matière de politique et de législation. Ce document tient spécifiquement compte des changements majeurs intervenus depuis 2004, année de création de notre institution, dans le contexte juridique, économique et technologique, en particulier l'entrée en vigueur du traité de Lisbonne, ainsi que le nombre de décisions importantes rendues par la Cour de justice de l'Union européenne qui ont souligné l'importance capitale de la protection de la vie privée et des données dans le processus de prise de décisions de l'UE.

Conformément à l'article 28, paragraphe 2, du règlement sur la protection des données, la Commission a l'obligation de consulter le CEPD lorsqu'elle adopte une proposition législative qui concerne la protection des libertés et droits individuels lors du traitement de données à caractère personnel. La portée de cette obligation est large puisque, conformément aux pratiques établies, le CEPD est également consulté *de manière informelle* avant que la Commission adopte ces propositions.

Afin de maximiser l'impact et l'utilité de notre travail, nous développons une «boîte à outils politique» qui inclut des conseils généraux pour le législateur, par exemple, par le biais de lignes directrices thématiques ou sectorielles. Cet instrument devrait aider les institutions à prendre des décisions éclairées sur les conséquences que peuvent avoir les nouvelles propositions sur la protection des données.

Document politique

AFFAIRES JUDICIAIRES

Google condamné à respecter le «droit à l'oubli»

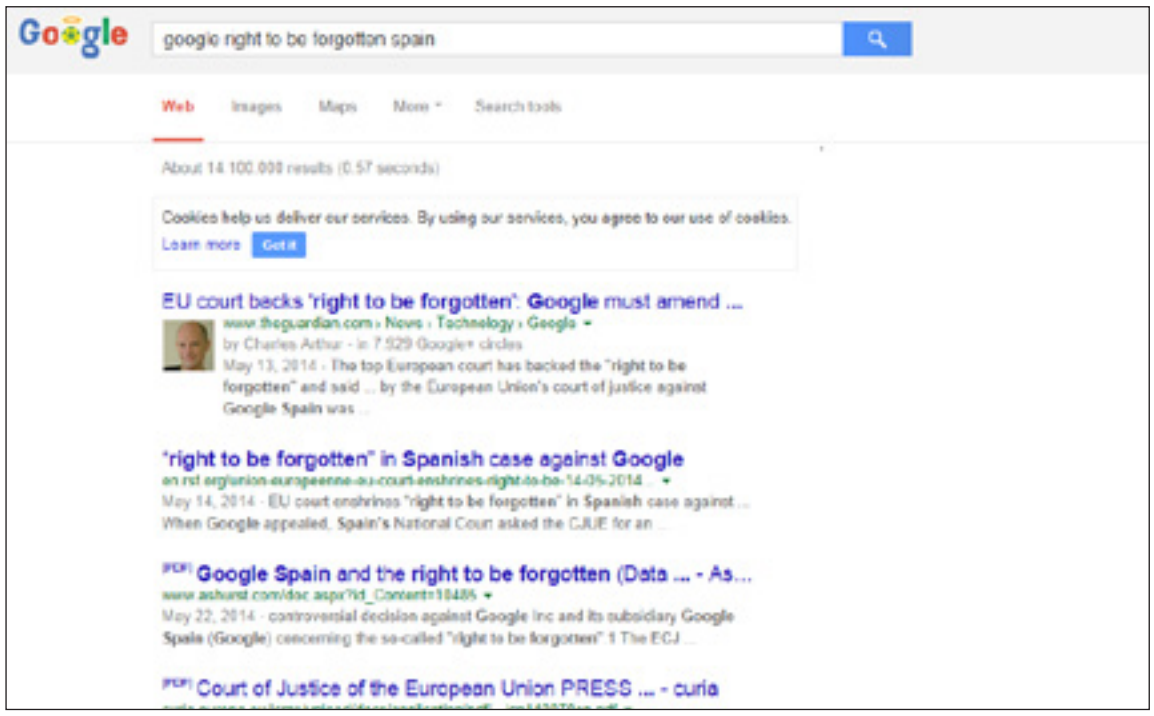
Le 13 mai 2014, la Cour de justice de l'Union européenne a une nouvelle fois rendu un jugement très important. Cette affaire impliquait l'interprétation de plusieurs dispositions clés de la directive 95/46/CE sur la protection des données dans le cadre de l'affaire impliquant un particulier, M. Costeja Gonzalez, qui a demandé que ses données personnelles soient retirées d'une liste de résultats publiées par le moteur de recherche Google.

Premièrement, la Cour a précisé que l'activité d'un moteur de recherche en ligne consiste effectivement en un «traitement de données à caractère personnel» et que l'opérateur de ce moteur de recherche est un responsable du traitement. Deuxièmement, la Cour s'est prononcée sur l'applicabilité de la directive relative à la protection des données aux entreprises basées dans des pays tiers (par exemple, les États-Unis) et opérant dans l'UE par le biais d'une succursale ou d'une filiale. Dans cette affaire, la directive a été considérée applicable puisque les activités de Google Inc. (le moteur de recherche) et de Google Spain (responsable de la promotion et de la vente d'espaces publicitaires) étaient «inextricablement liées». Enfin, concernant le prétendu droit à l'oubli, la Cour a jugé que les personnes concernées sont en droit de demander la suppression de leurs données (sur la base du droit d'effacement et du droit d'opposition, qui sont tous deux prévus par la directive), non seulement si leurs informations personnelles sont inexactes, mais aussi dans tous les cas où le traitement des données ne respecte pas les dispositions de la directive. Ces demandes peuvent être adressées directement au moteur de recherche.

Les autorités européennes de protection des données réunies au sein du groupe de travail «Article 29» vont désormais analyser la décision de la Cour et fournir des lignes directrices afin de développer une approche commune concernant la mise en œuvre de la décision au sein de l'UE.

Jugement

Communiqué de presse du groupe de travail «Article 29»



La Cour de justice déclare l'invalidité de la directive européenne relative à la conservation des données

Le 8 avril 2014, la Cour de justice de l'Union européenne a rendu son jugement dans les affaires jointes C-293/12 et C-594/12, concernant *Digital Rights Ireland* et *Seitlinger and Others*. Dans une décision importante (pour laquelle la Cour a invité le CEPD à contribuer à l'audience), la Cour a déclaré l'invalidité de la directive 2006/24/CE relative à la conservation des données.

Cette décision met en évidence la valeur concédée à la protection de ce droit fondamental qui se trouve au cœur même de la politique de l'UE. En effet, c'est la première fois qu'une directive est invalidée dans son intégralité au seul motif de son incompatibilité avec la charte des droits fondamentaux de l'Union européenne. Des limites claires sont également imposées à la surveillance gouvernementale globale des données de communication (ou «métadonnées»). En particulier, la Cour a précisé que la conservation des données constitue une incompatibilité sérieuse et injustifiée avec le droit fondamental à la vie privée consacré par l'article 7 de la Charte des droits fondamentaux de l'Union européenne. Lorsqu'une loi de l'UE impose des obligations qui interfèrent avec ce droit, le législateur de l'Union doit fournir les garanties nécessaires et ne pas laisser cette responsabilité entre les seules mains des États membres.

Ce jugement implique également que l'UE doit adopter une position ferme dans les discussions avec les pays tiers, en particulier les États-Unis, concernant l'accessibilité et l'utilisation des données de communication des résidents de l'UE.

Jugement

Atteinte à la protection de la vie privée sur Internet

En avril dernier, Heartbleed, une sérieuse vulnérabilité logicielle (CVE-2014-0160) a été découverte dans l'OpenSSL, un instrument de cryptographie populaire utilisé pour garantir la sécurité et la confidentialité des communications Internet. Dans les versions vulnérables d'OpenSSL, Heartbleed permet de lire et d'accéder à des données supposées protégées. Des applications Internet, comme le courrier électronique, la messagerie instantanée, les activités sur le web et les réseaux privés virtuels (VPN) sont ainsi exposées à l'exploitation et éventuellement au vol de données à caractère personnel.

La vulnérabilité est incluse dans différentes versions d'OpenSSL depuis 2012. Les fonctions vulnérables faisaient également partie de nombreux paquets de logiciels populaires, y compris certains jeux commerciaux et logiciels de bureau.

Étant donné son impact étendu et sérieux, l'ensemble des responsables de la sécurité ont réagi rapidement à ce problème. Des services en ligne tels que Wikipedia, Yahoo et Amazon se sont tous révélés vulnérables et ont pris les mesures nécessaires pour résoudre rapidement ce problème informatique au sein de leurs systèmes. Les institutions européennes ont également pris des dispositions pour protéger leurs services. Les utilisateurs des services affectés ont été invités à changer leurs mots de passe. De plus, les certificats utilisés pour le cryptage du trafic Internet entre les différents sites affectés ont été remplacés. En réaction à cet incident, la *Linux Foundation* a créé une nouvelle initiative visant à améliorer la qualité des contrôles de sécurité pour les logiciels open source largement utilisés. Pourtant, en dépit de toutes ces mesures, il est possible que certains serveurs n'aient toujours pas été mis à jour et utilisent encore les logiciels affectés.

Heartbleed représente une sérieuse menace pour la confidentialité des données personnelles et démontre combien il est important de garantir la sécurisation des ordinateurs et systèmes Internet utilisés dans le traitement des données à caractère personnel.

L'initiative de l'IPEN pour la protection de la vie privée

Les révélations d'Edward Snowden sur la surveillance massive de l'Internet ont déclenché un débat parmi les ingénieurs du web, qui considèrent qu'il est de leur responsabilité de *protéger les données personnelles et la vie privée* des utilisateurs d'Internet. En réaction, plusieurs projets remarquables ont été lancés, dans le but d'améliorer la sécurité et la protection de la vie privée des utilisateurs d'Internet. L'Internet Privacy Engineering Network (IPEN), lancé par le CEPD en collaboration avec des autorités nationales de protection des données, des universitaires et des ingénieurs, en est un exemple. Il est conçu comme une plateforme pour la coopération et l'échange d'idées entre les autorités de protection des données et les ingénieurs du web.

L'IPEN entend combler les écarts existant entre les outils techniques (conçus par des ingénieurs et des experts informatiques) et les besoins en matière de protection des données personnelles (régis par la loi) en encourageant le développement de solutions respectueuses de la vie privée aux problèmes d'ingénierie communs et en permettant aux développeurs de reconnaître l'impact potentiel de leurs choix techniques sur les principes de protection de la vie privée.

L'IPEN a pour objectif de constituer un réseau d'experts en protection de la vie privée issus des communautés techniques, politiques et de développeurs. Ce réseau partagera trois missions principales:

- Partager l'information sur les initiatives en cours et les projets traitant des besoins de développement liés à la protection de la vie privée.
- Identifier les *«cas d'utilisation»* – lorsque des techniciens informatiques identifient des procédures qui leur permettront de résoudre un problème spécifique – dans lesquelles le concept de protection de la vie privée peut être intégré dès la conception; et,
- Lancer des projets de développement d'outils et de d'éléments permettant d'assurer et d'améliorer la protection de la vie privée.

De plus, l'IPEN mettra en place une banque de ressources pertinentes, afin de mettre ses conclusions et sa base de connaissances à la disposition de tous les participants, développeurs et experts en protection de la vie privée.

Jusqu'ici, l'IPEN a été présenté lors de plusieurs événements et a obtenu le soutien de «pirates», de développeurs open source, d'ingénieurs du web, de chercheurs universitaires et de développeurs, ainsi que d'experts d'autorités nationales de protection des données.

Pour plus d'informations ou pour participer à l'initiative de l'IPEN, contactez-nous à l'adresse suivante : *ipen@edps.europa.eu*

ÉVÉNEMENTS

Vie privée, consommateurs, concurrence et données massives

Le 2 juin 2014, le CEPD a organisé un atelier dont l'objectif était de discuter des liens entre l'approche de l'UE en matière de concurrence, de protection des consommateurs et de protection des données et le contexte très changeant de l'économie digitale.

Des experts universitaires, des groupes de réflexion et des cabinets juridiques issus des deux côtés de l'Atlantique ont été rejoints par des décideurs politiques nationaux et des régulateurs de l'UE pour se pencher sur plusieurs thèmes examinés par le CEPD dans notre *avis préliminaire* publié le 26 mars 2014, notamment l'évaluation du pouvoir et de la prédominance du marché, l'intérêt du bien-être du consommateur et la possibilité d'abus et d'exploitation dans des secteurs qui commercialisent les données à caractère personnel en échange de services «gratuits», souvent sans informer pleinement le consommateur. Les principales interventions de deux commissaires de la FTC, l'un ancien et l'autre actuellement en poste, ont ajouté une perspective américaine à des questions qui sont de plus en plus répandues en conséquence de la nature globale et sans frontière de l'«écosystème du *big data*».

Les discussions confirment qu'en dépit de jargons distincts, les différents domaines politiques ont plus en commun qu'il n'y paraît à première vue. Le CEPD a pu relancer la discussion entre les faiseurs d'opinions issus de disciplines variées. Un consensus s'est clairement dégagé sur la nécessité de poursuivre l'identification des lacunes et synergies et de commencer à identifier les actions nécessaires et le responsable de la mise en œuvre.

C'est une séance à huis clos régie par la règle de Chatham House qui a permis le déroulement de discussions franches et honnêtes.

Un rapport plus complet de l'événement sera publié dans les prochaines semaines.

DÉLÉGUÉS À LA PROTECTION DES DONNÉES

Le prochain numéro de la newsletter du CEPD sortira à l'automne. Nous vous souhaitons un été agréable!

DISCOURS ET PUBLICATIONS

- Points de discussion (*PDF*) remis par Giovanni Buttarelli à l'INET 2014, «Internet: Privacy and Digital Content in a Global Context», Istanbul (21 mai 2014).
- «Rétablir la confiance de part et d'autre de l'Atlantique», article (*PDF*) de Peter Hustinx publié dans «TELOS, Revista de Pensamiento sobre Comunicación, Tecnologia y Sociedad» (2 mai 2014).

À propos de cette newsletter

Cette newsletter est publiée par le Contrôleur européen de la protection des données, une autorité européenne indépendante créée en 2004 en vue de :

- superviser le traitement des données à caractère personnel dans les institutions et organes de l'UE ;
- conseiller les institutions européennes sur la législation en matière de protection des données ;
- coopérer avec les autorités similaires afin de promouvoir la cohérence de la protection des données à caractère personnel.

Vous pouvez vous abonner à cette newsletter ou vous en désabonner sur notre site Internet.

COORDONNÉES

www.edps.europa.eu
Tél. : +32 (0)2 283 19 00
Fax : +32 (0)2 283 19 50
NewsletterEDPS@edps.europa.eu

ADRESSE POSTALE

CEPD
Rue Wiertz 60 – Bât. MTS
B-1047 Bruxelles
BELGIQUE

ADRESSE BUREAUX

Rue Montoyer 30
B-1000 Bruxelles
BELGIQUE

Suivez-nous sur Twitter : @EU_EDPS

CEPD – Le Contrôleur européen de la protection des données

QT-AC-14-002-FR-C doi:10.2804/62185 ISBN 978-92-9242-049-9