

# GLOBAL INTERNET LIBERTY CAMPAIGN



This interview is also available in [Spanish](#).

## NEWS

[GILC Actions  
Presswire](#)

**"Le droit au respect de la vie privée risque de perdre de sa substance."**

- LE MONDE INTERACTIF | 29.05.02 | 11h34
- MIS A JOUR LE 29.05.02 | 12h24

## ISSUES

[Free Speech](#)  
[Privacy](#)  
[Cryptography](#)  
[Access](#)

**La directive 97/66 sur la protection des données et informations dans le secteur des télécommunications doit être révisée. La discussion au Parlement européen aura lieu le 29 mai, et le vote le 30 mai. Que dit cette directive, dans l'état actuel ?**

## RESOURCES

[GILC Alert](#)  
[Mailing List](#)  
[GILC Events](#)

**Meryem Marzouki, présidente de l'association IRIS (Imaginons un réseau Internet solidaire) :** La révision vise à adapter au secteur des communications électroniques la directive européenne sur la protection des données personnelles dans le secteur des télécommunications, en vigueur depuis 1997 (directive 97/66). Ce texte consacre le principe de suppression ou d'anonymisation "des données relatives au trafic concernant les abonnés et les utilisateurs traitées en vue d'établir des communications et stockées par le fournisseur d'un réseau public de télécommunications et/ou d'un service de télécommunications accessible au public", dès que la communication est terminée.

## ABOUT GILC

[Principles](#)  
[Members](#)  
[Mail GILC](#)

Les seules exceptions autorisées sont encadrées par les principes de finalité, de proportionnalité et de limitation dans le temps en vertu du respect des textes fondamentaux de l'Union européenne. Ces exceptions doivent être énoncées précisément dans les textes législatifs ; c'est le cas notamment pour les besoins de facturation, ou la poursuite d'infractions pénales, dans le cadre de mesures exceptionnelles et encadrées par les autorités judiciaires.

[Home Page](#)

[US Site](#)  
[European Mirror](#)

Comme pour la plupart des mesures sécuritaires adoptées dans certains pays, dont la France par le biais de la loi sur la sécurité quotidienne (LSQ), ce "tour de vis" sévère se réclame aujourd'hui de la lutte contre le terrorisme mise en œuvre depuis le 11 septembre 2001, alors que les pressions en ce sens sont bien antérieures à cette date.

**Cédric Laurant, membre de l'Electronic Privacy Information Centre de Washington (EPIC) :** La directive 97/66 vise à protéger la vie privée dans le cadre de la fourniture de services de télécommunications accessibles au public

sur les réseaux publics de télécommunications, alors que la nouvelle directive s'appliquerait à toute communication électronique accessible au public, élargissant ainsi le champ d'application potentiel de la directive à toute communication électronique sur Internet et sur des réseaux de télécommunication (téléphonie cellulaire, téléphonie classique via le fil de cuivre, courrier électronique et autres formes de communication sur Internet, WAP, etc.). Dans la nouvelle proposition de directive (art. 15(1)), proposée par le Conseil de l'UE et entérinée par la Commission, une ligne a été ajoutée à l'ancien article 14. Il autorise les Etats membres à conserver les données de communication électroniques (de trafic et de localisation) pour une durée limitée lorsque cela est justifié pour sauvegarder la sûreté de l'Etat, la défense, etc., dans le respect des principes généraux du droit communautaire.

La version proposée dans le rapport Cappato – parlementaire qui a rédigé le rapport sur les modifications à apporter à la directive communautaire (2000) 385 dans le cadre de la Commission du Parlement européen responsable des questions justice et affaires intérieures (Commission "LIBE") – propose de mentionner dans le texte de l'article 15(1) une référence aux principes de base de la jurisprudence de la Cour européenne des droits de l'homme concernant la conservation des données (toute mesure dérogatoire doit être exceptionnelle et sanctionnée au cas par cas par les autorités judiciaires) et une référence au droit au respect de la vie privée qui figure dans la Charte des Droits fondamentaux de l'UE et la Convention européenne des droits de l'homme et des libertés fondamentales de 1950. Ce qui ne plaît pas au Conseil et à certains gouvernements des Etats membres qui veulent au contraire se réserver la possibilité de conserver les données de trafic et de localisation au cas où ils auraient à enquêter sur d'éventuelles infractions commises dans le futur par les utilisateurs de services de communications électroniques.

Sa position a jusqu'à présent toujours obtenu un vote de confiance de la part de sa Commission parlementaire ainsi qu'un vote positif en novembre lorsque le Parlement européen a été appelé à voter en séance plénière sur le premier rapport qu'il avait rédigé.

### **En quoi cette révision menace-t-elle la confidentialité des données professionnelles et privées ? Quels sont les Etats qui demandent cette révision ?**

**Meryem Marzouki** : Le principe d'interdiction de toute surveillance systématique des communications, notamment par la rétention des données de communication, est largement battu en brèche. Ce principe est inscrit dans la Directive de 1997. Les représentants des Etats et les autorités policières et judiciaires invoquent la nécessité des enquêtes ; les porte-parole des lobbies industriels mettent en avant la sécurisation de leurs réseaux (opérateurs et fournisseurs d'accès) et la poursuite d'infractions à la propriété intellectuelle (industrie du logiciel, majors de la musique et du cinéma). Nous n'avons pas le détail des discussions entre Etats-membres, mais la décision du Conseil des ministres de l'UE représente la décision commune des représentants des Quinze.

**Cédric Laurant** : Le danger provient de la conservation systématique par les fournisseurs d'accès à l'Internet, les opérateurs de télécommunication, sur la demande des services de police. Si la police peut avoir accès aux communications que vous et moi avons écrites il y a un an, 3 ans, voire même plus longtemps, en fonction des législations des Etats membres et alors que nous n'avons commis aucune infraction, notre liberté d'expression, notre droit au secret de la correspondance et à la confidentialité de nos communications privées sont substantiellement atteintes.

Le droit au respect de la vie privée figurant dans les textes fondamentaux protégeant les droits de l'homme (Convention européenne des droits de l'homme, Charte des droits fondamentaux de l'UE) risque de perdre de sa substance si la manière dont les autorités gouvernementales peuvent avoir accès à nos communications privées consiste à, par avance, demander une conservation systématique des communications afin de pouvoir plus tard y accéder pour une raison ou une autre. Comme la lettre de la Global Internet Liberty Campaign (GLIC) le souligne, permettre une conservation systématique et générale des communications est un danger pour la liberté d'expression, le droit au respect de sa vie privée et le principe fondamental de droit pénal de la présomption d'innocence.

Aux Etats-Unis, même après le passage en octobre 2001 d'une loi anti-terrorisme (USA Patriot Act) très restrictive, aucun texte n'autorise la conservation des communications privées, sauf sur demande, au cas par cas, faite par la police auprès d'un juge spécialement habilité à connaître de demandes d'interception de communication ("wiretapping"). Les Etats les plus prompts à demander la conservation des données, ou qui ont déjà légiféré en la matière pour permettre cette conservation, sont, entre autres, la France, Belgique, la Grande-Bretagne et l'Allemagne.

### **En quoi l'article 15 de la directive pose-t-il problème ?**

**Meryem Marzouki** : Ce qui pose problème est que les gouvernements veulent imposer la possibilité de conservation des données de communication, pendant une durée qui serait définie par les lois nationales, et pour des fins autres que les seules fins de facturation ou de maintenance des systèmes. Cela signifie la possibilité de conservation généralisée des données de communication, à des fins exploratoires (renseignement, par exemple). En pratique, on va pouvoir surveiller qui communique avec qui, et qui consulte quoi sur Internet, sans possibilité d'information ni de recours, comme avec la LSQ en France.

Le rapport Cappato, au contraire, exclut cette possibilité, en référence à la Convention européenne des droits de l'homme, à la charte des droits fondamentaux de l'UE, et à la jurisprudence de la cour européenne des droits de l'homme. Il stipule que de telles mesures de conservation des données doivent être exceptionnelles, et soumises à la demande d'une autorité judiciaire statuant au cas par cas (par exemple dans le cas d'une enquête judiciaire ouverte). Il stipule aussi qu'une telle mesure doit être "appropriée, proportionnée et

temporaire, au sein d'une société démocratique".

**Cédric Laurant** : La position du Conseil de l'UE est de dire que les Etats membres devraient être en mesure de décider pour eux-mêmes s'ils acceptent le principe de la conservation des données dans leur législation nationale. Cependant, le Conseil, de concert avec certains Etats membres, est déjà en train de rédiger une nouvelle proposition de décision-cadre (dans le cadre du troisième pilier de l'UE) qui instaure le principe de la conservation comme s'imposant à tous les Etats membres.

Or, une décision-cadre est prise par le Conseil et les gouvernements des Etats membres sans laisser aux parlements nationaux la possibilité de s'exprimer. Une décision-cadre fixe les conditions dans lesquelles les Etats membres doivent mettre en oeuvre les principes de base de la décision-cadre. Le fait que cette décision soit rédigée alors même que la directive communautaire(2000) 385 n'est pas encore adoptée montre le peu de respect que le Conseil a pour l'opinion et le vote du 30 mai du Parlement européen. Si cette décision-cadre est adoptée, aucun parlement des Etats membres n'aura la possibilité de s'opposer au principe de la conservation. C'est la raison pour laquelle la Global Internet Liberty Campaign (GILC) est d'avis que les membres du Parlement Européen ont une opportunité historique lors du vote du 30 mai pour rejeter le principe de la conservation des communications, sans s'en laisser conter par le Conseil quand il affirme dans ses déclarations officielles que chaque Etat membre pourra, plus tard, avoir la possibilité de se prononcer sur cette question.

### **Les parlementaires européens vont-ils nécessairement suivre la révision proposée par le conseil des ministres de l'Europe ?**

**Meryem Marzouki** : Il y a tout lieu de s'inquiéter depuis que les groupes PPE (droite) et PSE (socialistes) se sont alliés pour déposer un amendement dit de compromis, mais qui en fait va dans le sens de la position du Conseil des ministres. Or PPE+PSE, cela signifie une large majorité des députés européens.

**Cédric Laurant** : Notre organisation, ne pense pas que les parlementaires européens qui comprennent bien les enjeux du principe de la conservation des communications pour nos droits et libertés fondamentales vont voter en faveur de la position du Conseil. Nous pensons qu'ils vont voter à nouveau comme ils l'ont déjà fait en novembre dernier en faveur du rapport Cappato en tant qu'il s'oppose au principe de la conservation des données.

### **Quelle peut-être l'impact des ONG sur le processus législatif ?**

**Meryem Marzouki** : Nous espérons, par cette campagne, et sa médiatisation, peser sur la discussion et le vote des parlementaires européens. La lettre des ONG a reçu le soutien de plus de 12000 citoyens de l'UE.

Notre association a adressé une lettre en ce sens à tous les députés français - à l'exclusion des députés du Front national - élus au Parlement européen dont les

adresses étaient disponibles. La lettre d'IRIS adressée aux députés européens rappelait les circonstances de l'adoption de la LSQ en France, et la plainte déposée par IRIS contre la France auprès de la Commission européenne à ce sujet. Enfin, cette lettre se terminait ainsi : "En approuvant le 29 mai prochain la position de la Commission des libertés et des droits des citoyens sur le premier alinéa de l'Article 15, vous affirmerez aux citoyens européens, et aux citoyens français en particulier, que l'Union et son Parlement peuvent demeurer les garants de la démocratie et des libertés, au-dessus des contingences politiciennes qui prévalent parfois à l'échelle nationale. Les résultats du premier tour des élections françaises le 21 avril 2002 ont montré la nécessité de telles garanties."

**Cédric Laurant** : Des organisations comme EPIC aux Etats-Unis, LSIJolie en France, Quintessenz en Autriche, etc., sont très actives depuis l'année dernière pour alerter le public et la presse au de le sujet de la conservation des données. Diverses actions ont vu le jour depuis le 11 septembre dernier. La dernière action dans laquelle la Global Internet Liberty Campaign ([www.gilc.org](http://www.gilc.org)) s'était illustrée était l'envoi d'une lettre au premier ministre belge Verhofstadt, à l'époque président du Conseil des Ministres de l'UE dans le cadre de la présidence belge de l'UE.

Cette lettre visait à souligner l'ingérence du président américain G. W. Bush par son envoi à M. Verhofstad d'une liste des choses à faire en matière de lutte contre le terrorisme. Un des points sur lequel la lettre de la Global Internet Liberty Campaign s'insurgeait était la volonté de la Maison Blanche de s'ingérer dans le processus de décision politique au sein de l'UE en demandant que le principe de la protection des données dans les communications électroniques fasse l'objet de dérogations pour permettre la conservation par les fournisseurs de services de communications électroniques de ces données "pendant une période raisonnable" et pour des motifs différents de la facturation.

Propos recueillis par **Pierre Bouvier**

**Site de l'association Iris** : <http://www.iris.sgdg.org/>

**Site de l'Electronic privacy information center** : <http://www.epic.org/#about>

**Texte de la lettre envoyée à Pat Cox par la Global Internet Liberty Campaign** : [http://www.gilc.org/cox\\_fr.html](http://www.gilc.org/cox_fr.html)

---