Programme de surveillance de la NSA, organismes de surveillance dans divers Etats membres et incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures

2013/2188(INI) - 12/03/2014 - Texte adopté du Parlement, lecture unique

Le Parlement européen a adopté par 544 voix pour, 78 voix contre et 60 abstentions, une résolution sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures.

Le Parlement indique qu'en comparaison des mesures prises par les institutions européennes et par certains États membres, il a pris très au sérieux son obligation de faire la lumière sur les révélations des pratiques non sélectives de surveillance de masse des citoyens européens. Il a ainsi chargé sa commission des libertés civiles, de la justice et des affaires intérieures de mener une enquête approfondie sur la question.

Principales conclusions : le Parlement estime que les révélations faites dans la presse par des lanceurs d'alerte et des journalistes, ainsi que les témoignages d'experts recueillis pendant cette enquête, les aveux des autorités et l'insuffisance de la réaction face à ces allégations, ont permis d'obtenir des **preuves irréfutables de l'existence de systèmes vastes, complexes et technologiquement très avancés** conçus par les services de renseignement des États-Unis et de certains États membres dans le but de collecter, de stocker et d'analyser les données de communication, y compris les données de contenu, et les données et métadonnées de localisation des citoyens du monde entier, à une échelle sans précédent, sans aucun discernement et sans se baser sur des soupçons.

Il attire plus particulièrement l'attention sur :

- les programmes de renseignement de la NSA permettant la surveillance de masse des citoyens de l'Union européenne grâce à l'accès direct aux serveurs centraux des grandes entreprises américaines du secteur de l'internet (programme PRISM), à l'analyse de contenus et de métadonnées (programme Xkeyscore), au contournement du cryptage en ligne (BULLRUN), et à l'accès aux réseaux informatiques et téléphoniques et aux données de localisation ;
- les systèmes de l'agence de renseignement britannique GCHQ, notamment son activité de surveillance en amont (programme Tempora), etc.

Il souligne que la confiance entre les deux partenaires transatlantiques a été profondément mise à mal. Pour la restaurer, il est indispensable d'adopter un **plan d'intervention immédiat et global** prévoyant un ensemble de mesures soumises au contrôle des citoyens.

Alors que plusieurs gouvernements affirment que ces programmes de surveillance de masse sont nécessaires à la lutte contre le terrorisme, le Parlement considère que cela ne peut en aucun cas justifier l'existence de programmes de surveillance de masse non ciblés, secrets, voire illégaux. Il réfute l'idée selon laquelle toutes les questions liées aux programmes de surveillance de masse relèveraient strictement

de la sécurité nationale et, dès lors, de l'unique compétence des États membres. La discussion et l'action au niveau de l'Union européenne ne sont pas seulement légitimes, elles sont nécessaires pour l'autonomie de l'Union.

Recommandations : le Parlement demande aux autorités américaines et aux États membres de l'Union européenne **d'interdire les activités de surveillance de masse aveugle**. Il demande également à la nouvelle Commission de prendre des engagements politiques forts en vue de mettre en œuvre les propositions et recommandations de l'enquête.

Les États membres sont appelés à :

- procéder à un examen complet, et à la révision au besoin, de leurs législations et pratiques régissant les activités des services de renseignement, afin de s'assurer qu'elles font l'objet d'un contrôle parlementaire et judiciaire et sont soumises à la vigilance des citoyens ;
- satisfaire immédiatement à l'obligation qui leur incombe au titre de la convention européenne des droits de l'homme de protéger leurs citoyens des activités de surveillance contraires aux dispositions de celle-ci, y compris lorsque ces activités visent à garantir la sécurité nationale, que ces activités soient réalisées par des pays tiers ou par leurs propres services de renseignement ;
- veiller à ce que l'état de droit ne soit pas affaibli par l'application extraterritoriale du droit d'un pays tiers.

Le Royaume-Uni, la France, l'Allemagne, la Suède, les Pays-Bas et la Pologne sont spécifiquement appelés à veiller à ce que leur cadre législatif et leurs mécanismes de contrôle applicables aux activités des services de renseignement soient conformes aux normes de la convention européenne des droits de l'homme et au droit de l'Union et à faire la lumière sur les allégations concernant des activités de surveillance massive des communications transfrontalières. Les États membres sont également appelés à faire la lumière sur la présence sur le territoire de l'Union de personnels et d'équipements de renseignement américains **sans contrôle sur les opérations de surveillance**.

La Commission est quant à elle invitée à :

- réaliser, avant juillet 2014, une évaluation de l'applicabilité du règlement (CE) n° 2271/96 aux cas de conflits de législations lors de transferts de données à caractère personnel ;
- présenter des mesures prévoyant la suspension immédiate de sa décision 2000/520/CE, qui déclare la pertinence de la protection assurée par les principes de la "sphère de sécurité". Á ce sujet, les autorités des États-Unis sont invitées à présenter une proposition de nouveau cadre pour les transferts de données à caractère personnel de l'Union européenne vers les États-Unis, qui respecte les exigences de protection des données de l'Union et garantisse un degré de protection adéquat ;
- présenter d'ici décembre 2014 une évaluation complète du cadre américain en matière de respect de la vie privée, portant sur les activités commerciales, policières et de renseignement, ainsi que des recommandations concrètes en l'absence de loi générale sur la protection des données aux États-Unis ;
- travailler de concert avec les autorités des États-Unis afin d'établir un cadre juridique garantissant un degré élevé de protection des personnes eu égard à la protection de leurs données à caractère personnel lorsqu'elles sont transférées aux États-Unis, et veiller à l'équivalence des cadres européen et américain de respect de la vie privée ;
- effectuer, avant fin 2014, une **évaluation approfondie de l'accord en matière d'entraide judiciaire existant** ;
- reprendre immédiatement les négociations avec les États-Unis sur **l'accord-cadre pour la protection des données dans le domaine de la coopération policière et judiciaire**, en vue de placer les droits des citoyens de l'Union européenne sur un pied d'égalité avec ceux des ressortissants des États-Unis et **ne se lancer dans aucun autre accord** tant que l'accord-cadre ne sera pas entré en vigueur;

- réagir au fait que trois des principaux systèmes informatisés de réservation utilisés par les compagnies aériennes partout dans le monde sont basés aux États-Unis et que les données PNR sont sauvegardées dans des systèmes en nuage opérant sur le sol américain et régis par le droit américain, ce qui n'est pas conforme aux dispositions en matière de pertinence de la protection des données ;
- présenter, avant décembre 2014, une proposition concernant une **procédure européenne d'habilitation de sécurité pour l'ensemble des titulaires européens d'une charge publique** ;
- présenter une proposition législative visant à interdire le recours aux "portes dérobées" ("backdoors") par les services répressifs ;
- présenter, en janvier 2015 au plus tard, un **plan d'action en vue de renforcer l'indépendance de l'Union européenne dans le secteur informatique**, présentant une approche plus cohérente pour renforcer les capacités technologiques informatiques européennes (y compris systèmes, équipement, services informatiques, informatique en nuage, etc.) ;
- soutenir sans réserve, y compris au moyen de **financements dans le domaine de la recherche et du développement**, le développement des capacités innovatrices et technologiques européennes en matière d'outils, de sociétés et de fournisseurs dans le secteur de l'informatique (matériel, logiciels, services et réseau), notamment aux fins de la cybersécurité et des capacités de cryptage et cryptographiques ;
- présenter, avant décembre 2014, des propositions législatives pour encourager les fabricants de logiciels et de matériel à renforcer la sécurité et la vie privée en incluant des fonctions par défaut dans leurs produits, dès le stade de la conception. Ces propositions devraient également comprendre des mesures pour décourager la collecte excessive et disproportionnée de données à caractère personnel en masse et l’introduction d’une responsabilité légale pour les fabricants en cas de vulnérabilités connues non corrigées, de produits défectueux ou non sûrs, ou d'installation de portes dérobées secrètes permettant d'accéder sans autorisation aux données et de les traiter.

Menace de blocage de l’accord TTIP : le Parlement a également souligné que l'approbation de l’accord transatlantique (le TTIP) par le Parlement européen pourrait être menacée tant que les activités de surveillance de masse aveugle et l'interception des communications au sein des institutions et des représentations diplomatiques de l'Union européenne n'auront pas été complètement abandonnées et qu'une solution adéquate n'aura pas été trouvée en ce qui concerne les droits des citoyens de l'Union européenne en matière de confidentialité des données. Il souligne que le Parlement européen ne peut approuver le TTIP final qu'à condition que l'accord respecte pleinement, entre autres, les droits fondamentaux reconnus par la charte de l'Union européenne, et exige que la protection de la vie privée des individus en ce qui concerne le traitement et la diffusion des données à caractère personnel continue à être régie par l'article XIV de l'AGCS. Il souligne que la législation européenne en matière de protection des données ne saurait être vue comme une "discrimination arbitraire ou injustifiable" au sens de l'article XIV de l'AGCS.

Parallèlement, le Parlement demande la création d'un **groupe de haut niveau** qui proposerait, de manière transparente et en collaboration avec les parlements, des recommandations et des mesures pour :

- améliorer le contrôle démocratique, y compris le contrôle parlementaire, des services de renseignement ;
- renforcer la collaboration dans l'Union en matière de contrôle, en particulier en ce qui concerne la dimension transfrontières de cette collaboration ;
- définir des normes ou des **règles minimales contraignantes** à l'échelle de l'Europe **sur le contrôle** (*ex ante* et *ex post*) **des services de renseignement**, fondées sur les bonnes pratiques existantes et sur les recommandations d'organisations internationales ;
- préparer un rapport et collaborer à l'organisation d'une conférence à l'initiative du Parlement avec les organes de contrôle nationaux, qu'ils soient parlementaires ou indépendants, avant le début de l'année 2015.

La résolution propose en outre de lancer un «***habeas corpus* numérique européen protégeant les droits fondamentaux à l'ère numérique**», fondé sur huit actions et s'appuyant sur un calendrier à respecter. Sa mise en œuvre inclut, entre autres :

- l'adoption du paquet relatif à la protection des données en 2014 ;
- la conclusion de l'accord-cadre entre l'Union européenne et les États-Unis garantissant le droit fondamental des citoyens au respect de la vie privée et à la protection des données, et assurant des mécanismes de recours adéquats aux citoyens européens ;
- la suspension de la "**sphère de sécurité**" (normes volontaires sur la protection des données pour les entreprises non-européennes qui transfèrent des données à caractère personnel de citoyens de l'UE aux États-Unis) jusqu'à ce qu'une analyse complète de celle-ci soit effectuée et que ses lacunes soient corrigées ;
- **la suspension de l'accord TFTP** (programme de surveillance du financement du terrorisme) en attendant i) la conclusion des négociations concernant l'accord-cadre; ii) la réalisation d'une enquête approfondie sur la base d'une analyse européenne et la prise en compte de l'ensemble des préoccupations soulevées par le Parlement dans sa résolution du 23 octobre 2013 ;
- une proposition législative de la Commission établissant un programme européen efficace et global de protection des lanceurs d'alerte (le Parlement demande notamment aux États membres d'examiner de manière approfondie la possibilité d'octroyer aux lanceurs d'alerte, une protection internationale contre les poursuites) ;
- le développement d'une stratégie européenne en vue d'une plus grande indépendance informatique.

Enfin, les services compétents du secrétariat du Parlement européen sont appelés à effectuer, avant juin 2015, avec un **rapport intermédiaire** évaluant **la fiabilité du Parlement sur le plan de la sécurité informatique**, en s'intéressant plus particulièrement aux moyens budgétaires, aux ressources en personnel, aux capacités techniques, à l'organisation interne et à l'ensemble des éléments pertinents, en vue d'améliorer la sécurité des systèmes informatiques du Parlement.

Dans la foulée, la Plénière a chargé sa commission LIBE de s'adresser au Parlement sur le sujet un an après l'adoption de la présente résolution en vue d'évaluer la mesure dans laquelle les recommandations adoptées par le Parlement ont été suivies ou non d'effets.