

XXIII Conférence internationale des Commissaires de la Protection des Données
Paris, 24-26 septembre 2001

SYNTHÈSE DE L'INTERVENTION DE MARCO CAPPATO, DEPUTÉ EUROPÉEN DE LA "LISTA BONINO" ET RAPPORTEUR DU PE SUR LA PROTECTION DE LA VIE PRIVÉE DANS LES COMMUNICATIONS ÉLECTRONIQUES

INTRODUCTION

Dans l'arrêt Klass de 1978, la Cour européenne des Droits de l'Homme écrit :

"49. ...la Cour relève que le législateur national jouit d'un certain pouvoir discrétionnaire (quant au choix des modalités du système de surveillance). La Cour souligne néanmoins que les Etats contractants ne disposent pas pour autant d'une latitude illimitée pour assujettir à des mesures de surveillance secrète les personnes soumises à leur juridiction. Consciente du danger, inhérent à pareille loi, de saper, voire de détruire, la démocratie au motif de la défendre, elle affirme qu'ils ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure jugée par eux appropriée.

Dans ces mots, on trouve exprimés les risques que nos sociétés, nos Etats, nos citoyens, courent aujourd'hui, et les limites que l'État de droit ne peut pas dépasser. Les attentats terroristes farouches et sanguinaires qui ont frappé les Etats-Unis le 11 septembre dernier ont poussé certains à demander des lois "d'exception". En Italie, nous connaissons très bien les lois dites "d'exception" sur la criminalité organisée, sur le terrorisme, qui se sont enracinées dans le code pénal (qui est le code dont nous avons hérité du fascisme) de façon stable et qu'on a aussi exporté dans d'autres pays. Beaucoup de monde repète en ces jours qu'il faut renoncer à une partie de liberté pour acquérir plus de sécurité, et que dans une période d'insécurité il faut des mesures exceptionnelles. Cela ne me dérange pas quand il s'agit des contrôles à l'aéroport ou à la douane, mais je suis contre les propositions qui viseraient à instaurer des systèmes d'accès permanent à la vie privée des citoyens de la part de l'Etat.

L'UNION EUROPEENNE

La proposition de directive de la Commission européenne sur la protection de la vie privée dans le cadre des communications électroniques - qui modifie une directive de 1997 sur le même sujet à la lumière des nouveaux développements technologiques et dans un cadre de libéralisation du secteur des télécommunications – est actuellement à l'examen du PE et du Conseil. Certains Ministres des Télécommunications, poussés par leur collègues de l'Intérieur et par les Polices, veulent modifier la directive dans la partie qui impose l'effacement des données relatives au trafic téléphonique (numéro appelant, numéro appelé, durée de la communication, heure de début et de fin de la communication,...) et à la localisation du téléphone mobile une fois que le traitement de ces données pour la facturation est

terminé. Certains gouvernements au sein du Conseil veulent introduire ces modifications afin de pouvoir imposer aux fournisseurs de services de communication la rétention de ces données pendant des périodes plus longues, voire jusqu'à 7 ans, afin de permettre aux polices d'y chercher, suite à une autorisation judiciaire, les données nécessaires pour la recherche des criminels et de les utiliser comme des preuves.

Sur ce point, il faut rappeler que ces données "externes" de la communication, sont souvent traitées de la même façon que le contenu de la communication même, comme l'a fait par exemple la jurisprudence italienne: la Cour Suprême de Cassation a jugé, en 1998, que les données de trafic ne sont pas utilisables comme preuve dans un procès sans l'autorisation de l'autorité judiciaire. Donc la conservation de ces données – qui est une des phases du traitement - qu'elle soit faite par l'Etat ou le fournisseur de services, et étant assimilable à l'enregistrement du contenu de la conversation, est à considérer comme une interception de communication. L'idée qui circule au sein du Conseil viserait donc à l'instauration d'un système de surveillance à grande échelle.

Une deuxième considération doit être faite, d'ordre économique: l'obligation de conserver les données de trafic pendant sept ans représenterait un coût important pour les fournisseurs de services, qui aurait des conséquences économiques pour les abonnés et les utilisateurs. Ce facteur a par exemple fait échouer les plans du gouvernement du Royaume Uni de créer une banque de données étatique.

Si le Conseil se dirige vers le renforcement de la cybersurveillance, la Commission des libertés et des droits des citoyens avait appuyé à l'unanimité mes amendements qui visaient à introduire dans la directive une référence explicite à la jurisprudence de la Cour européenne des droits de l'homme. Le texte approuvé récitait:

(Art. 15, par.1): "Les États membres peuvent prendre des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1 à 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue, **dans une société démocratique**, une mesure nécessaire, **appropriée, proportionnée et limitée dans le temps** pour sauvegarder la sûreté de l'État, la défense, la sécurité publique, la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de l'utilisation non autorisée du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. **Ces mesures doivent être tout à fait exceptionnelles, fondées sur une loi précise qui soit compréhensible du grand public et autorisées par les autorités judiciaires ou compétentes dans des cas particuliers. En vertu de la Convention européenne des droits de l'homme et conformément aux arrêts rendus par la Cour européenne des droits de l'homme, toute forme de surveillance électronique générale ou exploratoire pratiquée à grande échelle est interdite**".

Après ce vote, mon Rapport a été renvoyé en commission suite à un vote en plénière très controversé, notamment sur la question de l'opt-in ou de l'opt-out sur les communications électroniques commerciales non sollicitées. Par conséquent les

propositions du PE sur la protection de la vie privée doivent être discutées à nouveau dans les prochains mois.

Personnellement, je vais maintenir ma position, et non seulement pour une question de fond, mais aussi de méthode, qui touche à l'ensemble des décisions que l'Union européenne est en train de prendre. Sur des sujets aussi sensibles, on ne peut pas accepter la méthode fondamentalement non démocratique de l'Union européenne, notamment en matière de coopération policière et judiciaire. Le Conseil débat et décide en secret. Europol, Schengen, Enfopol et Eurojust échappent à tout contrôle démocratique et juridictionnel. Après l'attentat aux USA, toutes les résistances au renforcement de ces instruments semblent surmontées; notamment presque tout le monde paraît d'accord avec le mandat opérationnel d'Europol, mais la question du pouvoir parlementaire et de la Cour de justice n'est pas abordé.

CYBERSECURITÉ OU CYBERDÉMOCRATIE: QUELLE PRIORITÉ ?

Evidemment, après ce qui c'est passé aux États-Unis, les discours se focalisent sur l'utilisation de l'informatique par les organisations criminelles et par les États. La réquête d'augmenter la sécurité des citoyens ne peut pas rester sans réponse. La route qu'on a pour l'instant décidé de parcourir est celle du renforcement des mécanismes de contrôle par l'Etat. Mais si l'on peut accepter un nouvel équilibre entre liberté et sécurité, on ne peut certainement pas renoncer, au nom de la sécurité, à des principes et à des libertés fondamentales qui caractérisent les États de droit démocratiques. On doit en particulier s'opposer à tous ce qui profitent de la situation afin d'imposer, comme des véritables chacal du pouvoir, des politiques répressives et même violentes (voire les déclaration de Putin, qui fait le parallèle entre la violence subit par les USA et celle que la Russie "subirait" en Tchétchénie, où en réalité il a amené la guerre et la terreur).

CONSIDÉRATIONS ET PROPOSITIONS

* Les spécialistes des services secrets sont presque unanimes à souligner que les limites de "l'intelligence" résident surtout dans une stratégie trop axée sur le travail à distance et la technologie, notamment l'interception des données, et trop peu basée sur le travail de terrain, avec des agents en chair et os. On comprend bien la raison de cette stratégie, qui prend en compte les coûts humains et économiques de l'action directe. Si cette stratégie, seule, a échoué, il est peut-être nécessaire de l'accompagner d'autres mesures, en donnant la priorité au travail sur le terrain.

* Les criminels organisés ne vont pas s'arrêter face à des systèmes de sécurité conçus pour contrôler la généralité des citoyens; ils sont en mesure d'utiliser des systèmes sophistiqués. Par contre, on ne peut pas accepter que le surveillé, l'"ennemi", devienne le simple citoyen qui surfe sur le Net ou qui passe un coup de téléphone.

* Les systèmes de protection de la vie privée, comme la cryptographie, peuvent être très utiles non seulement pour les criminels, mais aussi pour se défendre des criminels.

* On doit concevoir et réaliser une contre-offensive démocratique, pour la diffusion de la connaissance et des instruments qui aident les citoyens à exercer leur pouvoir. Il n'est seulement question de protéger les citoyens (privacy), ou de lutter contre les criminels (cybercrime), mais aussi et surtout de renforcer le citoyen grâce aux nouvelles technologies:

- démocratie en ligne: transmission "on line" de tous les moments publics des nos démocraties; possibilité de réaliser via Internet tous les actes "publiques" (c'est ce qui demandent les propositions de loi d'initiative populaire sur lesquels les radicaux italiens sont en train de recueillir les signatures)
- diffusion de l'information: Radio "Voice of europe"; battre les centrales de propagande avec la contre-information.
- surmonter la censure, les filtres qui bloquent le réseau; la liberté d'expression doit être insérée comme condition dans les accords internationaux.

Marco Cappato