Parlement européen
2014-2019

TEXTES ADOPTÉS
Édition provisoire

P8_TA-PROV(2015)0388

Suivi de la résolution du Parlement européen du 12 mars 2014 sur la surveillance électronique de masse des citoyens de l'Union européenne

Résolution du Parlement européen du 29 octobre 2015 sur le suivi de la résolution du Parlement européen du 12 mars 2014 sur la surveillance électronique de masse des citoyens de l'Union européenne (2015/2635(RSP))

Le Parlement européen,

– vu le cadre juridique établi par le traité sur l'Union européenne (traité UE), notamment ses articles 2, 3, 4, 5, 6, 7, 10 et 21, la charte des droits fondamentaux de l'Union européenne, notamment ses articles 1, 3, 6, 7, 8, 10, 11, 20, 21, 42, 47, 48 et 52, la convention européenne des droits de l'homme, notamment ses articles 6, 8, 9, 10 et 13, et la jurisprudence des juridictions européennes en matière de sécurité, de respect de la vie privée et de liberté d'expression,

– vu sa résolution du 12 mars 2014 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[1] (ci-après "la résolution");

– vu le document de travail du 19 janvier 2015 relatif au suivi de l'enquête de la commission LIBE sur la surveillance électronique de masse des citoyens de l'Union européenne[2];

– vu la résolution de l'Assemblée parlementaire du Conseil de l'Europe du 21 avril 2015 sur la surveillance de masse;

– vu les questions posées au Conseil et à la Commission sur le suivi de la résolution du Parlement européen du 12 mars 2014 sur la surveillance électronique de masse des citoyens de l'Union européenne (O-000 114/2015 – B8-0769/2015 et O-000 115/2015 – B8-0770/2015),

---

1 Textes adoptés de cette date, P7_TA(2014)0230.
2 PE546.737v01-00.

– vu la proposition de résolution de la commission des libertés civiles, de la justice et des affaires intérieures,

– vu l'article 128, paragraphe 5, et l'article 123, paragraphe 2, de son règlement,

A. considérant que dans sa résolution, le Parlement appelait les autorités des États-Unis et les États membres à interdire les activités de surveillance de masse aveugle et le traitement massif de données à caractère personnel de citoyens et dénonçait les actions des services de renseignement signalées comme ayant gravement nui à la confiance et aux droits fondamentaux des citoyens de l'Union européenne; que la résolution attirait l'attention sur l'existence possible d'autres motifs, notamment l'espionnage politique ou économique, eu égard à la capacité des programmes de surveillance de masse signalés;

B. considérant que la résolution lançait "un habeas corpus numérique européen protégeant les droits fondamentaux à l'ère numérique" fondé sur huit actions spécifiques et chargeait la commission des libertés civiles, de la justice et des affaires intérieures de faire rapport au Parlement d'ici un an afin d'évaluer dans quelle mesure les recommandations auront été suivies;

C. considérant que le document de travail du 19 janvier 2015 rendait compte des avancées depuis l'adoption de la résolution, alors que de nouvelles allégations d'activités de surveillance électronique de masse sont régulièrement dévoilées, et de l'état de la mise en œuvre de l'"habeas corpus numérique européen" proposé dans la résolution, en mentionnant la réaction limitée des institutions, des États membres et des parties concernées suite à cet appel à agir;

D. considérant que dans sa résolution, le Parlement invitait la Commission et les autres institutions, organes, offices et agences européens à donner suite aux recommandations, conformément à l'article 265 du traité FUE ("abstention");

E. considérant que Wikileaks a récemment révélé la surveillance ciblée des communications des trois derniers présidents de la République française, de ministres français et de l'ambassadeur de France aux États-Unis; que cet espionnage stratégique et économique mené à grande échelle par la NSA au cours des dix dernières années a pris pour cible l'ensemble des structures de l'État français ainsi que les principales entreprises françaises;

F. considérant que dans son rapport, le rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression indique que le cryptage et l'anonymat apportent la confidentialité et la sécurité nécessaires à l'exercice du droit à la liberté d'opinion et d'expression à l'ère numérique; que ce rapport indique aussi que toutes les restrictions en matière de cryptage et d'anonymat doivent être strictement limitées et conformes aux principes de légalité, de nécessité, de proportionnalité et de légitimité dans l'objectif;

1. se félicite de l'ouverture d'enquêtes par le Bundestag allemand, le Conseil de l'Europe, les Nations unies et le Sénat brésilien, des débats tenus dans plusieurs autres parlements nationaux et de l'action de nombreux acteurs de la société civile, qui ont contribué à sensibiliser l'opinion publique au sujet de la surveillance électronique de masse;

2. invite les États membres de l'Union à abandonner toute poursuite en cours contre Edward Snowden, à lui offrir une protection et à empêcher en conséquence son extradition ou sa restitution par une tierce partie, en signe de reconnaissance de son statut de lanceur d'alerte et de défenseur international des droits de l'homme;

3. se déclare toutefois profondément déçu par le manque généralisé de sentiment d'urgence et de volonté dont ont fait preuve la plupart des États membres et les institutions de l'Union appelés à examiner attentivement les points abordés dans la résolution et à appliquer les recommandations concrètes qu'elle contient, ainsi que par le manque de transparence et de dialogue envers le Parlement;

4. s'inquiète de certaines lois qui, adoptées récemment dans certains États membres, étendent les capacités de surveillance des services de renseignements, notamment, en France, de la nouvelle loi adoptée par l'Assemblée nationale le 24 juin 2015, dont plusieurs dispositions soulèvent, selon la Commission, d'importants problèmes juridiques, au Royaume-Uni, de l'adoption du *Data Retention and Investigatory Powers Act* (loi sur la conservation des données et les pouvoirs d'enquête) de 2014 et de la décision de justice ultérieure selon laquelle certains articles étaient contraires à la loi et ont dû être écartés et, aux Pays-Bas, des propositions de nouvelle législation visant à actualiser la loi de 2002 sur le renseignement et la sécurité; réitère son appel à tous les États membres de veiller à ce que leurs cadres législatifs et mécanismes de surveillance régissant les activités des agences de renseignement actuels et futurs soient conformes aux normes de la convention européenne des droits de l'homme et à tous les actes législatifs pertinents de l'Union;

5. se félicite de l'enquête du Bundestag allemand sur la surveillance de masse; s'inquiète vivement de la révélation de surveillance de masse des télécommunications et des données en circulation sur internet au sein de l'Union par le BND (services de renseignements allemands), en coopération avec la NSA; estime qu'il s'agit d'une violation du principe de coopération loyale consacré à l'article 4, paragraphe 3, du traité UE;

6. demande à son Président d'inviter le secrétaire général du Conseil de l'Europe à lancer la procédure au titre de l'article 52 qui prévoit que "[t]oute Haute Partie contractante fournira sur demande du Secrétaire Général du Conseil de l'Europe les explications requises sur la manière dont son droit interne assure l'application effective de toutes les dispositions de cette Convention";

7. considère que la manière dont la Commission a jusqu'ici réagi à la résolution est très insuffisante compte tenu de l'ampleur des révélations; appelle la Commission à agir avant décembre 2015 au plus tard concernant les demandes incluses dans la résolution; se réserve le droit d'engager un recours en carence ou de placer en réserve certaines ressources budgétaires destinées à la Commission jusqu'à ce que toutes les recommandations aient été correctement prises en compte;

8. insiste sur l'importance de l'arrêt rendu le 8 avril 2014 par la Cour de justice de l'Union européenne qui invalide la directive 2006/24/CE sur la conservation de données; rappelle que la Cour a décidé que la manière dont l'instrument interfère avec le droit fondamental au respect de la vie privée doit se limiter au strict nécessaire; souligne que cette décision présente un aspect nouveau dans la mesure où la Cour renvoie spécifiquement à une jurisprudence particulière de la Cour européenne des droits de

l'homme relative à la question des "programmes généraux de surveillance" et qu'elle a désormais effectivement intégré les mêmes principes, provenant de cette jurisprudence particulière de la Cour européenne des droits de l'homme, dans le droit de l'Union dans ce même domaine; souligne qu'il faut donc s'attendre à ce que la Cour applique également, à l'avenir, le même raisonnement lors de l'évaluation de la validité, au regard de la charte, d'autres actes législatifs de l'Union et des États membres dans ce même domaine des "programmes généraux de surveillance";

Train de mesures sur la protection des données

9. se félicite de l'ouverture de négociations interinstitutionnelles informelles sur le projet de règlement général sur la protection des données et de l'adoption, par le Conseil, d'une orientation générale sur le projet de directive relative à la protection des données; réaffirme son intention de mener à bien les négociations sur le train de mesures sur la protection des données en 2015;

10. rappelle au Conseil qu'il s'est engagé à respecter la charte des droits fondamentaux de l'Union européenne dans les amendements qu'il apporte aux propositions de la Commission; rappelle, en particulier, que le niveau de protection offert ne doit pas être inférieur à celui déjà fixé par la directive 95/46/CE;

11. souligne que le règlement relatif à la protection des données et la directive relative à la protection des données sont tous deux nécessaires pour protéger les droits fondamentaux des individus et qu'ils doivent dès lors être traités comme un tout à adopter simultanément afin de s'assurer que l'ensemble des activités de traitement de données dans l'Union prévoient un niveau élevé de protection en toutes circonstances; insiste sur le fait que l'objectif du renforcement des droits et de la protection des personnes physiques lors du traitement de leurs données personnelles doit être satisfait lors de l'adoption du train de mesures;

Accord-cadre entre l'Union européenne et les États-Unis

12. observe que, depuis l'adoption de la résolution, les négociations avec les États-Unis sur l'accord-cadre UE-États-Unis sur la protection des données à caractère personnel lors de leur transfert et de leur traitement à des fins répressives (ci-après dénommé l'"accord-cadre") ont été menées à bien et que le projet d'accord a été paraphé;

13. se félicite des efforts déployés par le gouvernement des États-Unis afin de restaurer la confiance par l'intermédiaire de l'accord-cadre, et salue en particulier le fait que le *Judicial Redress Act* de 2015 ait été adopté avec succès par la Chambre des représentants le 20 octobre 2015, ce qui témoigne des efforts considérables et constructifs consentis par les États-Unis afin de répondre aux préoccupations de l'Union; estime qu'il est crucial de garantir, dans toutes les circonstances identiques, les mêmes droits en matière de recours juridique effectif aux citoyens ou personnes physiques de l'Union dont les données personnelles sont traitées au sein de l'Union et transférées aux États-Unis sans distinction entre citoyens de l'Union et des États-Unis ; invite le Sénat des États-Unis à adopter des dispositions législatives en ce sens; insiste sur le fait qu'une condition préalable à la signature et à la conclusion de l'accord-cadre est l'adoption du *Judicial Redress Act* au Congrès américain;

Sphère de sécurité

14. rappelle que la résolution demande la suspension immédiate de la décision sur la sphère de sécurité dans la mesure où celle-ci n'assure pas une protection suffisante des données personnelles des citoyens de l'Union;

15. rappelle que tout accord international conclu par l'Union prime sur le droit dérivé de l'Union et souligne par conséquent qu'il faut s'assurer que l'accord-cadre ne limite pas les droits des personnes concernées et les garanties qui s'appliquent au transfert de données en vertu du droit de l'Union; prie donc instamment la Commission d'évaluer précisément la façon dont l'accord-cadre interagirait avec le cadre juridique de l'Union relatif à la protection des données et les effets qu'il aurait sur ce cadre juridique, et notamment la présente décision-cadre du Conseil, la directive relative à la protection des données (95/46/CE) et les futurs règlement et directive relatifs à la protection des données; demande à la Commission de remettre un rapport d'évaluation juridique sur la question au Parlement avant d'entamer la procédure de ratification;

16. rappelle que la Commission a adressé 13 recommandations aux États-Unis dans ses communications du 27 novembre 2013 sur le fonctionnement de la sphère de sécurité, afin d'assurer un niveau de protection adéquat;

17. se félicite que dans son arrêt du 6 octobre 2015, la Cour de justice de l'Union européenne ait déclaré invalide la décision 2000/520/CE de la Commission relative à la pertinence de la protection assurée par les principes de la sphère de sécurité; souligne que cet arrêt a confirmé la position adoptée de longue date par le Parlement relative à l'absence d'un niveau de protection adéquat dans le cadre de cet instrument; invite la Commission à prendre immédiatement les mesures nécessaires pour faire en sorte que les données à caractère personnel transférées vers les États-Unis fassent l'objet d'un bon niveau de protection, en substance équivalent à celui garanti dans l'Union européenne;

18. déplore que le Parlement n'ait reçu aucune communication formelle de la part de la Commission concernant l'état de la mise en œuvre des 13 recommandations, contrairement à ce que la Commission avait annoncé, à savoir qu'elle communiquerait à ce sujet d'ici l'été 2014; souligne qu'à la suite de la décision de la Cour de justice d'invalider la décision 2000/520/CE, il est aujourd'hui urgent que la Commission fasse un point complet sur l'état des négociations à ce stade et l'incidence de l'arrêt sur la poursuite des négociations qui ont été annoncés; demande à la Commission de réfléchir sans plus attendre à des solutions de substitution à la sphère de sécurité ainsi qu'à l'incidence de l'arrêt sur tout autre instrument pour ce qui concerne le transfert de données à caractère personnel vers les États-Unis, et de les présenter avant la fin de l'année 2015 au plus tard;

19. demande instamment à la Commission d'évaluer l'incidence et les implications juridiques de l'arrêt de la Cour de justice du 6 octobre 2015 dans l'affaire Schrems (C-362/14) à l'égard des accords conclus avec des pays tiers autorisant le transfert de données à caractère personnel tels que l'accord UE-US relatif au programme de surveillance du financement du terrorisme (TFTP), les accords sur l'utilisation et le transfert des données des dossiers passagers (PNR), l'accord-cadre UE-US et d'autres instruments du droit de l'Union qui impliquent la collecte et le traitement de données à caractère personnel;

Surveillance démocratique

20. tout en respectant pleinement que les parlements nationaux soient maîtres du contrôle des services de renseignements nationaux, appelle l'ensemble des parlements nationaux qui ne l'ont pas encore fait à évaluer de manière approfondie et à mettre en place une surveillance appropriée des activités de renseignement et à s'assurer que ces comités/organes de surveillance soient dotés des ressources, de l'expertise technique et des moyens juridiques nécessaires à cet égard et disposent d'un accès à tous les documents pertinents afin de pouvoir assurer un contrôle efficace et indépendant des services de renseignement tout comme des échanges d'informations avec d'autres services de renseignement étrangers; réitère sa volonté de coopérer étroitement avec les parlements nationaux afin que des mécanismes de surveillance efficaces soient mis en place, y compris par l'échange de bonnes pratiques et de normes communes;

21. compte assurer un suivi de la conférence sur la surveillance démocratique des services de renseignement dans l'Union européenne qui s'est tenue les 28 et 29 mai 2015 et poursuivra ses efforts de partage des bonnes pratiques sur la surveillance du renseignement, en coordination étroite avec les parlements nationaux; se réjouit de l'intention des coprésidents de cette conférence, contenue dans leurs observations finales communes, de convoquer une conférence de suivi dans deux ans;

22. estime que les instruments actuels de coopération entre les organes de surveillance, par exemple le réseau européen des organes nationaux de contrôle des services de renseignement (ENNIR), devraient être soutenus et plus largement utilisés, par exemple en tirant profit du potentiel d'IPEX pour l'échange d'informations entre les parlements nationaux, dans le respect de son champ d'application et de sa capacité technique;

23. demande à nouveau la suspension de l'accord sur le programme de surveillance du financement du terrorisme;

24. insiste sur la nécessité d'une définition commune de la "sécurité nationale" pour l'Union et ses États membres, de manière à garantir la sécurité juridique; fait observer que l'absence d'une définition claire rend possible les comportements arbitraires ainsi que les violations des droits fondamentaux et de l'état de droit par les organismes exécutifs et de renseignement dans l'Union;

25. encourage la Commission et les États membres à introduire des clauses d'extinction et d'extension dans leurs textes législatifs autorisant la collecte de données à caractère personnel ou la surveillance de citoyens européens; insiste sur le caractère essentiel de ces clauses pour garantir qu'un instrument invasif pour la vie privée voie son utilité et sa proportionnalité régulièrement évaluées dans une société démocratique;

Rétablissement de la confiance

26. souligne qu'une relation saine entre l'Union et les États-Unis reste absolument indispensable pour les deux parties; observe que les révélations au sujet de la surveillance ont sapé le soutien du public vis-à-vis de cette relation et souligne qu'il convient de prendre des mesures afin de restaurer cette confiance, notamment compte tenu du besoin actuel et urgent de coopération dans un grand nombre de questions géopolitiques d'intérêt commun; insiste, dans ce contexte, sur le fait qu'il importe de parvenir à une solution négociée entre les États-Unis et l'Union dans son ensemble qui respecte les droits fondamentaux;

27. se félicite des récentes décisions législatives et juridiques adoptées aux États-Unis visant à limiter la surveillance de masse par la NSA, telles que l'adoption de l'*USA Freedom Act* au Congrès sans que n'y soit apportée de modification, dans le cadre d'un accord entre les deux chambres et les deux grands partis, et l'arrêt de la *Second Circuit Court of Appeals* (cour d'appel du second circuit) sur le programme de collecte d'enregistrements téléphoniques de la NSA; regrette toutefois que ces décisions concernent principalement les citoyens des États-Unis tandis que la situation reste inchangée pour les citoyens de l'Union;

28. estime que toute décision de recours à une technologie de surveillance devrait s'appuyer sur une évaluation minutieuse de la nécessité et de la proportionnalité; se félicite des résultats du projet de recherche SURVEILLE, qui propose une méthodologie d'évaluation des technologies de surveillance fondée sur des critères juridiques, éthiques et technologiques;

29. souligne que l'Union devrait contribuer à l'élaboration, au niveau des Nations unies, de normes ou de principes internationaux conformes au pacte international des Nations unies relatif aux droits civils et politiques, afin de créer un cadre global de protection des données qui prévoie des restrictions spécifiques en matière de collecte à des fins de sécurité nationale;

30. est convaincu que seule l'élaboration de normes sûres à l'échelle mondiale peut éviter la surenchère en matière de surveillance;

Sociétés privées

31. salue l'initiative du secteur privé des TIC en matière de développement de solutions de sécurité cryptographique et de services internet offrant une meilleure protection de la vie privée; encourage la poursuite du développement d'applications aux paramètres conviviaux, qui aident les clients à déterminer quelles informations ils désirent partager, avec qui et de quelle manière; observe que diverses sociétés ont déjà annoncé leur intention de crypter les communications de bout en bout, en réaction aux révélations concernant la surveillance de masse;

32. rappelle qu'en vertu de l'article 15, paragraphe 1, de la directive 2000/31/EC, les États membres ne doivent pas imposer aux prestataires, pour la fourniture de services de transport, stockage et d'hébergement, une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites; rappelle en particulier que la Cour de Justice de l'Union Européenne, dans les arrêts C-360/10 et C-70/10, a rejeté les mesures de " surveillance active " de la quasi-totalité des utilisateurs des services concernés (fournisseurs d'accès à internet dans un cas, réseau social dans l'autre) et a précisé que toute injonction imposant au prestataire de services d'hébergement une surveillance générale est interdite;

33. se félicite de la publication, par les entreprises de technologies de l'information et de télécommunications, de rapports de transparence au sujet des exigences formulées par les gouvernements en matière de données d'utilisateurs; invite les États membres à publier des statistiques sur leurs exigences à l'égard des entreprises privées en matière d'informations sur les utilisateurs privés;

Accord TFTP

34. est déçu que la Commission n'ait pas tenu compte de l'appel clair lancé par le Parlement en faveur de la suspension de l'accord TFTP dans la mesure où aucune information n'a permis de préciser si les données SWIFT auraient été consultées en dehors de l'accord TFTP par un autre organisme gouvernemental ou ministère américain; entend, à l'avenir, en tenir compte au moment de l'examen d'accords internationaux pour éventuelle approbation;

Autres échanges de données à caractère personnel avec des pays tiers

35. insiste sur sa position selon laquelle il revient à la Commission, en tant que garante des traités, d'effectuer une surveillance rigoureuse et d'adopter des mesures de suivi concernant l'ensemble des accords, mécanismes et décisions adéquates relatifs à des échanges avec des pays tiers concernant des données à caractère personnel;

36. se félicite de l'adoption, le 3 juin 2015, par l'Union et les États-Unis, de la déclaration de Riga visant à renforcer la coopération transatlantique dans le domaine de la liberté, de la sécurité et de la justice, dans laquelle les signataires s'engagent à améliorer la mise en œuvre du traité d'entraide judiciaire (TEJ) entre l'Union et les États-Unis, à achever son examen tel que le prévoit l'accord et à discuter de ces questions avec les autorités compétentes au niveau national; souligne que c'est au titre de l'instrument que sont les TEJ que les autorités répressives des États membres devraient coopérer avec les autorités des pays tiers; invite, à cet égard, les États membres et le gouvernement américain à tenir les engagements précités en vue d'une conclusion rapide de l'examen du TEJ entre l'Union et les États-Unis;

37. invite la Commission à faire rapport, d'ici la fin de l'année 2015 au plus tard, au Parlement sur les failles découvertes dans les divers instruments utilisés pour les transferts internationaux de données en ce qui concerne l'accès par les autorités répressives et les services de renseignements de pays tiers, et sur les moyens d'y remédier, afin de garantir la continuité de la protection adéquate indispensable des données à caractère personnel de l'Union transférées vers des pays tiers;

Protection de l'état de droit et des droits fondamentaux des citoyens de l'Union / renforcement de la protection des lanceurs d'alerte et des journalistes

38. estime que les droits fondamentaux des citoyens de l'Union restent menacés et que trop peu a été fait pour garantir leur protection intégrale en cas de surveillance électronique de masse; déplore les progrès limités quant à la protection des lanceurs d'alerte et des journalistes;

39. regrette que de nombreux programmes de renseignement de masse et à grande échelle semblent aussi répondre aux intérêts économiques des sociétés qui développent et exploitent ces programmes, comme cela s'est produit lors du remplacement du programme ciblé "Thinthread" de la NSA par le programme de surveillance à grande échelle "Trailblazer", attribué à la société SAIC en 2001;

40. réaffirme ses graves préoccupations au sujet des travaux en cours au sein du comité de la convention sur la cybercriminalité du Conseil de l'Europe concernant l'interprétation de l'article 32 de la convention sur la cybercriminalité du 23 novembre 2001

(convention de Budapest) concernant l'accès transfrontalier à des données informatiques stockées avec autorisation ou lorsque le public peut les consulter, et s'oppose à la conclusion de tout protocole additionnel et à la formulation de toute orientation visant à élargir le champ d'application de cette disposition au-delà du régime établi par la convention, qui constitue déjà une exception de taille au principe de territorialité, en ce qu'il pourrait donner aux autorités répressives la possibilité d'accéder librement à distance aux serveurs et aux systèmes informatiques situés dans d'autres juridictions sans avoir recours aux accords multilatéraux ou aux autres instruments de coopération judiciaire mis en place pour garantir les droits fondamentaux des personnes physiques, y compris la protection des données et l'application régulière de la loi; souligne que l'Union a exercé sa compétence dans le domaine de la cybercriminalité et que les prérogatives tant de la Commission que du Parlement doivent être respectées;

41. déplore que la Commission n'ait pas donné suite à la requête du Parlement d'examiner la possibilité d'un programme européen complet de protection des lanceurs d'alerte et invite la Commission à présenter une communication sur ce sujet avant la fin de l'année 2016 au plus tard;

42. se félicite de la résolution adoptée le 23 juin 2015 par l'Assemblée parlementaire du Conseil de l'Europe intitulée "Améliorer la protection des donneurs d'alerte", et notamment de son point 9 sur l'importance de donner l'alerte pour assurer le respect des limites légales imposées à la surveillance massive, et de son point 10, dans lequel elle appelle l'Union européenne à adopter une législation relative à la protection des donneurs d'alerte qui vise également le personnel des services de sécurité nationale ou de renseignement et des entreprises privées qui exercent leurs activités dans ce domaine, et à octroyer l'asile, autant que possible en vertu du droit interne, aux donneurs d'alerte menacés de mesures de rétorsion dans leur pays d'origine, sous réserve que leurs révélations réunissent les conditions nécessaires à leur protection au titre des principes énoncés par l'Assemblée;

43. fait valoir que la surveillance de masse remet sérieusement en question le secret professionnel des professions réglementées, notamment des médecins, des journalistes et des avocats; insiste en particulier sur les droits des citoyens de l'Union à être protégés contre toute surveillance de communications confidentielles avec leurs avocats, surveillance qui serait contraire à la charte des droits fondamentaux de l'Union européenne, notamment à ses articles 6, 47 et 48, et à la directive 2013/48/UE relative au droit d'accès à un avocat; invite la Commission à présenter une communication sur la protection des communications confidentielles dans les professions bénéficiant de la confidentialité des communications, et ce d'ici à la fin de 2016 au plus tard;

44. demande à la Commission d'élaborer des recommandations à l'attention des États membres sur la manière de mettre en conformité les instruments de collecte des données à caractère personnel à des fins de prévention, de détection, d'enquête et de poursuites en matière d'infractions pénales, notamment de terrorisme, avec les arrêts rendus par la Cour de justice de l'Union européenne le 8 avril 2014 sur la conservation des données (affaires C-293/12 et C-594/12) et du 6 octobre 2015 sur la sphère de sécurité (affaire C-362/14); fait notamment référence aux points 58 et 59 de l'arrêt sur la conservation des données et aux points 93 et 94 de l'arrêt sur la sphère de sécurité, qui exigent clairement une collecte de données de manière ciblée plutôt que leur collecte indiscriminée;

45. souligne que la jurisprudence la plus récente, et notamment l'arrêt de la Cour de justice de l'Union européenne du 8 avril 2014 sur la conservation des données, indique clairement que la loi doit apporter la preuve de la nécessité et de la proportionnalité de toute mesure prévoyant la collecte et l'utilisation de données à caractère personnel susceptible d'interférer avec le droit au respect de la vie privée et familiale et le droit à la protection des données; estime regrettable que des considérations politiques entravent souvent le respect de ces principes juridiques lors de l'adoption de décisions; demande à la Commission de faire en sorte, dans le cadre de son programme d'amélioration de la législation, que la législation de l'Union soit de qualité, respecte toutes les normes juridiques et la jurisprudence et soit conforme à la Charte des droits fondamentaux de l'Union européenne; recommande que l'analyse d'impact de toute mesure de sécurité ou de répression prévoyant l'utilisation ou la collecte de données à caractère personnel comporte systématiquement un examen de sa nécessité et de sa proportionnalité;

Stratégie européenne en vue d'une plus grande indépendance informatique

46. est déçu par le fait que la Commission n'ait entrepris aucune action de suivi des recommandations détaillées contenues dans la résolution en vue d'améliorer la sécurité informatique et la protection de la vie privée en ligne au sein de l'Union;

47. se félicite des mesures prises jusqu'à présent pour renforcer la sécurité informatique du Parlement telles qu'elles sont présentées dans le plan d'action sur la sécurité des TIC au Parlement élaboré par la DG ITEC; demande que ces efforts soient poursuivis et que les recommandations contenues dans la décision soient pleinement et rapidement mises en œuvre; invite à examiner à nouveau et, le cas échéant, à modifier la législation dans le domaine des marchés publics afin d'améliorer la sécurité informatique des institutions européennes; appelle au remplacement systématique des logiciels propriétaires par des logiciels ouverts contrôlables et vérifiables dans toutes les institutions de l'Union, à l'introduction d'un critère de sélection "open-source" obligatoire dans toutes les procédures de passation de marchés dans le domaine des TIC à l'avenir, et à la mise à disposition rapide d'outils de cryptage;

48. renouvelle avec force son invitation à développer, dans le cadre de nouvelles initiatives telles que le marché unique numérique, une stratégie européenne destinée à améliorer l'indépendance informatique et la protection de la vie privée en ligne afin de dynamiser l'industrie informatique au sein de l'Union;

49. compte présenter de nouvelles recommandations dans ce secteur à la suite de sa conférence "Protection de la vie privée en ligne par l'amélioration de la sécurité informatique et de l'indépendance informatique de l'Union européenne", prévue pour la fin de l'année 2015, lesquelles se fonderont sur les conclusions de la récente étude STOA sur la surveillance de masse des utilisateurs informatiques;

Gouvernance démocratique et neutre de l'internet

50. se félicite de l'objectif de la Commission visant à faire de l'Union une référence en matière de gouvernance d'internet, ainsi que sa vision d'un modèle de gouvernance multipartite d'internet, réaffirmée au cours de la réunion multipartite mondiale sur l'avenir de la gouvernance d'internet (NETMundial) organisée au Brésil en avril 2014; attend avec intérêt les résultats des projets internationaux en cours dans ce domaine, notamment dans le cadre du forum sur la gouvernance de l'internet;

51. met en garde contre la spirale négative évidente qui menace le droit fondamental au respect de la vie privée et à la protection des données à caractère personnel lorsque chaque fragment d'information sur le comportement humain est considéré comme potentiellement utile à la lutte contre des actes criminels futurs, ce qui se traduit obligatoirement par une culture de la surveillance de masse dans laquelle chaque citoyen est considéré comme un suspect potentiel et entraîne la désagrégation du tissu social et des liens de confiance;

52. a l'intention de tenir compte des résultats de l'étude approfondie de l'Agence des droits fondamentaux concernant la protection des droits fondamentaux dans le contexte de la surveillance, en particulier en ce qui concerne la situation juridique actuelle des personnes physiques au regard des voies de recours dont elles disposent à l'égard des pratiques en cause;

Suivi

53. charge sa commission des libertés civiles, de la justice et des affaires intérieures de continuer à surveiller les avancées dans ce domaine et d'assurer le suivi des recommandations contenues dans la résolution;

o

o o

54. charge son Président de transmettre la présente résolution au Conseil, à la Commission, aux gouvernements et aux parlements des États membres ainsi qu'au Conseil de l'Europe.