Service communication et presse
450 route des Chappes – CS 50193
06904 Biot Sophia Antipolis cedex
Tel : +33 (0)4 93 00 81 21
Laurence.Grammare@eurecom.fr

Sophia Antipolis le 19/03/13

INFORMATION PRESSE

La protection des données personnelles en Europe
Plus de 90 personnalités du monde académique prennent position

EURECOM signataire du document de soutien pour la législation en faveur de la protection des données personnelles aux côtés d'Inria, du Cnrs, de l'Institut de l'Ouest et de l'Université de Versailles.

Le traitement automatique de données personnelles se développe à un rythme invraisemblable et devient une partie intégrante des activités économiques, administratives et sociales en Europe et dans le monde entier. Sur le Web en particulier, les internautes se sont habitués à utiliser des services apparemment gratuits, en fournissant en contrepartie certaines données personnelles à des fins de marketing. Dans ce contexte, une refonte de la réglementation protégeant les données personnelles est actuellement en discussion en Europe. Il y a un an, la Commission Européenne a présenté un projet de nouveau Règlement Européen sur la Protection des Données. Le Parlement Européen et le Conseil de l'Europe sont en train de définir leur position sur ce nouveau règlement. Pendant ce temps, d'importants groupes de pression tentent d'influencer massivement les instances réglementaires.

EURECOM mène, depuis sa création, une activité de recherche importante dans le domaine de la protection des données et de la vie privée qui l'implique naturellement dans la discussion sur cette réglementation. Refik Molva, professeur et chef du département de recherche Réseaux et Sécurité d'EURECOM est parmi les signataires français de la lettre de soutien à la nouvelle réglementation.

Pour contribuer à la formation d'une opinion plus objective dans ce débat passionné, nous voudrions apporter quelques arguments professionnels.
Nous voulons aussi répondre à certains arguments visant à affaiblir la protection des données en Europe.

L'innovation et la concurrence ne sont pas menacées

Le principal argument contre le règlement qui est proposé pour protéger les données personnelles est que ce règlement aura un impact négatif sur l'innovation et la concurrence. Les critiques prétendent que les règles suggérées pour protéger les données sont trop strictes et vont ralentir l'innovation à un point qui désavantage les acteurs européens dans le marché global actuel. Nous ne partageons pas cette opinion. Au contraire, nous avons pu constater qu'un contexte réglementaire

peut favoriser l'innovation. Ce fut le cas, par exemple, des réglementations sur la sécurité routière, sur la protection de l'environnement et sur l'énergie. Pour ce qui est de la protection des données, on a vu la création à travers toute l'Europe d'entreprises innovantes qui proposent des solutions clés en main permettant aux citoyens européens de protéger leurs données personnelles. Des experts en sécurité et en protection de la vie privée vendent du conseil aux entreprises pour les aider à sécuriser leurs systèmes d'information. Pour de nombreux secteurs professionnels, ce n'est pas la réglementation sur les données personnelles qui empêche les entreprises d'adopter des services d'informatique "en nuage", mais plutôt l'inquiétude sur la protection des données elle-même.

Un récent rapport du Boston Consulting Group sur la "valeur de l'identité numérique" soutient que le nouveau règlement sur la protection des données proposé par la Commission Européenne ne freinera pas l'économie des données personnelles. Cinq des six domaines d'utilisation des données personnelles identifiés par BCG sont compatibles avec le règlement proposé. Ce bureau de conseil voit en particulier les données personnelles comme un levier pour automatiser, personnaliser et améliorer les produits et services. De notre point de vue, les entreprises peuvent utiliser les données personnelles à ces fins si elles maintiennent des relations personnelles avec leurs clients. Depuis longtemps, on voit que les gens acceptent de fournir leurs données personnelles en échange de services de qualité. Des offres personnalisées et une amélioration continue des services sont possibles dans le contexte de relations équitables entre les entreprises et leurs clients. De plus, une meilleure confiance dans la façon d'utiliser les données renforcera ces relations.

Les pratiques commerciales actuelles ne subiront de contraintes que si les entreprises créent de la valeur uniquement sur l'agrégation et le commerce des données personnelles plutôt que d'investir dans les relations directes avec les clients finaux. Par exemple, les grands réseaux de ciblage de publicité et de profilage d'utilisateurs devront limiter davantage leur utilisation des données personnelles si le règlement est adopté dans sa forme actuelle. Mais c'est justement dans ce domaine que nous constatons un besoin d'adapter la réglementation et d'introduire des sanctions.

De plus, l'innovation n'est pas menacée par le nouveau règlement sur la protection des données personnelles, puisque de nombreux services n'ont pas besoin de données directement reliées à des personnes. Dans de nombreux cas, l'exploitation de données personnelles peut être évitée par l'utilisation de techniques d'anonymisation. Lorsqu'un service a réellement besoin de données personnelles, ces données peuvent être collectées sur une base contractuelle. Des services peuvent aussi obtenir un accès à des données en requérant des citoyens — en toute équité — leur consentement explicite.

Sur « le consentement explicite »

Depuis 1995, l'utilisation des données personnelles en Europe repose sur le principe du consentement explicite. Ce principe est la clé de l'autodétermination des citoyens en matière de données personnelles. Cependant, on ne peut pas dire qu'il ait été bien mis en pratique jusqu'à présent.
D'une part, les utilisateurs se plaignent que les déclarations de respect de la vie privée et les termes d'utilisation et conditions générales sont difficiles à lire et ne laissent pas de véritable choix aux utilisateurs : si on veut utiliser un service, il faut confirmer plus ou moins aveuglément. D'autre part, les entreprises considèrent la rédaction des termes juridiques de protection des données comme un exercice d'équilibriste et une opération coûteuse. Dans le même temps, les utilisateurs se sentent démunis et sont rebutés par la petite taille des caractères utilisés.

En conséquence, de nombreux représentants de l'industrie suggèrent d'inverser le principe du consentement explicite et d'adopter un principe d'acceptation implicite sauf refus exprès (« opt-out »), comme c'est le cas actuellement aux États-Unis. Aux États-Unis, la plupart des traitements de données personnelles sont autorisés par défaut, tant que l'utilisateur ne les refuse pas expressément.

Le projet de règlement, au contraire, renforce l'autodétermination des citoyens sur leurs données. Le consentement explicite est préservé. De plus, lorsqu'il y a un déséquilibre significatif entre la

position de la personne concernée et celle du responsable du traitement, le consentement ne constitue pas un fondement juridique valable pour le traitement.

Nous soutenons la proposition de règlement sur la protection des données parce que nous croyons qu'un consentement explicite est indispensable. D'abord, une inversion du principe de consentement explicite pour un principe d'autorisation par défaut affaiblit considérablement la position des citoyens. Une telle inversion laisse moins de contrôle aux individus et donc réduit leur confiance dans l'Internet. Ensuite, nous voyons apparaître des solutions qui permettent de résoudre les problèmes actuels des utilisateurs. Des entreprises européennes fournissent des outils techniques qui aideront les utilisateurs à gérer leurs décisions pour protéger leur vie privée de façon automatique ou avec très peu d'efforts. Aux États-Unis, le W3C a lancé l'initiative "do-not-track" (ne-tracez-pas), qui prévoit une mise en œuvre renforcée des préférences de l'utilisateur dans les navigateurs. De plus, des technologies sont actuellement développées pour interpréter les termes de respect de la vie privée et les résumer de façon à faciliter la prise de décision.

Les utilisateurs ne pourront faire de vrais choix que si le couplage de l'utilisation de données personnelles avec des services sans rapport avec celles-ci demeure illégal.

Sur "l'intérêt légitime"

Actuellement, des entreprises peuvent traiter des données personnelles sans le consentement de l'utilisateur si elles peuvent affirmer qu'elles ont un intérêt légitime à utiliser ces données. Malheureusement, jusqu'à présent, le terme "intérêt légitime" laisse beaucoup trop de place à interprétation. Quand l'intérêt est-il légitime et quand ne l'est-il pas ?

Afin d'empêcher les abus éventuels de cette règle, dont le principe est raisonnable, le nouveau règlement sur la protection des données définit et contrebalance les intérêts légitimes des entreprises et des clients. Le règlement exige que les entreprises non seulement déclarent un intérêt légitime, mais aussi qu'elles le justifient. Le rapporteur au Parlement Européen a également insisté sur les intérêts légitimes des citoyens. Il a défini quand les intérêts des citoyens prévalent sur ceux des entreprises et vice-versa. Dans les amendements émis par le rapporteur, les citoyens ont un intérêt légitime à ce qu'il ne soit pas créé de profil sur eux sans qu'ils le sachent et que leurs données ne soient pas partagées avec une myriade de tiers dont ils ne savent rien. Nous trouvons que cet équilibrage entre les intérêts des uns et des autres est une proposition très équitable qui permet d'allier les meilleures pratiques industrielles avec les intérêts des citoyens.

Quand appliquer le règlement ? Quand des données sont-elles "personnelles" ?

Un point important de désaccord porte sur les activités de traitement de données qui devraient effectivement être couvertes par le règlement. Les internautes sont souvent identifiés implicitement : en fait, les utilisateurs sont identifiés par les adresses réseau de leurs connexions (adresses IP) ou par des "cookies" qui sont insérés dans leurs navigateurs. Les identifiants implicites peuvent être utilisés pour créer des profils. Certains de ces identifiants implicites changent constamment, ce qui explique qu'à première vue ils ne semblent pas poser de problème pour le respect de la vie privée. Pour certains, il peut sembler impossible de ré-identifier des individus à partir de tels identifiants dynamiques. Cependant, de nombreuses expériences ont montré qu'une telle ré-identification peut être réalisée.

Malgré la capacité indiscutable de construire des profils et de ré-identifier des données, certains représentants de l'industrie maintiennent que les données liées à des identifiants implicites ne doivent pas être couvertes par le règlement. Ils prétendent que les entreprises sur Internet qui collectent beaucoup de données sur leurs utilisateurs ne sont intéressées que par des données agrégées et statistiques, et que donc elles ne s'engagent pas dans des pratiques de ré-identification.

Pour des raisons techniques, économiques et juridiques, nous ne pouvons accepter cette position. Techniquement, il est facile de relier des données collectées sur une longue période à un individu

unique. Économiquement, il est peut-être vrai que l'identification d'un individu n'est pas actuellement une priorité de l'industrie. Cependant, le potentiel d'une telle ré-identification est très attrayant, et il ne peut donc être exclu qu'elle survienne un jour. Juridiquement, nous devons protéger les données qui peuvent être ré-identifiables d'une façon ou d'une autre, puisque de telles mesures de précaution pourraient devenir le seul remède efficace.

Certains parlementaires européens suggèrent que les données anonymisées, pseudonymisées et chiffrées ne devraient en général pas être couvertes par le règlement sur la protection des données. Selon eux, des telles données ne sont plus "personnelles". Cette méconnaissance est dangereuse. Indiscutablement, l'anonymisation, la pseudonymisation et le chiffrement sont des instruments utiles pour la protection technique des données : le chiffrement aide à maintenir la confidentialité des données ; les pseudonymes réduisent la connaissance qu'on peut avoir sur des individus et leurs données sensibles (par exemple, la relation entre les données médicales d'un patient) à ceux qui en ont réellement besoin. Cependant, bien souvent même ce type de données protégées peut être utilisé pour ré-identifier des individus. Nous pensons donc que ce type de données doit aussi être couvert par le règlement sur la protection des données, même s'il peut être traité d'une manière différente de celle des données personnelles qui sont directement identifiées. De plus, couvrir ce type de données est nécessaire pour s'assurer que la protection des données est traitée de manière adéquate et professionnelle. Il nous faut des règles contraignantes qui soient régulièrement ajustées aux standards techniques (c'est-à-dire aux meilleures pratiques) et qui définissent quand les données sont suffisamment pseudonymisées et quand elles peuvent être considérées comme anonymes.

Qui devrait définir les exigences en matière de protection des données ?

En dehors des nombreux aspects positifs de la proposition de règlement, nous y voyons une faiblesse structurelle, qui pourrait être facilement rectifiée : dans de nombreux articles, la proposition actuelle de la Commission Européenne ne définit que des objectifs vagues. Plus précisément, elle institue la Commission Européenne elle-même comme l'organe qui définirait plus tard les détails par des « actes délégués » et des « actes d'exécution ». Ce plan mettrait la Commission Européenne dans une position de pouvoir qui ne correspond pas aux exigences constitutionnelles européennes. Les règles sur la protection des données peuvent avoir un impact majeur sur les activités économiques, administratives et sociales. Il est donc du devoir des instances législatives européennes de prendre de telles décisions elles-mêmes. Toutes les règles concernées doivent donc être intégrées dans le règlement lui-même. Seuls les détails moins critiques sur le plan politique ou concernant les droits fondamentaux peuvent être laissés à la discrétion de la Commission.

La liste des signataires est disponible à http://dataprotectioneu.eu/

A propos d'EURECOM:

Situé dans la Technopole de Sophia Antipolis, EURECOM est une école d'ingénieurs et un centre de recherche en systèmes de communication fondé en 1991 sous forme d'un GIE qui réunit des partenaires académiques et industriels1. Depuis sa création, EURECOM a une stratégie de développement international très marquée.

Les activités d'enseignement et de recherche d'EURECOM sont organisées autour de trois domaines : réseaux et sécurité, communications mobiles, et contenu multimédia.

EURECOM est particulièrement actif en recherche dans ses domaines d'excellence et forme un grand nombre de doctorants. Sa recherche contractuelle, à laquelle participe activement ses membres industriels, est largement reconnue en Europe et contribue pour une large part à son budget.

Depuis 2006 EURECOM est labélisé « Institut Carnot » conjointement avec l'Institut Mines Télécom dont EURECOM est une école filiale.

---

[1] TELECOM ParisTech, Politecnico di Torino, Helsinki University of Technology, Technische Universität Munchen, Norwegian University of science and technology, Vietnam National University Ho Chi Minh city.

Swisscom, Orange, SFR, ST Microelectronics, BMW Group research & technology, Monaco Telecom, Symantec, SAP, IABG.

Partenaire institutionnel: Principauté de Monaco

En savoir plus:

- Contact réseaux et sécurité : Prof Refik Molva, (personnalité signataire pour EURECOM)
- +33 (0)4 93 00 81 66 , Refik.Molva@eurecom.fr

- Contact presse : Laurence Grammare, responsable communication
  EURECOM – CS 50193
  F-06904 Sophia Antipolis cedex
  Tel: +33 (0)4 93 00 81 21 - +33 (0)6 16 32 40 88
  mailto:Laurence.Grammare@eurecom.fr
  http://www.eurecom.fr