Note d'information
Évaluation de la mise en œuvre

Parlement européen

Février 2017

Réexamen de la directive «Vie privée et communications électroniques»

Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques

La présente note d'information fait partie d'une série d'«évaluations de la mise en œuvre» portant sur l'application dans la pratique de la législation en vigueur de l'Union européenne. Chacune de ces notes d'information traite d'une législation spécifique de l'Union qui est susceptible d'être modifiée ou révisée, conformément au programme de travail annuel de la Commission européenne. Ces évaluations de la mise en œuvre ont pour objectif de présenter un bref aperçu des documents publics concernant la mise en œuvre, l'application et l'efficacité de la législation de l'Union à ce jour, en s'appuyant sur les contributions existantes des institutions de l'Union et d'organisations extérieures. Ces textes aideront les commissions parlementaires dans leur travail d'examen des nouvelles propositions, une fois celles-ci déposées.

Commission du Parlement européen compétente au moment de l'adoption de la législation de l'Union: commission des libertés civiles, de la justice et des affaires intérieures (LIBE)[1]
Date d'adoption de la législation initiale en séance plénière: 30 mai 2002.
Entrée en vigueur de la législation initiale: 31 juillet 2002 (article 20).
Date de transposition: avant le 31 octobre 2003 (article 17); les amendements adoptés en 2009[2]devaient être transposés avant le 25 mai 2011 (article 17 de la directive 2009/136).
Date prévue pour la révision de la législation: L'article 18 de la directive exige de la Commission qu'elle présente aux colégislateurs un rapport sur l'application et sur les effets de la directive au plus tard trois ans après la date de transposition[3]et qu'elle fasse les propositions nécessaires de modification de la directive afin d'améliorer son efficacité.
Calendrier pour la modification de la législation: la modification de la directive 2002/58/CE est incluse dans l'annexe 1 au programme de travail 2017 de la Commission (CWP 2017). La proposition a été publiée le 10 janvier 2017.

[1] Commission des libertés et des droits des citoyens, de la justice et des affaires intérieures au moment de l'adoption.

[2] Le texte original a été modifié en 2009 par la directive 2009/136 (directive «droits des citoyens»). Le règlement 611/2013 de la Commission sur la notification des violations de données à caractère personnel fait partie des mesures supplémentaires associées à la directive «Vie privée et communications électroniques». Pour une analyse détaillée de ces modifications et de leurs conséquences, voyez Y. Poullet (2010), Commentary on Directive 2002/58/EC, article 3, 4 and 5 – *Concise European IT law*, pp. 183-199; V. Papakonstantinou et P. de Hert (2011), The Amended EU Law on ePrivacy and Electronic Communications after its 2011 Implementation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights, J. *Marshall Journal of Computer & Information Law* 29 (1).

[3] Les rapports concernés sont disponibles ici.

EPRS | Service de recherche du Parlement européen
Auteure: Lorna Schrefler
Unité Cycle politique
PE 587.347

1. Contexte

Depuis l'adoption de la directive 2002/58/CE concernant le respect de la vie privée dans les communications électroniques (directive «Vie privée et communications électroniques»), d'énormes changements technologiques, économiques et sociaux ont sensiblement influencé la façon dont nous utilisons les communications électroniques et les équipements de communications électroniques tels que les téléphones et les ordinateurs portables. Ces changements ont, entre autres, eu des effets directs sur la façon dont nos données à caractère personnel sont consultées, traitées, employées et, en définitive, protégées[4]. Ce phénomène a eu à son tour un effet sur la capacité de la directive «Vie privée et communications électroniques» à atteindre l'un de ses objectifs principaux: garantir un niveau de protection égal, dans un environnement de communications électroniques, du droit fondamental au respect de la vie privée et familiale, du domicile et des communications et du droit fondamental à la protection des données à caractère personnel (articles 7 et 8, respectivement, de la charte des droits fondamentaux de l'Union européenne)[5]. Cette directive fait partie du cadre réglementaire des communications électroniques; en tant que telle, elle applique la définition des «communications électroniques» donnée dans l'article 2 de la directive 2002/21 (la directive «cadre»)[6]. Comme la suite de cette analyse le montrera, cela a des conséquences directes sur le champ d'application actuel des règles de respect de la vie privée dans les communications électroniques et sur la préservation de la capacité de celles-ci à garantir la clarté juridique dans un environnement technologique en rapide évolution. Ainsi, malgré les modifications apportées en 2009 à la directive 2002/58/CE, la récente expansion des acteurs *over-the-top* (ou OTT, hors offre du fournisseur d'accès à internet) proposant aux consommateurs différents services internet, de messagerie instantanée par exemple, laisse subsister des zones d'ombre, les OTT n'étant actuellement pas couverts par les dispositions de respect de la vie privée dans les communications électroniques[7].

Dans ce contexte, la stratégie pour un marché unique numérique de mai 2015 place le réexamen et la mise à jour des règles existantes en matière de protection de la vie privée dans les communications électroniques parmi ses principales priorités afin de compléter et préciser le cadre législatif de l'Union européenne en matière de protection des données. En effet, la révision de la directive 2002/58/CE a également pour but de garantir que les futures règles en matière de respect de la vie privée dans les communications électroniques soient conformes au règlement général sur la protection des données (RGPD) qui entrera en vigueur en mai 2018[8]. Une proposition à cet effet a été adoptée par la Commission européenne le 10 janvier 2017. Elle

[4] À propos de la définition des données à caractère personnel, de la question de la confiance dans un environnement numérique et des principaux défis en matière de protection des données, voyez S. Monteleone, Golden Eye: Who rules tomorrow's Europe?, At a glance, EPRS, avril 2016. Pour une vue d'ensemble exhaustive des effets des évolutions technologiques sur le respect de la vie privée dans différents aspects de nos vies, voyez C. Akrivopoulou et A. Psygkas (éds.), Personal data privacy and protection in a surveillance era: technologies and practices, IGI global, 2011; ainsi que T. Payton et T. Claypoole, Privacy in the age of big data recognizing threats, defending your rights, and protecting your family, Rowman & Littlefield, 2014.

[5] L'article 1 de la directive «Vie privée et communications électroniques» mentionne le «droit à la vie privée, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques». Il convient de noter que la directive protège à la fois les personnes physiques et les personnes morales utilisant les communications électroniques. La libre circulation dans le marché intérieur de l'Union des données traitées dans le secteur des communications électroniques ainsi que des équipements et services de communications électroniques fait également partie des objectifs principaux mentionnés à l'article 1.

[6] Pour plus de détails concernant le cadre réglementaire et les discussions en cours concernant la pertinence d'une révision de la notion de communications électroniques, voyez L. Schrefler, Reforming the regulatory framework for electronic communications networks and services, Évaluation de la mise en œuvre, EPRS, août 2016. Pour une analyse approfondie, consultez l'avis 03/2016 du groupe de travail «article 29» concernant l'évaluation et le réexamen de la directive «Vie privée et communications électroniques» (2002/58/CE), juillet 2016; et l'avis préliminaire du CEPD sur le réexamen de la directive «Vie privée et communications électroniques» (2002/58/CE), avis 5/2016, Contrôleur européen de la protection des données, juillet 2016. Le groupe de travail «article 29» est une plateforme de coopération composée de représentants des autorités nationales chargées de la protection des données, de la Commission et du CEPD.

[7] Sur ce point, voyez la communication de la Commission intitulée «Les plateformes en ligne et le marché unique numérique – Perspectives et défis pour l'Europe» du 25 mai 2016, COM(2016)288, pp. 6-7.

[8] Pour plus de détails, voyez Review of the ePrivacy Directive – Legislative Train Schedule, Train N. 2, Parlement Européen.

a pour but d'abroger la directive initiale et de la remplacer par un règlement dans le but d'atteindre trois objectifs principaux par un ensemble de modifications ciblées du texte actuel[9]: 1) la confidentialité effective de toutes les communications électroniques grâce à une législation plus neutre du point de vue technologique et ouverte aux évolutions futures; 2) la protection efficace contre les communications commerciales non sollicitées par, entre autres, l'interdiction des appels anonymes de marketing; et 3) une plus grande harmonisation et une plus grande simplification du cadre juridique existant par l'adoption d'un ensemble unique de règles pour l'intégralité de l'Union européenne et par l'élimination des dispositions redondantes et obsolètes[10].

2. Rapports, évaluations et études à l'échelle de l'Union européenne

Rapport pour la Commission européenne – Directive «Vie privée et communications électroniques»: évaluation de sa transposition, de son efficacité et de sa compatibilité avec le projet de règlement général sur la protection des données

Achevée en 2015, cette étude externe [11]menée pour le compte de la Commission européenne s'est concentrée sur cinq sujets principaux concernant la directive «Vie privée et communications électroniques»: son champ d'application géographique et matériel (articles 1 à 3); la confidentialité des communications (article 5, paragraphe 1); les cookies (témoins de connexion) et les autres dispositifs couverts par l'article 5, paragraphe 3; les données relatives au trafic et à la localisation (articles 6 et 9) et les communications commerciales non sollicitées (article 13). Ce rapport s'était fixé trois objectifs: faire un état des lieux de la transposition et de l'application des cinq éléments indiqués ci-dessus[12]; déterminer si la directive 2002/58/CE avait atteint ses objectifs; et fournir une analyse de l'interaction entre la directive «Vie privée et communications électroniques» et la future législation de protection des données[13].

Comment fonctionnent les cookies ou témoins de connexion?
La directive «Vie privée et communications électroniques» est souvent appelée «loi cookies» du fait de sa disposition concernant le stockage des informations et l'accès à des informations dans l'équipement terminal des utilisateurs (article 5, paragraphe 3). Cet article concerne différents dispositifs et, en particulier, les témoins de connexion, de petits fichiers de données qu'un navigateur peut sauvegarder/stocker lorsqu'un utilisateur visite un site internet. Les cookies permettront ensuite au site, lorsque l'utilisateur le visite à nouveau, de reconnaître l'équipement, de mieux comprendre les préférences de l'utilisateur dans le temps et d'utiliser ces informations pour cibler les publicités ou personnaliser la visite en ligne. Il existe différents types de cookies. Lorsqu'ils sont classés par durée de vie, les cookies peuvent être des **témoins de connexion de session** s'ils sont effacés une fois que l'utilisateur ferme son navigateur ou des **témoins de connexion permanents** s'ils sont stockés sur l'appareil de l'utilisateur pendant un certain temps. Le domaine plaçant les cookies donne lieu à une autre distinction importante. Les **témoins de connexion propriétaires** sont ceux placés par le site internet visité. Ils visent essentiellement à améliorer son efficacité et la visite de l'utilisateur. À la différence de ceux-ci, les **témoins de connexion tiers** sont ceux placés par un domaine qui n'est pas le même que le domaine de la page visitée. Ils sont utilisés, entre autres choses, par les réseaux de publicité pour surveiller le comportement des utilisateurs et mieux cibler leurs publicités dans le temps. Une analyse récente du groupe de travail «article 29» a établi que **70 % des témoins de connexion détectés** (35 en moyenne par site internet) sur presque 500 sites internet **étaient des témoins tiers** et tendaient à être **de type permanent**.

En ce qui concerne **le champ d'application géographique et matériel** de la directive «Vie privée et communications électroniques», le rapport relevait que des services semblables (tout du moins du point de vue des utilisateurs) étaient toujours réglementés par trois ensembles séparés de dispositions: le cadre des communications électroniques (auquel la directive «Vie privée et

[9] Pour plus de détails, consultez la section 6.2 de l'analyse d'impact SWD(2017)3 accompagnant la proposition.
[10] Voir Commission européenne, SWD(2017)4, p. 2.
[11] SMART 2013/0071, janvier 2015.
[12] Un ensemble complet de fiches par pays concernant la transposition et l'application dans les États membres est disponible dans l'annexe 1 du rapport et dans un tableau de concordance contenant des références aux rapports par pays.
[13] Il faut noter que le RGPD était encore au stade de projet dans la procédure législative ordinaire durant la rédaction du rapport SMART 2013/0071. Cette section spécifique du rapport n'est donc pas couverte dans la présente note.

communications électroniques» appartient), la législation concernant les services de la société de l'information et les règles concernant les services audiovisuels. En conséquence, la directive 2002/58/CE avait été transposée dans différents cadres juridiques au niveau national. En effet, elle était intégrée, dans certains pays, à la législation concernant les communications électroniques tandis qu'elle faisait partie, dans d'autres, de la législation générale de protection des données ou de la législation de protection des consommateurs. En dernière analyse, cela pouvait signifier que le champ d'application des dispositions individuelles de la directive, en particulier l'article 3 relatif aux services concernés par la législation, variait d'un pays à l'autre. Le rapport ajoutait également que le champ d'application de la directive lui-même était ambigu car il tendait à exclure certains services de la société de l'information qui devaient incontestablement en faire partie. Cette ambiguïté a également entraîné un traitement inégal de services très semblables d'un point de vue fonctionnel. Dans les faits, certains États membres (l'Allemagne et la Finlande par exemple) ont étendu le champ d'application de la directive à des services supplémentaires dans le cadre de la transposition du texte.

Les exigences en matière de **confidentialité des communications** définies dans l'article 5, paragraphe 1, n'ont pas atteint l'objectif d'harmonisation des dispositions nationales dans l'Union européenne. Dans de nombreux États membres, cet aspect avait déjà été réglementé avant l'adoption de la directive «Vie privée et communications électroniques». Malgré la transposition, la diversité des traditions juridiques ayant cours dans l'Union européenne ont résulté en différentes définitions, conditions et modalités de protection de la confidentialité ainsi qu'en différentes exceptions applicables, par exemple concernant la surveillance des communications afin de garantir l'application des lois ou dans un contexte professionnel. Des problèmes potentiels ont également été relevés concernant le respect des droits accordés par la directive. Cela peut s'expliquer par le fait que différentes autorités sont responsables, dans différents États membres, de l'application de la directive «Vie privée et communications électroniques»[14]. Une telle situation peut parfois entraîner des incohérences et une incertitude dans l'application des règles existantes dans un seul et même pays.

Selon le rapport, l'article 5, paragraphe 3, concernant les **témoins de connexion**, les logiciels espions et les autres dispositifs ainsi que l'exigence d'obtenir **le consentement préalable des utilisateurs** «n'a pas entièrement atteint son objectif». La modification concernant les témoins de connexion introduite dans la révision de la directive en 2009 aurait, semble-t-il, résulté en une incertitude concernant son application sur le terrain. Il exigeait également une interprétation et des orientations de la part du groupe de travail «article 29»[15], par exemple au sujet de la configuration des réglages du navigateur et de la façon dont le consentement devrait être donné. De plus, une utilisation excessive des cookies de la part de nombreux sites internet semble avoir non seulement provoqué l'irritation des utilisateurs mais également réduit la portée informative de ces messages d'avertissement. En effet, les utilisateurs «bombardés» de cookies ne comprennent pas, ou ne prennent pas le temps de comprendre, la différence entre les types de situation, comme celle entre l'utilisation des témoins de connexion tiers et l'utilisation de témoins de connexion servant la finalité recherchée par l'utilisateur lorsqu'il navigue sur le site (témoins analytiques propriétaires).

Le rapport a constaté que l'article 6 de la directive (**données relatives au trafic**)[16] avait été correctement transposé dans la législation nationale. Toutefois, des questions demeuraient concernant son application.

[14] L'article 15 donne aux États membres la possibilité de choisir l'autorité nationale compétente ou les autorités nationales compétentes pour faire appliquer la directive 2002/58/CE.
[15] Cf. supra, note 6.
[16] C'est-à-dire «les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation». Cf. glossaire, annexe 14 de SWD(2017)3.

Des problèmes ont également été constatés au sujet des **données relatives à la localisation** (article 9)[17], en particulier dans la mesure où certains services de localisation comportant des risques concernant le respect de la vie privée ne sont pas couverts par la directive lorsqu'ils sont fournis sur un réseau *privé*. En effet, la directive couvre les services sur les réseaux *publics* du fait de son lien avec le cadre des communications électroniques et la définition des services de communications électroniques qu'il contient[18]. Enfin, concernant **les communications de marketing direct non sollicitées**, le rapport a conclu que les États membres avaient transposé avec succès l'article 13 de la directive, entraînant l'interdiction des systèmes automatisés d'appel et de communication à des fins de marketing direct sans consentement préalable. D'autres formes de marketing direct peuvent toujours recevoir un traitement différent au niveau national et il s'avère que certains pays ont choisi un régime de désistement pour ces cas, tandis que d'autres ont favorisé une démarche de choix actif dans leur législation.

Les conclusions du rapport ont amené une série de recommandations dans chacun des cinq domaines, telles que résumées dans le tableau 1 ci-dessous.

Tableau 1: Recommandations dans des domaines choisis

Domaine	Recommandation
Champ d'application	Modification de l'art. 3 pour le rendre applicable au traitement des données à caractère personnel «dans le cadre de la fourniture de services accessibles au public *sur des réseaux de communication publics ou privés accessibles au public* dans l'Union».
Confidentialité	Modification de l'art. 5, paragraphe 1, pour le rendre applicable «à la confidentialité des communications et à l'utilisation afférente des données relatives au trafic au moyen d'un *réseau de communication public ou privé accessible au public*»; clarification du champ d'application de l'art. 5, paragraphe 2, concernant «les exceptions dans le cadre des usages professionnels» afin de garantir une transposition et une application uniformes dans l'Union.
Témoins de connexion et dispositifs analogues	Reformulation des exceptions de l'art. 5, paragraphe 3, afin d'améliorer la clarté et d'insérer des exceptions supplémentaires; ajout d'exigences de «consentement spécifique, actif et préalable dans tous les cas où des témoins de connexion ou des dispositifs analogues sont utilisés à des fins de marketing direct».
Données relatives au trafic et à la localisation	Modifications mineures de l'art. 6, paragraphe 1, et de l'art. 9, paragraphe 1, pour garantir leur applicabilité à tous les services fournis au moyen de réseaux de communication publics ou privés accessibles au public, conformément à la modification suggérée pour l'art. 3 ci-dessus.
Communications de marketing direct non sollicitées	Alignement de l'art. 13 sur les modifications suggérées ci-dessus pour l'art. 3 de sorte que la règle de désistement disposée à l'art. 13 s'applique aux courriels transmis via des services de la société de l'information; maintien de la liberté de choix des États membres entre le désistement et le choix actif pour les messages de marketing direct.
Liens avec le RGPD	Transformation de la directive «Vie privée et communications électroniques» en un règlement.

Source: élaboré par l'auteure à partir de SMART 2013/0071, pp. 7-18.

Évaluation REFIT de la directive

Comme indiqué dans l'analyse d'impact initiale de la Commission annonçant la révision de la directive, les autres éléments qui ne sont pas couverts par le rapport ci-dessus ont été abordés dans une évaluation REFIT séparée[19]. Cette dernière a été menée en parallèle avec l'analyse d'impact et les deux documents ont été publiés avec la proposition le 10 janvier 2017.

[17] C'est-à-dire «toutes les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public»; SWD(2017)3, annexe 14.

[18] Cela peut également résulter en des situations ambiguës: le rapport cite par exemple le cas des réseaux Wi-Fi gratuits dans les aéroports. Doivent-ils être considérés comme publics ou privés?

[19] Commission européenne, SWD(2017)5. Il convient de noter que l'évaluation REFIT s'est basée, entre autres, sur deux autres études externes: Deloitte (2016), Evaluation and review of Directive 2002/58 on privacy and the electronic communications sector (SMART 2016/0080), et ECORYS, TNO et al. (2016), Study on future trends and business models in communication services, (SMART

Les éléments recueillis pour l'évaluation REFIT couvrent l'Union des 28 et la période 2009-2016[20]. Conformément aux lignes directrices pour une meilleure réglementation de la Commission, le rapport applique les cinq **critères d'évaluation** (efficience, efficacité, pertinence, cohérence et valeur ajoutée européenne) à cinq domaines principaux de la directive: 1) la sécurité des communications électroniques; 2) la confidentialité des communications et des données associées relatives au trafic; 3) la confidentialité des informations stockées dans les équipements terminaux; 4) la protection des utilisateurs contre les communications non sollicitées; et 5) les autres dispositions garantissant le respect de la vie privée des utilisateurs et la protection des intérêts légitimes des abonnés[21].

De plus, l'évaluation a abordé **deux questions horizontales** (le champ d'application de la directive et le choix des autorités compétentes) qui ont des conséquences directes sur son efficacité au vu des objectifs établis par le législateur. Sur ces deux points, l'évaluation REFIT a conclu que le fait que la directive se soit fondée sur la définition des services de communications électroniques a rendu son champ d'application **trop étroit ou obsolète**. De plus, le champ d'application actuel a été jugé ambigu et susceptible de provoquer une **incertitude juridique**. En définitive, cette situation a nui à l'efficacité de la législation. Certains problèmes découlaient également du fait que la directive ne désignait pas le droit national applicable, en particulier dans les situations transfrontalières, et de l'attribution des compétences d'exécution à différentes autorités entre les États membres, et souvent au sein de ceux-ci.

Au sujet des domaines couverts par les questions d'évaluation, il a été jugé que les exigences en matière de **sécurité des communications électroniques** (article 4) conservaient leur pertinence et constituaient une «condition préalable essentielle» pour remplir les objectifs de la directive, à la lumière notamment du nombre croissant d'incidents de sécurité affectant la vie privée des utilisateurs. Considérant que des dispositions analogues ont été insérées dans d'autres actes législatifs, comme le RGPD, l'évaluation a conclu que **certaines sections de la directive «Vie privée et communications électroniques» étaient devenues redondantes**. L'article 4 n'a, semble-t-il, été que partiellement efficace malgré les améliorations apportées par la révision de la directive en 2009. Pourtant, la formulation actuelle de l'article laisse planer quelques incertitudes, en particulier concernant le type de risques de sécurité couverts par l'obligation d'information des abonnés et concernant les possibles mesures d'atténuation à adopter dans de tels cas. Cela a entraîné des **variations dans le degré et dans les modalités de l'application** de cette exigence par les États membres de l'Union. Ce résultat n'a pu être attribué à l'échec de la transposition ou au caractère incomplet de celle-ci mais a plutôt été considéré comme un problème de clarté du texte.

Les autorités publiques ont également invoqué des **difficultés dans l'application de l'exigence de notification de violation des données**, une constatation qui semble être corroborée par le nombre relativement bas de violations rapportées dans les États membres signalé dans l'une des études justificatives[22]. En termes de cohérence, l'évaluation a noté que la récente adoption du RGPD et de ses dispositions sur les notifications de violation des données (articles 33 et 34) pouvait amener à deux démarches distinctes si la directive «Vie privée et communications électroniques» n'était pas modifiée. La démarche introduite par le RGPD semblant plus efficace, l'évaluation a conclu que seul l'article 4, paragraphe 2, de la directive «Vie privée et communications électroniques» demeurait pertinent, considérant qu'il n'était pas couvert par d'autres instruments législatifs. Ce chevauchement a également été remarqué dans l'évaluation de l'efficience de l'article 4, jugé comme l'une des dispositions les plus onéreuses

2013/0019). Les estimations quantitatives fournies par Deloitte (2016) sont disponibles dans l'analyse d'impact SWD(2017)3, annexe 8, accompagnant la nouvelle proposition.

[20] Comme indiqué, la dernière révision de la directive date de 2009. Lorsque celles-ci étaient disponibles et pertinentes, l'évaluation a également employé des données anciennes.

[21] SWD(2017)5, section 3 et p. 22.

[22] SWD(2017)5, pp. 27-28 concernant Deloitte (2016) p. 68.

de la directive. Enfin, si la valeur ajoutée européenne que représentent les dispositions concernant les violations des données à caractère personnel a été confirmée, en particulier dans les situations transfrontalières, l'évaluation a constaté une fois de plus que les dispositions pertinentes du RGPD seraient suffisantes.

Concernant la **confidentialité des communications et des données associées relatives au trafic** (article 5, paragraphe 1, article 6 et article 9), l'évaluation confirme la pertinence de ces dispositions qui n'apparaissent dans aucun autre acte législatif de l'Union. Cela est également confirmé par les conclusions de l'évaluation concernant la cohérence de ces dispositions avec le reste de l'*acquis communautaire*. Il est apparu toutefois que la directive **n'a pas été entièrement efficace dans la garantie de la confidentialité**. Ces résultats peuvent s'expliquer par différents facteurs comme certains problèmes de formulation et d'application de l'article 5, paragraphe 1, et le fait que certaines dispositions ont été dans une certaine mesure rendues obsolètes par l'évolution du secteur des communications électroniques. De plus, des divergences entre les différentes démarches nationales persistent concernant le traitement du contenu et des données relatives au trafic. En outre, le fait que la directive ne s'applique pas actuellement aux OTT a affaibli la protection qu'elle assure effectivement et a rendu «inéquitables» les conditions entre les acteurs du marché. Enfin, la possibilité offerte aux États membres de déroger à la directive pour des raisons de sécurité nationale a été exploitée différemment dans l'Union européenne, entraînant un certain degré de fragmentation.

Le manque de données quantitatives, un problème relevé tout au long de l'évaluation, n'a pas permis de tirer de conclusions définitives concernant l'efficience de ces articles. Les consommateurs et les représentants du secteur ont une vision différente de l'efficience, comme il sera expliqué dans la section 4 de cette note. L'évaluation **confirme la valeur ajoutée européenne** des dispositions concernant la confidentialité des communications et des données associées relatives au trafic, non seulement du fait de la dimension transfrontalière croissante des communications mais également grâce aux **avantages provenant de l'harmonisation des notions et des définitions** (les données relatives au trafic et à la localisation, par exemple) qu'a entraînée la directive.

L'évaluation soutient la pertinence des exigences de **confidentialité des informations stockées dans les équipements terminaux** (article 5, paragraphe 3), bien que la portée de l'article soit jugée excessive dans la mesure où il concerne également des pratiques qui ne portent pas atteinte à la vie privée. Sa valeur ajoutée européenne reste incontestée et sa cohérence avec le RGPD est également soulignée. En revanche, l'efficacité de la disposition est apparue amoindrie par plusieurs des raisons déjà mentionnées ailleurs dans cette note, c'est-à-dire un usage excessif des témoins de connexion entraînant une lassitude et un consentement automatique des utilisateurs, ainsi que le phénomène des *cookie-walls* (une proposition «à prendre ou à laisser» qui empêche les utilisateurs d'accéder à un site internet s'ils refusent ses cookies). De plus, comme dans le cas d'autres dispositions, les différences entre États membres dans la mise en œuvre et l'application ont eu un effet négatif sur son efficacité. Enfin, selon les estimations quantitatives, la mise en conformité avec les exigences de l'article 5, paragraphe 3, pourrait coûter environ 300 EUR par site internet et par an, pour un coût de mise en conformité cumulé dans toute l'Union estimé à 1,8 milliard d'EUR pour 2015[23]. L'évaluation précise que des méthodes plus efficaces d'application de la directive pourraient être trouvées.

Concernant la **protection contre les communications non sollicitées** (article 13), l'évaluation explique que le coût de ces pratiques a diminué au cours des derniers années, accroissant par là même l'ampleur potentielle du problème et confirmant la pertinence de la disposition. Toutefois, **l'opinion des parties intéressées varie concernant le type de protection que doit assurer la directive**. D'une part, les éléments factuels recueillis

[23] SWD(2017)5, p. 47.

indiquent une efficacité partielle de l'article 13, tel qu'en témoigne le nombre élevé d'appels importuns rapportés par les citoyens aux autorités compétentes de chaque pays. D'autre part, les représentants du secteur consultés dans le cadre de l'évaluation ainsi que les études indiquent des difficultés à la fois dans la compréhension et dans l'application des dispositions pertinentes. La fragmentation et l'incertitude juridique provoquées par les différentes modalités d'application des États membres sont ici à nouveau citées. L'évaluation de l'efficience en termes quantitatifs s'est avérée difficile. Il est important de noter toutefois que, du point de vue des entreprises, les coûts résultant de l'article 13 sont essentiellement des coûts d'opportunité provenant des pertes de marketing et de vente. La valeur ajoutée européenne de ces dispositions a été reconnue. Enfin, l'évaluation a constaté la complémentarité de l'article 13, du RGPD, de la directive 2000/31 sur le commerce numérique et de la directive 2011/83 relative aux droits du consommateur, indiquant ainsi une cohérence entre différents actes législatifs sur ce point.

Pour terminer, **d'autres dispositions**, telles que le droit de recevoir des factures non détaillées (article 7) et le droit de refuser l'inscription dans un annuaire (article 12), ont été jugées pertinentes par les citoyens et la société civile tandis que les professionnels adoptaient un point de vue opposé, appelant à leur abrogation ou à leur adaptation aux évolutions technologiques. L'évaluation a également constaté que, de façon générale, ces autres dispositions **avaient été efficaces au regard des objectifs visés et avaient apporté une valeur ajoutée européenne**. L'évaluation de l'efficience de telles exigences s'est avérée difficile du fait du manque de données quantitatives. L'évaluation est également arrivée à la conclusion qu'il existe une cohérence générale entre les dispositions en question et les autres domaines pertinents de l'*acquis communautaire*.

3. Position du Parlement européen/Questions parlementaires

3.1 Résolutions du Parlement européen

Résolution du Parlement européen du 19 janvier 2016 «Vers un acte sur le marché unique numérique»

Soulignant la nécessité de respecter les droits fondamentaux, et en particulier la législation en matière de protection des données, le Parlement européen a demandé que la révision de la directive 2002/58/CE «assure la cohérence des dispositions avec le paquet législatif relatif à la protection des données lors de l'entrée en vigueur de ce dernier» (mai 2018). Il a également rappelé que les révélations sur la surveillance électronique de masse ont érodé la confiance des citoyens dans les services numériques et le respect effectif de leur vie privée, soulignant une fois de plus la nécessité de «respecter scrupuleusement la législation en vigueur en matière de protection des données [...] lorsque des données à caractère personnel sont traitées à des fins commerciales ou répressives». Le Parlement a rappelé que la confiance des citoyens et des entreprises dans l'environnement numérique était essentielle pour l'innovation et la croissance futures et pour l'établissement d'un marché unique numérique compétitif.

Dans le suivi de la résolution, la Commission européenne a confirmé qu'elle avait déjà lancé la procédure de réexamen de la directive «Vie privée et communications électroniques». Elle a aussi précisé son intention initiale d'adopter une proposition avant la fin de l'année 2016. En termes de contenu, la Commission a déclaré qu'elle tiendrait également compte de l'importance du chiffrement comme moyen de protection de la vie privée des utilisateurs et de la sécurité des communications électroniques, tel que souligné dans la résolution du Parlement.

3.2 Questions écrites des députés au Parlement européen

Question écrite de Morten Messerschmidt (ECR, Danemark), 15 avril 2016 (en anglais)

Au sujet de l'article 5, paragraphe 3, de la directive «Vie privée et communications électroniques» concernant le consentement préalable en connaissance de cause pour le stockage d'informations ou l'accès à des informations stockées dans l'équipement terminal d'un utilisateur, le député relevait que l'heure était

venue d'évaluer si la législation avait atteint ses objectifs et si elle était proportionnée en termes de contraintes à l'égard des utilisateurs. D'une part, les utilisateurs étaient irrités par les demandes constantes d'autorisation des témoins de connexion; d'autre part, l'agrément était souvent donné sans une connaissance complète des conséquences et il n'améliorait donc pas la sécurité. Il désirait donc savoir si la Commission européenne était prête à supprimer cette disposition spécifique qui semblait créer davantage de contraintes qu'elle ne procurait de bénéfices.

Réponse de Günther Oettinger au nom de la Commission, 14 juin 2016 (en anglais)

Le commissaire a rappelé que le consentement n'était pas nécessaire à «un stockage ou à un accès techniques visant exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur». Il a également observé qu'il était souvent possible de ne donner son consentement qu'une seule fois pour un site internet donné ou de fixer un comportement général dans les réglages du navigateur. Toutefois, il a également rappelé que le groupe de travail «article 29» avait constaté que de nombreux sites internet utilisaient toujours des cookies inutiles visant fréquemment principalement le pistage des utilisateurs et le profilage de leurs existences et de leurs habitudes. Il a indiqué que ces questions étaient abordées dans la consultation publique et l'évaluation sous-tendant une révision de la directive 2002/58/CE.

Question écrite de Santiago Fisas Ayxelà (PPE, Espagne), 27 avril 2016 (en anglais)

Les sites internet barrent de plus en plus l'accès à leur contenu aux utilisateurs ayant installé un bloqueur de fenêtres contextuelles sur leur ordinateur. Le député relevait que les mécanismes actuels barrant l'accès au contenu d'une telle façon pouvaient être contraires à l'article 5, paragraphe 3, de la directive «Vie privée et communications électroniques» dans la mesure où ils n'exigeaient pas le consentement exprès des utilisateurs[24]. Il désirait donc savoir comment la Commission prévoyait de protéger la vie privée des utilisateurs lorsque ces pratiques étaient utilisées et s'enquérait de la possibilité de trouver un équilibre entre la protection des utilisateurs et la «viabilité des sites internet du point de vue de la publicité».

Réponse de Günther Oettinger au nom de la Commission, 8 juillet 2016 (en anglais)

Le commissaire a expliqué que la technologie utilisée par les sites internet pour détecter la présence de bloqueurs de fenêtres contextuelles déterminait si l'article 5, paragraphe 3, de la directive 2002/58/CE s'appliquait à une situation donnée. Il a également rappelé que le contrôle et l'application de la législation existante relevaient des autorités de surveillance et des tribunaux des États membres, y compris la question de savoir si la disposition de la directive s'appliquait aux dispositifs de détection des bloqueurs de fenêtres contextuelles utilisés par les sites internet. Il a également indiqué que le règlement général sur la protection des données récemment adopté devait renforcer encore la confiance des utilisateurs dans les services numériques. Enfin, il a observé que l'efficience et l'efficacité de la directive «Vie privée et communications électroniques», y compris ses coûts et ses avantages, étaient en cours d'évaluation.

Question écrite de Kathleen Van Brempt (S&D, Belgique), 13 avril 2015 (en anglais)

Un rapport commandé par la commission belge de la protection de la vie privée a constaté que Facebook enregistrait l'usage d'internet des personnes qui n'utilisaient pas ses services et ne visitaient même pas le site de ce média social. Cette pratique était mise en œuvre sans qu'elles en aient connaissance ou sans leur consentement. La députée désirait donc savoir si la Commission européenne avait connaissance de «l'utilisation de témoins de connexion d'identification à long terme pour pister les utilisateurs non inscrits» et si celle-ci enfreignait la directive «Vie privée et communications électroniques». La députée demandait

[24] Veuillez noter que des préoccupations concernant l'obligation d'accepter les témoins de connexion pour accéder à un site internet, et plus largement concernant l'accès aux informations à caractère personnel (y compris les informations relatives au trafic et à la localisation), avaient également été exprimées dans certaines des questions reçues par l'unité «Demandes d'informations des citoyens» du Parlement européen (AskEP) au cours des deux dernières années.

également quelles actions prévoyait la Commission afin de lutter contre le pistage illégal des utilisateurs et garantir que les utilisateurs d'internet aient connaissance du pistage par des tiers.

Réponse de Günther Oettinger au nom de la Commission, 7 juillet 2015 (en anglais)

Le commissaire a confirmé que la Commission avait connaissance de la pratique mentionnée par la députée et a rappelé que l'utilisation des témoins de connexion pour pister les utilisateurs devait se conformer aux mesures nationales d'application de la directive «Vie privée et communications électroniques » et en particulier à l'article 5, paragraphe 3, révisé en 2009, concernant le consentement informé des utilisateurs. Il a également rappelé que l'application de ces dispositions relevait de la compétence des États membres. Les autorités nationales compétentes, fortes de leurs pouvoirs d'enquête, sont donc les interlocuteurs appropriés auxquels les utilisateurs concernés doivent faire part de leurs préoccupations. Il a enfin noté que la Commission soutenait les efforts du secteur visant à améliorer la connaissance qu'avaient les utilisateurs de leurs droits au titre de la directive 2002/58/CE au moyen de systèmes d'interdit de suivi (DNT, *Do Not Track*) ou par l'utilisation de boîtes de dialogue fournissant des informations concernant les témoins de connexion et de divers dispositifs visant à obtenir le consentement.

4. Consultations publiques organisées par la Commission européenne

Enquête Eurobaromètre concernant la vie privée et les communications électroniques

À la demande de la Commission européenne, près de 27 000 citoyens de l'Union ont été contactés durant l'été 2016 pour une enquête concernant la protection de leur vie privée[25]. Les questions de l'enquête traitaient des sujets suivants: l'utilisation faite par les citoyens des technologies de communication; l'importance qu'ils accordaient à la protection de la vie privée en ligne et à la confidentialité de leurs communications; le type de précautions prises par les citoyens pour protéger leur vie privée en ligne; leur connaissance de la législation en vigueur; et leur attitude vis-à-vis des communications non sollicitées par courriel ou par des appels de marketing.

Cette enquête a montré que, quotidiennement ou presque quotidiennement, plus de 70 % des citoyens interrogés utilisaient leur téléphone portable pour passer des appels ou envoyer des SMS, que 60 % d'entre eux naviguaient sur internet et que 46 % d'entre eux utilisaient des courriels. L'utilisation d'une messagerie instantanée par internet à fréquence hebdomadaire était rapportée par la moitié des répondants. Seulement 8 % d'entre eux ont déclaré utiliser quotidiennement internet pour passer des appels téléphoniques et vidéo[26].

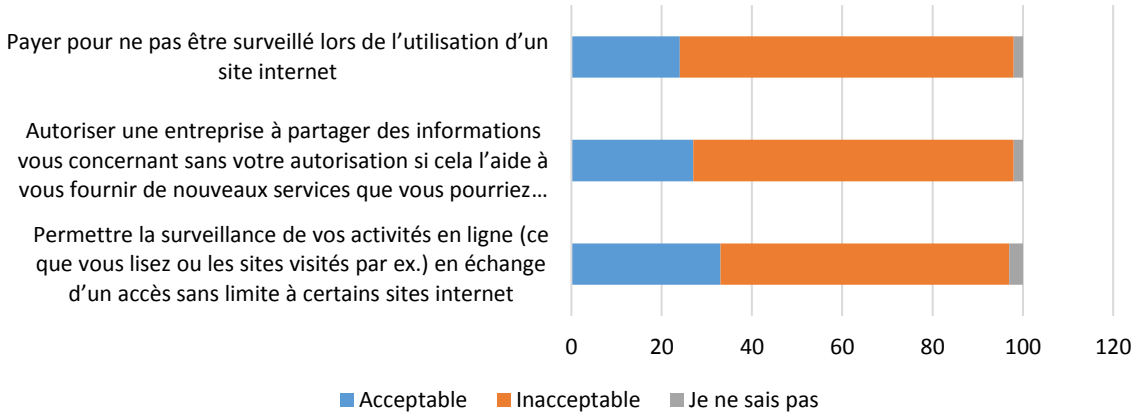
En ce qui concerne la connaissance des citoyens de la législation en vigueur au sujet de la vie privée et des communications électroniques, la majorité d'entre eux (67 %) semblaient savoir que les informations à caractère personnel, telles que les photographies et l'historique des appels, stockées sur leur appareil ne pouvaient être consultées qu'avec leur consentement et 58 % des répondants avaient également connaissance des règles concernant le stockage sans autorisation des informations (telles que les témoins de connexion) sur leur appareil. Il est intéressant de constater que la sensibilisation sur ce second point montrait des niveaux plus variables entre les États membres que sur la question précédente. À l'inverse, seules 37 % des personnes interrogées savaient que la messagerie instantanée et les conversations orales en ligne n'étaient pas systématiquement confidentielles et jusqu'à 58 % d'entre elles croyaient à tort que personne ne pouvait avoir accès à ces communications sans leur permission. Si les réponses fournies à cette question montraient des différences géographiques de sensibilisation, les facteurs sociodémographiques ne semblaient pas avoir une influence sur le niveau de connaissance des répondants.

[25] Enquête Eurobaromètre Flash 443, juillet 2016.

[26] Pour une ventilation des réponses à l'enquête par États membres, par catégories d'âge et par niveaux d'éducation, et pour des données concernant l'utilisation des réseaux sociaux, des lignes de téléphonie fixe, etc., voyez Eurobaromètre 443, pp. 8-21.

Les résultats de l'enquête montraient également un large soutien à la confidentialité des informations à caractère personnel, des courriels et des messages instantanés et indiquaient que 65 % des répondants prenaient activement des précautions pour renforcer la protection de leur vie privée, par exemple en modifiant les réglages de protection de la vie privée sur leurs appareils ou en évitant certains sites internet de façon à ne pas être surveillés[27]. Ces précautions actives étaient plus répandues parmi les répondants âgés de 15 à 39 ans et parmi les personnes d'un niveau d'éducation élevé. Presque 70 % des personnes interrogées soutenaient entièrement l'opinion selon laquelle les réglages par défaut des navigateurs «devraient empêcher [...] le partage des informations» et 65 % d'entre elles étaient entièrement favorables au chiffrement des appels et des messages de sorte que les communications ne soient accessibles qu'aux récipiendaires prévus. Les opinions étaient variables concernant les préférences en matière de fréquence des demandes d'accès aux informations des utilisateurs de la part des sites internet. Enfin, 60 % des répondants estimaient recevoir un nombre trop élevé d'appels commerciaux non sollicités et soutenaient la proposition selon laquelle ce type d'appels devrait toujours afficher un préfixe spécifique. Le soutien à cette proposition était proportionnel au niveau d'éducation des répondants. Cette enquête demandait également l'opinion des répondants concernant l'acceptabilité d'une série de scénarios, comme illustré dans la figure ci-dessous. Le soutien aux deux dernières options variait entre les États membres et était inversement proportionnel à l'âge des répondants.

Figure 1: Dans quelle mesure considérez-vous chacune des propositions suivantes comme acceptable (% UE)?



Source: élaboré par l'auteure à partir de l'enquête Eurobaromètre Flash 443 (juillet 2016), p. 55.

Consultation publique ouverte

La Commission européenne a tenu, entre avril et juillet 2016, une consultation publique ouverte abordant à la fois l'évaluation et le réexamen prévu de la directive «Vie privée et communications électroniques»[28].

La première partie du **questionnaire de consultation** concernait l'évaluation de la directive et posait des questions relatives à son efficacité au regard de ses trois principaux objectifs, les problèmes potentiels de compréhension et d'application de dispositions spécifiques et l'incidence estimée de l'attribution de la compétence au sujet de la directive à différentes autorités au sein des États membres. Le questionnaire

[27] Dans tous les États membres, seule une minorité de répondants a rapporté l'utilisation de logiciels spécifiques pour prévenir l'affichage des publicités en ligne ou le pistage de leurs activités en ligne, Eurobaromètre 443, pp. 39-40.

[28] En parallèle, la Commission a conduit des activités consultatives supplémentaires par l'intermédiaire de la plateforme REFIT, du groupe de travail «article 29», du réseau de coopération pour la protection des consommateurs et de deux ateliers avec les parties intéressées. Les résultats de ces activités sont rapportés dans le document SWD(2017)3, annexe 3.

abordait également la pertinence de la directive, en particulier concernant le caractère opportun d'un ensemble spécifique de règles concernant la vie privée et les communications électroniques en plus de celles contenues dans d'autres actes législatifs. Il examinait également la cohérence avec d'autres articles spécifiques d'autres actes de l'Union et la valeur ajoutée européenne de la directive. Comme la section précédente concernant l'évaluation REFIT l'a exposé, cette consultation visait également à recueillir des éléments qualitatifs et quantitatifs concernant les coûts et les avantages de la directive afin d'évaluer son efficience. La seconde moitié du questionnaire se tournait davantage vers l'avenir, s'enquérant des priorités que devait établir tout instrument futur abordant les questions de protection de la vie privée et des données dans les communications électroniques, ainsi que de la nécessité de remplacer la directive par un règlement et d'en élargir le champ d'application. Elle s'intéressait également à l'opinion des parties intéressées concernant: différentes perspectives de renforcement de la sécurité et de la confidentialité des communications et d'amélioration de l'expérience des utilisateurs grâce aux témoins de connexion; les exemptions existantes au consentement pour le traitement des données relatives au trafic et à la localisation; et le régime de choix actif, par opposition à celui du désistement, vis-à-vis des communications de marketing non sollicitées. Elle se conclut par une série de questions concernant la fragmentation et le manque de cohérence dans l'application.

La consultation a reçu **421 réponses** provenant de différentes catégories de parties intéressées comme les citoyens (39 %), les représentants du secteur (44 %), les autorités publiques (10 %) et les associations de la société civile et de consommateurs (8 %). Sur le plan de la distribution géographique, 26 % des réponses provenaient d'Allemagne, 14 % du Royaume-Uni, 10 % de Belgique et 7 % de France. Les réponses reçues[29]peuvent être approximativement réparties en trois groupes (citoyens, organisations de consommateurs et de la société civile; professionnels du secteur; et autorités publiques)[30] adoptant des vues relativement contradictoires sur les principaux thèmes de la consultation. Il convient d'ajouter toutefois que **ces catégories ne sont pas aussi uniformes qu'elles le paraissent au premier abord**: ainsi, les parties intéressées du secteur incluent à la fois les opérateurs traditionnels de télécommunication et les OTT qui ont des positions différentes sur des éléments clés de la directive, comme son champ d'application.

Considérant que de nombreuses conclusions de la consultation ont alimenté directement l'évaluation REFIT mentionnée ci-dessus, cette section se concentrera exclusivement sur un ensemble de questions choisies abordées par la consultation. En ce qui concerne tout d'abord les **cinq critères examinés par l'évaluation**, la vaste majorité des citoyens et des organisations de consommateurs et de la société civile n'ont pas jugé la version actuelle de la directive apte à garantir efficacement une protection complète de la vie privée et de la confidentialité des communications. Ils citent la limitation du champ d'application et l'absence de véritable choix concernant les témoins de connexion comme quelques-unes des raisons les ayant conduits à cette conclusion. Du côté des professionnels du secteur, les acteurs des services de communications électroniques ont pris le parti des citoyens sur ce point tandis que 57 % des répondants du secteur jugeaient la directive efficace. Les autorités publiques avaient elles aussi des opinions semblables et globalement favorables.

Les citoyens et les représentants de la société civile ont largement confirmé la pertinence de règles spécifiques dans le secteur des communications électroniques pour atteindre les objectifs de protection de la vie privée et de confidentialité. Les autorités publiques ont également adopté cette position à 90 %. À l'inverse, les répondants du secteur ne voyaient pas d'avantage à disposer d'une réglementation spécifique au secteur, considérant que de nombreuses exigences de la directive «Vie privée et communications

[29] Toutes les contributions, classées par type de répondants, sont disponibles ici.
[30] Cette classification a également été adoptée par la Commission européenne dans son rapport complet concernant la consultation.

électroniques» pouvaient être reprises dans le RGPD ou d'autres cadres législatifs[31]. Les réactions des citoyens et de la société civile étaient relativement limitées concernant la cohérence de la directive vis-à-vis d'autres instruments législatifs. Les professionnels ont en revanche rapporté un niveau plus élevé de cohérence entre la directive «Vie privée et communications électroniques», le RGPD, la directive-cadre sur les communications électroniques et la directive sur la sécurité des réseaux et des systèmes d'information (directive SRI). Les réactions des autorités publiques vont également dans ce sens. Comme mentionné ci-dessus, l'obtention d'informations qualitatives permettant d'évaluer l'efficience de la directive s'est avérée difficile. Si, d'une part, de nombreux répondants du secteur ont indiqué que les coûts de mise en conformité générés par la directive étaient significatifs (62 %) ou modérés (21 %) et généralement disproportionnés, les citoyens et les représentants des consommateurs et de la société civile (57 %) les jugeaient proportionnés à leurs objectifs, tout comme les autorités publiques (73 %). Néanmoins, les citoyens et les acteurs du secteur se sont, de façon générale, entendus pour considérer que la directive et les dispositions d'application nationales avaient échoué à renforcer la confiance des utilisateurs. Les autorités publiques ont adopté une attitude légèrement plus positive sur ce point. Enfin, presque 87 % des citoyens et des représentants des consommateurs et de la société civile ont confirmé la valeur ajoutée européenne apportée par la directive. Les autorités publiques avaient à 65 % la même opinion tandis que 50 % des représentants du secteur, avec un pic à 60 % parmi les acteurs des communications électroniques, contestaient cette affirmation.

Concernant la **révision prochaine de la directive**, les parties intéressées affichaient à nouveau des opinions contrastées. Si une analyse détaillée sort du cadre de cette note d'information, la comparaison (cf. tableau 2 ci-dessous) du classement par les trois catégories de répondants des différentes options de réexamen du texte actuel est assez édifiante et mérite d'être mentionnée. Le pourcentage de répondants préférant chacune des options est indiqué entre parenthèses[32].

Concernant la forme future de l'instrument révisé, le remplacement de la directive actuelle par un règlement était soutenu par 66 % des citoyens et des organisations de consommateurs et de la société civile et par 67 % des autorités publiques ayant répondu à la consultation. Les représentants du secteur étaient davantage favorables à d'autres options, comme l'abrogation de la directive 2002/58/CE ou le recours à d'autres actes législatifs comme le RGPD.

Enfin, la **rationalisation de la structure de gouvernance existante** et l'attribution de la responsabilité de l'application de la directive à une entité unique, avec une préférence pour les autorités nationales chargées de la protection des données, faisaient l'objet d'un large consensus entre les citoyens, la société civile et les professionnels. Seules 39 % des autorités publiques étaient favorables à cette option tandis que 50 % y étaient opposées[33].

[31] Il convient de noter que certains répondants du secteur estimaient toutefois que certaines règles spécifiques restaient nécessaires concernant le marketing direct et les annuaires. Rapport de consultation complet, p. 5.

[32] Une analyse plus détaillée des différentes positions résumées ici est disponible aux pages 9 à 18 du rapport complet de consultation.

[33] Il convient de noter que ces réponses cachent des disparités quant aux motifs du soutien apporté à une certaine option et que 21 % de l'ensemble des répondants étaient en faveur d'autres options qui ne sont pas présentées ci-dessus. L'abrogation de la directive figurait parmi celles-ci. D'autres répondants ont déclaré craindre que le fait de confier l'application aux autorités chargées de la protection des données ne fasse en sorte que moins d'attention soit accordée aux valeurs autres que celles du respect de la vie privée.

Tableau 2: Classement des priorités pour la révision par groupes principaux de répondants

Citoyens, consommateurs et société civile	Professionnels du secteur	Autorités publiques
Modification des règles de confidentialité des communications et des équipements terminaux (69 %)	Dispositions désormais inutiles (56 %)	Élargissement du champ d'application aux OTT (72 %)
Élargissement du champ d'application aux OTT (63 %)	Élargissement du champ d'application aux OTT (29 %)	Modification des règles concernant les communications commerciales non sollicitées (59 %)
Modification des règles concernant la gouvernance (62 %)	Modification des règles concernant les communications commerciales non sollicitées (23 %)	Modification des règles concernant la confidentialité (52 %)
Modification des règles concernant les communications commerciales non sollicitées (58 %)	Modification des règles concernant la gouvernance (23 %)	Modification des règles concernant la sécurité (41 %)
Modification des règles concernant la sécurité (56 %)	Modification des règles de confidentialité des communications et des équipements terminaux (20 %)	Modification des règles concernant la gouvernance (41 %)
Dispositions désormais inutiles (4 %)	Modification des règles concernant la sécurité (17 %)	Autres options (7 %)

Source: élaboré par l'auteure à partir du rapport de consultation, p. 9

5. Comité économique et social européen

Une étude entreprise, et récemment achevée, par le Comité économique et social européen au sujet de l'éthique des mégadonnées[34]a abordé la question délicate de la façon dont peut être atteint un équilibre entre les droits fondamentaux, comme le respect de la vie privée et la confidentialité, et les possibilités économiques croissantes offertes par les mégadonnées. Cette étude a mené à la définition de **cinq actions d'équilibrage** qui pourraient être transposées dans les politiques. Si les actions recommandées sont étroitement associées au RGPD, les actions 1, 2 et 5 pourraient avoir des conséquences substantielles dans les domaines actuellement couverts par la directive «Vie privée et communications électroniques».

Plus particulièrement, la première action définie consiste en la création d'une plateforme européenne de gestion de la protection de la vie privée: un portail central ou une base de données de référence pour l'ensemble de l'Union permettant aux personnes physiques de contrôler la façon dont leurs données à caractère personnel sont utilisées. La deuxième action envisageait l'établissement d'un protocole de gestion éthique des données sous la forme d'un système de certification européen permettant d'identifier les acteurs vertueux sur le marché dans le domaine de la protection des données. La cinquième action concernait l'éducation dans le domaine numérique afin de favoriser l'approfondissement de la compréhension des mégadonnées et de leurs conséquences pour l'individu. L'ensemble de ces cinq actions ont fait l'objet d'une consultation des parties intéressées, notamment pour examiner les possibilités de leur mise en pratique. Si certaines suggestions, comme la création d'un portail central ou d'une base de données de référence, ont été jugées prématurées ou inappropriées dans le contexte actuel, les actions d'investissement dans l'éducation et dans la sensibilisation et de développement d'un système de certification européen pour les entreprises ont reçu le soutien de différentes parties intéressées.

[34] Evodevo srl (2017), L'éthique des mégadonnées: équilibrer les avantages économiques et les questions d'éthique liées aux données massives dans le contexte des politiques européennes, étude pour le CESE. Cette étude sera publiée au début du mois de février sur le site internet du Comité.

6. Conclusions

Le paysage technologique, économique et social a sensiblement changé depuis l'adoption de la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques. Malgré les modifications ciblées adoptées en 2009, le texte actuel de la directive ne reflète pas entièrement les évolutions récentes du secteur et des habitudes des consommateurs. L'entrée sur le marché de nouveaux types d'acteurs et la généralisation de l'usage de services par internet, comme la messagerie instantanée, ayant des effets potentiels sur l'efficacité des règles existantes en matière de protection de la vie privée dans les communications électroniques, font partie des évolutions les plus notables à cet égard. De plus, l'adoption du règlement général sur la protection des données en 2016 a modifié le cadre législatif de la protection des données, remettant potentiellement en question la pertinence et le maintien de la cohérence de la directive «Vie privée et communications électroniques» vis-à-vis de la nouvelle législation.

Les éléments rassemblés pour évaluer l'efficacité, l'efficience, la cohérence, la pertinence et la valeur ajoutée européenne de la directive 2002/58/CE, ainsi que les réactions recueillies par la Commission européenne au moyen d'ateliers ciblés, d'une consultation publique en ligne et d'une enquête Eurobaromètre, ont confirmé l'existence de différents problèmes. Ceux-ci ont également été abordés lors d'une conférence spéciale organisée par le Parlement européen en 2015[35]. En particulier, certaines des principales dispositions de la directive n'ont pas été suffisamment efficaces pour garantir les niveaux de confidentialité et de protection visés par le législateur. C'est le cas de l'article 5, paragraphe 3, par exemple, concernant les témoins de connexion et les autres dispositifs permettant de stocker des informations et d'y accéder sur l'équipement des utilisateurs, une question également soulevée à diverses occasions par les députés au Parlement européen. De plus, il apparaît que certaines sections de la directive 2002/58/CE sont désormais technologiquement obsolètes et que des logiques juridiques plus appropriées ont été adoptées depuis. Enfin, l'analyse de l'application des règles européennes de protection de la vie privée dans les communications électroniques dans les États membres a mis au jour différents degrés de fragmentation juridique, la coexistence de différents niveaux de protection dans l'Union européenne et une structure de gouvernance complexe avec une attribution des responsabilités d'application à différents types d'autorités, parfois même au sein du même pays. De façon générale, cela a contribué à un manque de sécurité juridique et de clarté, ainsi qu'à l'existence de conditions inéquitables en Europe. D'autre part, la valeur ajoutée européenne et la pertinence générale de dispositions spécifiques protégeant la vie privée et garantissant l'application pratique de l'article 7 de la charte des droits fondamentaux de l'Union européenne ont été confirmées à de multiples reprises. En effet, la modernisation de la réglementation actuelle constitue un élément central de la stratégie de l'Union pour un marché unique numérique, modernisation qui devrait permettre de rétablir et de renforcer la confiance des citoyens et des entreprises dans l'environnement numérique.

Le 10 janvier 2017, la Commission européenne a adopté une proposition visant à abroger la directive 2002/58/CE et à la remplacer par un règlement afin de résoudre plusieurs des problèmes soulignés ci-dessus, de simplifier la réglementation existante et de l'ouvrir aux évolutions futures. Les colégislateurs vont désormais avoir la tâche de trouver un équilibre entre les différentes positions contraires et les attentes qui ont émergé tout au long du processus menant au réexamen de la directive.

[35] Protecting online privacy by enhancing IT security and strengthening EU IT capabilities, conférence de haut niveau coorganisée par la commission LIBE du Parlement européen et par le panel STOA en collaboration avec la présidence luxembourgeoise, 8 décembre 2015.

7. Autres sources de référence

Carey, P. (2015), Data protection: a practical guide to UK and EU law, Oxford University Press.

Davies, R., Regulating electronic communications: A level playing field for telecoms and OTTs?, note d'information, EPRS, 31 août 2015.

Leith, P. (2015), Privacy in the Information Society – The library of essays on law and privacy, volume II, Aldershot, Ashgate Publishing Group.

Luzak, J. (2013), «Much Ado about Cookies: The European Debate on the New Provisions of the ePrivacy Directive regarding Cookies», European Review of Private Law, vol. 21, nº 1, pp. 221–245.

Plateforme REFIT, Avis sur la contribution du forum économique danois concernant la directive «Vie privée et communications électroniques» et la réglementation actuelle relative aux témoins de connexion, 27 et 28 juin 2016.

Pour contacter l'unité Cycle politique, veuillez envoyer un courrier électronique à l'adresse suivante: EPRS-PolicyCycle@ep.europa.eu

Manuscrit achevé en janvier 2017. Bruxelles, © Union européenne, 2017.

www.europarl.europa.eu/thinktank (internet)– www.epthinktank.eu (blog) – www.eprs.sso.ep.parl.union.eu (intranet)