QUESTIONNAIRE CONCERNANT LA CONSULTATION PUBLIQUE SUR L'ÉVALUATION ET LA RÉVISION DE LA DIRECTIVE «VIE PRIVÉE ET COMMUNICATIONS ÉLECTRONIQUES»

Réponses La Quadrature Du Net

I.1. EFFICACITÉ DE LA DIRECTIVE «VIE PRIVÉE ET COMMUNICATIONS ÉLECTRONIQUES»

Question 1 : en vous appuyant sur votre expérience, pensez-vous que la directive a atteint ses objectifs, notamment en ce qui concerne les aspects suivants:

Dans une large mesure / dans une certaine mesure / dans une faible mesure / pas du tout / je ne sais pas

- Protection totale de la vie privée et de la confidentialité des communications dans l'UE : **dans une faible mesure**
- Libre circulation des données à caractère personnel traitées dans le cadre de la fourniture de services de communications électroniques : **dans une certaine mesure**
- Libre circulation des équipements et services de communications électroniques dans l'UE : **dans une large mesure**

Question 1 A : Veuillez préciser votre réponse.

La directive 2002/58/CE a certes apporté des améliorations en matière de protection de la vie privée et des données à caractère personnel mais elle n'a pas atteint ses objectifs car elle comporte encore de nombreuses lacunes. Tout d'abord son champ d'application est trop restreint car elle ne s'applique pas aux fournisseurs de services par contournement (OTT). Comme nous l'expliquons dans nos compléments de réponse à la question 33, ces services devraient être soumis aux mêmes obligations (sécurité, confidentialité, consentement, communications commerciales non sollicitées etc.) mais tout cela sans être qualifiés "d'opérateurs" car nous leur reconnaissons des caractéristiques intrinsèques.

Par ailleurs la directive laisse aux États membres la possibilité de choisir entre consentement préalable et droit d'opposition dans le cas d'appels téléphoniques à des fins de prospection directe visant des particuliers. Au delà d'être un problème pour l'harmonisation du marché numérique au sein de l'UE, un système basé sur le droit d'opposition ne garantit pas un respect du droit à la vie privée et à la protection des données tel que garantit par la Charte des droits fondamentaux de l'UE.

Enfin l'article 15 de la directive est trop large et n'encadre pas assez les possibilités de dérogations pour les États membres. Cela peut conduire à des dérives dans les dispositions nationales de transposition comme c'est le cas en France avec l'article 34-1 III du CPCE (voir réponse 10).

****

Question 2 : en tant que prestataire ou particulier, avez-vous eu des difficultés à appliquer ou à comprendre les règles, notamment en ce qui concerne les aspects suivants:

Notification des violations de données à caractère personnel : **oui**

Confidentialité des communications électroniques: **oui**

Règles spécifiques concernant les données de trafic et de localisation : **oui**

Communications commerciales non sollicitées, envoyées et reçues *via* internet : **oui**

Factures détaillées : **oui**

Présentation et restriction des lignes appelante et connectée : **oui**

Renvoi d'appel automatique : **oui**

Annuaires d'abonnés : **oui**

Question 2 A : Si avez répondu «Oui», veuillez préciser votre réponse.

Oui nous avons eu des difficultés à comprendre ces règles. C'est un vrai casse tête juridique: il y a d'importantes ambiguïtés sur le champ d'application, il est difficile de déterminer quels types de services sont concernés par cette directive. Par ailleurs il est difficile de savoir à qui s'adresser pour avoir des explications car on ne sait jamais qui est l'autorité ou qui sont les autorités compétentes dans notre État membre, cela rend la notification de violations d'autant plus complexe. Le fait que les États membres puissent choisir la disposition à mettre en place (consentement préalable ou droit d'opposition) concernant la prospection non-sollicitée rend encore moins effective les règles découlant de cette directive, qui ne sont pas harmonisées, ces règles sont d'autant moins intelligibles qu'il est difficile de détemriner le régime applicable à une situation donnée.
Enfin selon le contexte, certaines données peuvent être à la fois des données de trafic et des données de localisation. Il est nécessaire d'apporter des clarifications sur le type de régime qui s'applique tout en assurant une protection maximale dans chaque cas.

****

Question 3 : actuellement, ce sont les États membres qui doivent mettre en place les organismes nationaux chargés de faire appliquer la directive «vie privée et communications électroniques». L'article 15 bis de la directive fait référence à l'«autorité nationale compétente» et, le cas échéant, à «d'autres organismes nationaux», tels que les entités chargées de pouvoirs de surveillance et d'exécution des dispositions nationales mettant en œuvre la directive «vie privée et communications électroniques».

En vous appuyant sur votre expérience, est-ce que le fait que certains États membres aient attribué des compétences d'exécution à différentes autorités a entraîné:

- des divergences d'interprétation des règles dans l'UE? **Dans une large mesure**
- une application inefficace de la directive? **Dans une certaine mesure**

Question 4 : si vous avez répondu «dans une large mesure» ou «dans une certaine mesure», cette situation constitue-t-elle une source de confusion pour:

Oui / non / sans avis

- les fournisseurs de services de communications électroniques, les services de la société de l'information et les responsables du traitement des données en général? **Oui**
- les citoyens? **Oui**
- les autorités compétentes? **Oui**

Question 4 A : Veuillez préciser votre réponse.

Cette situation est une source de confusion pour tous les acteurs mentionnés. Les fournisseurs de services sont soumis à de nombreuses obligations et il est difficile de trouver l'information afin de rendre leurs activités conformes à la législation du fait de la multiplicité des autorités compétences et donc des sources. Il est normal dans ce cas de s'informer auprès de l'autorité de contrôle compétente. Mais quand deux voire trois autorités différentes sont compétentes et se partagent les missions de façon opaque, le fournisseur de service concerné ne sait pas vers qui se tourner. Pour les individus, c'est exactement la même chose : lorsqu'ils sont à la recherche d'informations ou souhaitent notifier une atteinte à leurs droits, cela peut-être très décourageant de ne pas savoir à qui s'adresser (dans le cas de la France doit-on s'adresser à la CNIL ou à l'ARCEP).
Enfin, pour les autorités compétentes, c'est également une réelle source de confusion dans la mesure où le partage des missions n'est pas toujours suffisamment clair et précis. Ainsi personne ne bouge. Le cas de la protection de la confidentialité en est un bon exemple. Aucune autorité ne s'est estimée compétente pour assurer la protection de ce principe fondamental.

****

I.2. PERTINENCE DE LA DIRECTIVE «VIE PRIVÉE ET COMMUNICATIONS ÉLECTRONIQUES»

- Question 5 : selon, vous, faut-il adopter des règles spécifiques au niveau de l'UE pour atteindre les objectifs suivants ?

oui /non /sans avis

- Niveau équivalent de protection (protection totale) dans l'ensemble de l'UE : **oui**
- Libre circulation des données à caractère personnel traitées dans le cadre de la fourniture de services de communications électroniques : **oui**
- Libre circulation des équipements et services de communications électroniques dans l'UE) : **oui**

- Question 6 : le fait de disposer de règles spécifiques dans les domaines ci-après apporte-t-il une valeur ajoutée? oui / non

oui /non /sans avis

- Notification des violations de données à caractère personnel : **oui**
- Confidentialité des communications électroniques : **oui**
- Données de trafic et de localisation : **oui**
- Communications commerciales non sollicitées, envoyées et reçues *via* internet : **oui**
- Factures détaillées : **oui**
- Présentation et restriction des lignes appelante et connectée : **oui**
- Renvoi d'appel automatique : **oui**
- Annuaires d'abonnés : **oui**

- Question 6 A : Veuillez préciser votre réponse si nécessaire.

La nécessité de règles spécifiques d'harmonisation au niveau européen est nécessaire afin d'apporter une protection maximale aux citoyens européens. (des règles spécifiques en elles-mêmes ne sont pas l'ultime objectif puisqu'une harmonisation abaissant les normes de protection dans certains pays n'est pas acceptable). Les dispositions inclues dans la directives peuvent largement être renforcées.

****

I.3. COHÉRENCE DE LA DIRECTIVE «VIE PRIVÉE ET COMMUNICATIONS ÉLECTRONIQUES»

Question 7 : les obligations en matière de sécurité de la directive « vie privée et communications électroniques » sont-elles cohérentes avec les exigences de sécurité définies dans les différents instruments juridiques suivants ?

Dans une large mesure / dans une certaine mesure / dans une faible mesure / pas du tout / je ne sais pas

- Directive-cadre (article 13 bis) : **dans une certaine mesure**
- Futur règlement général sur la protection des données définissant des obligations de sécurité applicables à tous les responsables du traitement des données: **dans une faible mesure**
- Directive sur les équipements radioélectriques : **dans une certaine mesure**
- Future directive concernant la sécurité des réseaux et de l'information (SRI) : **dans une certaine mesure**

Question 7 A : Veuillez préciser votre réponse si nécessaire.

L'article 4 de la directive ePrivacy est cohérent avec la directive cadre seulement dans une certaine mesure car cette dernière est plus précise et spécifie la nécessité de gérer les risques liés à « l'intégrité des réseaux et services et garantir la continuité de l'approvisionnement », ce que la directive ePrivacy

ne fait pas. Elle devrait pourtant contenir ce point pour rendre les exigences en matière de sécurité complètes.
La directive ePrivacy est également plutôt cohérente avec le futur réglement général mais comporte tout de même deux importantes lacunes : d'une part, contrairement au RGDP, elle ne mentionne pas es sous-traitants, qu isont porutant un maillon central dans le traitement des données. D'autre part la directive reste très évasive concernant les mesures techniques en matière de confidentialité. Afin de transposer et de préciser les principes affirmés dans le réglements général dans le contexte spécifique des réseaux de communication numérique, elle devrait pourtant évoquer clairement le droit au chiffrement et le droit à l'anonymat. Enfin, s'agissant des OTT, rappelons qu'aujourd'hui, le flou juridique les entourant conduit à un affaiblissement de la protection de la vie privée. En effet, puisque la directive ne mentionne pas clairement les prestataires de services de communications interpersonnelles par contournement, la Commission européenne mais aussi les autorités de contrôle des données personnelles ou les autorités de régulation de télécommunications de certains États membres ne considèrent pas que ces services sont soumis aux mêmes obligations en matière de sécurisation et de confidentialité des données personnelles.
Enfin concernant la directive SRI, la cohérence n'est pas assurée puisque d'après la directive ePrivacy c'est au fournisseur de prendre les mesures appropriées en matière de sécurité alors que du côté de la directive SRI, ce sont les États membres qui doivent demander aux opérateurs d'assurer la sécurité. La responsabilité n'incombe pas aux mêmes entités.

****

Question 8 : **la directive « vie privée et communications électroniques » interdit d'utiliser le courrier électronique, les télécopieurs et les systèmes d'appel automatisés à des fins de prospection directe, sauf si les utilisateurs ont donné leur consentement préalable (article 13, paragraphe 1). Les États membres sont cependant libres de choisir entre le consentement préalable et le droit d'opposition en cas d'appels à des fins de prospection avec interaction humaine (article 13, paragraphe 3).**

À votre avis, le fait de laisser aux États membres le choix de subordonner les appels à des fins de prospection avec interaction humaine à un consentement préalable ou à un droit d'opposition est-il cohérent avec l'article 13, paragraphe 1 (qui demande un consentement préalable en cas d'appels au moyen de courriers électroniques, de télécopieurs ou de systèmes d'appel automatisés), compte tenu des incidences sur la vie privée et des coûts entraînés par chacun de ces moyens de communication?

Non

Question 8 A : Veuillez préciser votre réponse si nécessaire.

L'intrusion dans la vie privée est tout aussi grave que ce soit par des appels automatisés que dans le cas de prospection avec interaction humaine et que ce soit par Internet ou par téléphone. Qu'il s'agisse du démarchage ou du profilage, des portions de vie privée sont exploitées à des fins publicitaires. Ces différents cas devraient être soumis à la même législation et le fait que les États membres puissent

définir le régime afférent rend la directive encore un peu plus incohérente et inapplicable dans la pratique. Néanmoins si le consentement préalable est préférable au droit d'opposition (qui ne peut être valable que dans une démarche pré-contentieuse) il ne faut pas le considérer comme une solution optimale car il ne garantit en rien la non-ingérence dans la vie privée. Le RGDP adopté en 2016 stipule que le consentement doit être libre, spécifique, éclairé et univoque et en ce qui concerne les données sensibles il doit être explicite. Or les techniques utilisées pour obtenir le consentement préalable des utilisateurs ne permettent pas toujours à ces derniers de donner un consentement éclairé car ce sont des formulations compliquées. Il arrive également que l'information sur les conséquences de ce consentement soient cachées dans un flot d'informations.Si la solution du consentement préalable est pour l'heure la moins mauvaise des solutions, il nous faut réfléchir à de nouvelles formes de garde-fous pour assurer le respect de la vie privée et de la confidentialité.

Question 9 : il existe une incertitude juridique quant à savoir si les messages de prospection envoyés via les médias sociaux sont couverts par le consentement préalable (« opt-in ») applicable au courrier électronique (article 13, paragraphe 1) ou par le droit d'opposition (« opt-out », article 13, paragraphe 3). Veuillez indiquer si vous êtes ou n'êtes pas d'accord avec les affirmations ci-après :

oui / non / sans avis

- Je trouve plus raisonnable d'appliquer aux messages de prospection envoyés via les médias sociaux les mêmes règles que celles appliquées au courrier électronique (consentement préalable) : **oui**
- Je trouve plus raisonnable d'appliquer le droit d'opposition aux messages de prospection envoyés via les médias sociaux (article 13) : **non**

****

I.4. EFFICACITÉ DE LA DIRECTIVE « VIE PRIVÉE ET COMMUNICATIONS ÉLECTRONIQUES »

Question 10 : **la protection de la vie privée et des données à caractère personnel dans le secteur des communications électroniques est également destinée à renforcer la confiance des utilisateurs dans ces services. Dans quelle mesure les dispositions nationales mettant en œuvre la directive « vie privée et communications électroniques » ont-elles contribué à renforcer la confiance des utilisateurs dans la protection de leurs données lorsqu'ils utilisent des services et réseaux de communications électroniques ?**

- **Dans une certaine mesure**

Question 10 A : Veuillez préciser votre réponse si nécessaire.

Les dispositions nationales mettant en œuvre la directive sont pour le cas de la France relativement peu innovantes. Les dispositions sur la sécurité, sur la confidentialité et sur les données de localisation semblent avoir été transposées de façon assez direct et sans grands changements.

Néanmoins il y a au moins une disposition de transposition que la France a mal appliqué. Il s'agit de l'article 15 sur les dérogations que les États membres peuvent mettre en place. Cet article se retrouve transposé de façon bien trop large dans l'article L34-1 III du Code des postes et des communications électroniques (CPCE) puisqu'il permet à l'État français de déroger au principe d'anonymisation et oblige la conservation des données pendant un an maximum, ce qui apparaît disproportionné et contraire à la Charte des droits fondamentaux telle qu'interprétée par l'Union européenne.. Cela entre en contradiction avec l'article 15 de la directive ePrivacy qui évoque des mesures « nécessaires, appropriées et proportionnées, au sein d'une société démocratique ».

****

Question 11 : dans quelle mesure la directive « vie privée et communications électroniques » engendre-t-elle des coûts supplémentaires pour les entreprises ?

- **Dans une certaine mesure**

Question 11 A : Veuillez donner une estimation du pourcentage du coût total et/ou indiquer toute autre information.

N/A

Question 12 : Selon vous, le coût de mise en conformité avec la directive « vie privée et communications électroniques » est-elle proportionnée aux objectifs poursuivis, notamment en ce qui concerne la confidentialité des communications, qui vise à préserver le droit fondamental à la vie privée?

Oui

Question 12 A : Veuillez préciser votre réponse si nécessaire.

Il y a en effet un coût non négligeable pour les entreprise notamment en matière de conservation des données et d'installation de systèmes de sécurité performants. Néanmoins il est évident que ce coût est non seulement nécessaire à la poursuite des objectif mais également proportionné, quand il n'est pas, au surplus, un atout concurrentiel. Les opérateurs doivent être en mesure d'assurer la confidentialité des communications des utilisateurs et également la sécurité de leurs infrastructures.

****

I.5. VALEUR AJOUTÉE EUROPÉENNE DE LA DIRECTIVE « VIE PRIVÉE ET COMMUNICATIONS ÉLECTRONIQUES »

Question 13 : pensez-vous que des mesures nationales seraient nécessaires s'il n'y avait pas de législation européenne sur la vie privée et les communications électroniques ?

Oui

Question 14 : Selon votre expérience, jusqu'à quel point la Directive vie privée et communications électroniques a-t-elle démontré qu'elle avait une claire valeur ajoutée au niveau européen pour réaliser les objectifs suivants :

Tout à fait d'accord / d'accord / pas d'accord / pas du tout d'accord / je ne sais pas

- La directive renforce la confidentialité des communications électroniques en Europe : **d'accord**
- La directive harmonise la confidentialité des communications électroniques en Europe : **d'accord**
- La directive garantit la libre circulation des données à caractère personnel et des équipements : **tout à fait d'accord**

****

II. RÉVISION DE LA DIRECTIVE « VIE PRIVÉE ET COMMUNICATIONS ÉLECTRONIQUES » : PERSPECTIVES

Question 15 : en vous appuyant sur votre expérience de la directive « vie privée et communications électroniques » et en tenant dûment compte de la proposition de règlement général sur la protection des données, quelles devraient être les priorités d'un futur instrument juridique couvrant la protection de la vie privée et des données dans le secteur des communications électroniques ? (plusieurs réponses possibles)

X Élargir le champ d'application de la directive aux prestataires de services par contournement (services OTT)

X Modifier les dispositions sur la sécurité

X Modifier les dispositions sur la confidentialité des communications et des équipements terminaux

X Modifier les dispositions sur les communications non sollicitées

X Modifier les dispositions sur la gouvernance (autorités nationales compétentes, coopération, amendes, etc.)

Autres

Aucune de ces dispositions n'est plus nécessaire

****

Question 16 : selon vous, un instrument directement applicable ne devant pas être mis en œuvre par les États membres (c'est-à-dire un règlement) serait-il mieux à même de garantir un niveau équivalent de protection de la vie privée dans le cadre du traitement des données dans le secteur des communications électroniques, ainsi que la libre circulation de ces données ?

Oui

Question 16 A : Si vous avez répondu «Autre», veuillez préciser.

Un règlement qui viendrait remplacer la directive « vie privée et communications électroniques » pourrait en effet être une solution intéressante afin de renforcer l'harmonisation des législations en matière de protection des données et de vie privée au sein de l'Union européenne. Cela permettrait aux entreprises et aux citoyens de mieux anticiper les législations de chaque État membre. Nous savons que les règlements ont pu être depuis quelques temps de plus en plus larges en laissant une plus grande marge de manœuvre aux États membres et se sont ainsi, sur le papier, rapproché du format des directives. Si à court terme une telle évolution n'apparaît pas comme cruciale, elle pourrait le devenir à plus long terme. En effet, de petites différences de mise en œuvre à court terme deviennent des incohérences et des traditions irréconciliables à long terme. C'est pour cela qu'à l'avenir, l'UE devra opter pour un règlement le plus précis possible et ainsi assurer une harmonisation ambitieuse de long terme. Il serait qui plus est opportun qu'une symétrie soit respectée avec le RGDP et que l'Union européenne affirme le principe de confidentialité des communications de façon impérieuse.

****

II.1. RÉEXAMEN DU CHAMP D'APPLICATION DE LA DIRECTIVE

Question 17 : faudrait-il élargir le champ d'application de la directive pour que les fournisseurs

de services par contournement (« services OTT ») offrent un niveau de protection identique lorsqu'ils fournissent des services de communication comme services de voix sur IP, messagerie instantanée et messagerie sur les réseaux sociaux ?

Oui

Question 18 : si vous avez répondu «Oui» ou «En partie», veuillez indiquer les principes et les obligations en matière de vie privée qui devraient s'appliquer aux services OTT (plusieurs réponses possibles):

Tout à fait d'accord / d'accord / pas d'accord / pas du tout d'accord / je ne sais pas

- Obligations en matière de sécurité - **tout à fait d'accord**
- Confidentialité des communications (consentement préalable à l'interception des communications électroniques) - **tout à fait d'accord**
- Données de trafic et de localisation (consentement préalable avant traitement) - **tout à fait d'accord**
- Communications commerciales non sollicitées (Est-ce que l'article 13 devrait s'appliquer aux messages envoyés à travers des services OTT ?) - **tout à fait d'accord**

****

Question 19 : selon vous, quelles sont les obligations qui devraient s'appliquer aux réseaux ci-après (éventuellement sujettes à des adaptations pour les différents acteurs sur la base du principe de proportionnalité) ?

	Tous les réseaux publics, privés ou fermés	**Accès non-commercial à l'internet WiFi (p.ex. accessoire à d'autres activités) fourni aux clients/au public dans les aéroports, hôpitaux, centres commerciaux, universités, etc.)**	**Uniquement les réseaux publics (comme à l'heure actuelle)**
Sécurité		X	X
Confidentialité des communications		X	X
Données de trafic et de localisation		X	X

****

II.2. ASSURER LA SÉCURITÉ ET LA CONFIDENTIALITÉ DES COMMUNICATIONS

Question 20 : **la responsabilisation des utilisateurs et les moyens mis à leur disposition pour protéger leurs communications, notamment en sécurisant leur connexion WiFi et/ou en appliquant des mesures techniques de protection, acquièrent une importance croissante compte tenu des risques existant en matière de sécurité.**

Pensez-vous que la législation devrait garantir le droit des particuliers à sécuriser leurs communications (en choisissant des mots de passe appropriés pour les réseaux sans fil à domicile ou en utilisant des applications de cryptage, p. ex.), sans que cela porte atteinte à la nécessité de faire appliquer la loi pour protéger des intérêts publics majeurs, conformément aux procédures, conditions et garanties prévues par la législation?

Oui

Question 20 A : Veuillez préciser si nécessaire.

Les outils, technologies et services de chiffrement sont essentiels pour protéger notre infrastructure numérique et nos communications personnelles des intrusions indésirables. A l'ère numérique, la croissance économique repose sur la capacité à faire confiance et à authentifier nos interactions, et à nous livrer à des activités commerciales en toute sécurité, à l'échelle nationale comme transnationale. L'absence de chiffrement facilite l'accès à des données personnelles sensibles, notamment les informations d'identité et les données financières, par des criminels et autres acteurs malintentionnés. Selon le Rapporteur spécial des Nations Unies pour la liberté d'expression : « le chiffrement et l'anonymat, et les concepts protecteurs qui en découlent, fournissent la confidentialité et la sécurité nécessaires pour l'exercice du droit à la liberté d'opinion et d'expression à l'ère numérique. » Les utilisateurs devraient avoir le choix d'utiliser, et les entreprises de proposer, les méthodes de chiffrement les plus efficaces actuellement disponibles, y compris le chiffrement de bout en bout, sans craindre de voir les gouvernements les contraindre à fournir un accès au contenu, aux métadonnées ou aux clés de chiffrements, si ce n'est dans le respect à la fois de la procédure judiciaire et des droits de l'Homme.

Toutefois, nous insistons sur le fait que la question porte sur le « droit des particulier à sécuriser leurs communication ». Notamment s'agissant des accès WiFi, ce droit ne doit pas devenir une obligation. Nous pensons ici au cas français et plus précisement aux dispositions de la loi n°2009-669 du 12 juin 2009 qui créent une obligation de sécurisation de son accès WiFi et fait du titulaire d'un accès WiFi le responsable des activités conduites par les utilisateurs de cet accès, ou encore à une affaire pendante devant la CJUE – l'affaire MacFadden – portant sur la responsabilité d'une personne mettant librement (i.e. sans mot de passe ou autre mécanisme d'authentification) à disposition un accès WiFi. De telles obligations de sécurisation, directes (comme dans la loi française) ou indirecte (via les règles de responsabilités civiles ou pénales) de sécurisation sont disproportionnées s'agissant de particuliers,

d'acteurs non commerciaux ou même d'acteurs commerciaux offrant ces accès à titre accessoire ou gracieux. La libre fourniture de point d'accès à Internet ouverts au public et ne nécessitant pas de mécanismes d'authentification participe des objectifs publics en matière d'accès au haut-débit. Pour cette raison, leur déploiement doit être encouragé et les règles juridiques entravant un tel déploiement être revues.

Attention : le développement des réponses dans la consultation est limité à 1500 caractères. Notre argumentaire ici en comptabilise beaucoup plus mais nous avons tenu à ne pas nous restreindre sur ce thème primordial qu'est le droit à la sécurisation des données. Ainsi si vous souhaitez vous inspirer de notre raisonnement pour répondre à la consultation, nous vous laissons choisir vos 1500 caractères.

****

Question 21 : **malgré les nombreuses dispositions législatives existant en matière de sécurité, les atteintes à la sécurité fréquemment rapportées soulignent la nécessité d'adopter des mesures supplémentaires. Selon vous, dans quelle mesure les actions suivantes permettraient-elles d'améliorer cette situation?**

	dans une large mesure	dans une certaine mesure	dans une faible mesure	pas du tout	je ne sais pas
Élaboration de normes minimales de sécurité ou de respect de la vie privée pour les réseaux et services					
Extension des exigences en matière de sécurité afin d'élargir la couverture des logiciels liés à la fourniture d'un service de communication, comme les systèmes d'exploitation embarqués dans des équipements terminaux					
Extension des exigences en matière de sécurité afin d'élargir la couverture de l'internet des objets, tels que ceux utilisés dans les dispositifs informatiques portés sur soi (« wearable computing »), la domotique, la communication de véhicule à véhicule, etc.					
Extension des exigences en matière de sécurité afin d'élargir la couverture de tous les composants de réseau, y compris les cartes SIM, les appareils utilisés pour la commutation ou le routage des signaux, etc.					

****

Question 22 : les pratiques de certains sites web, qui refusent l'accès aux utilisateurs n'acceptant pas les cookies (ou d'autres technologies) ont suscité des critiques sur l'absence de choix réel laissé aux internautes. **Que pensez-vous des mesures proposées ci-après en vue d'améliorer cette situation?**

Tout à fait d'accord / d'accord / pas d'accord / pas du tout d'accord

- Les fournisseurs de services de la société de l'information devraient être tenus de proposer un service payant (sans publicité comportementale), à la place des services payés par les informations à caractère personnel des utilisateurs : **tout à fait d'accord**
- Les fournisseurs de services de la société de l'information ne devraient pas avoir le droit d'empêcher l'accès aux services non soumis à abonnement lorsque les utilisateurs refusent le stockage d'identifiants dans leur équipement terminal (identificateurs non nécessaires au fonctionnement du service, p. ex.) : **d'accord**

Question 22 A : Veuillez préciser si nécessaire.

Les utilisatrices et utilisateurs devraient systématiquement pouvoir choisir la manière dont ils rémunèrent les services en ligne qu'ils utilisent, en permettant l'exploitation de leurs données personnelles ou via une autre forme de contribution. Celle-ci peut prendre différentes formes : bénévolat, packaging avec un autre service, ou, comme suggéré dans la question, un prix proche des revenus tirés par le fournisseur de service au travers de l'exploitation de ces données (généralement une somme modique). À plus large échelle, la mise en place d'une « contribution créative » ou d'un autre système de mutualisation coopérative permettrait de financer les contributrices et contributeurs des services et d'envisager le développement de nouveaux modèles économiques.

C'est là la meilleure manière de garantir une réelle liberté de choix aux utilisatrices et utilisateurs tout en encourageant le développement de modèles économiques qui ne reposent pas sur la collecte des données personnelles, lesquels comportent nécessairement des risques en terme de respect du droit à la vie privée.

La seconde proposition pourrait être soutenue à condition d'introduire une différenciation des cookies par le fournisseurs de service. Très peu de fournisseurs offrent un choix réellement différencié et explicite aux utilisateurs. Les pratiques de la CNIL sont un point de départ intéressant en la matière. Laisser le libre choix à l'utilisateur de choisir les cookies qu'il souhaite autoriser et ceux qu'il souhaite bloquer en faisant la distinction, de façon simple et pédagogique, entre cookies de fonctionnement et cookies de *traçage* est non seulement possible mais est également indispensable pour mettre en place cette deuxième proposition.
Afin de ne pas importuner l'utilisateur inutilement tout en lui permettant de prendre pleinement conscience des enjeux de l'utilisation des cookies, une information réellement pertinente devrait être fournie (par exemple : quelles sites/entreprises auront *in fine* usage des informations et à quelles fins précises). Aussi, des formulaires clairs de refus de traitement des données personnelles par les *data brokers* est devenue indispensable. L'accès à de tels formulaires devrait être rendu obligatoire, par exemple au travers d'une bannière diffusée sur les sites internet.

Attention : le développement des réponses dans la consultation est limité à 1500 caractères. Notre argumentaire ici en comptabilise beaucoup plus mais nous avons tenu à ne pas nous restreindre sur ce thème primordial qu'est le consentement face aux coockies . Ainsi si vous souhaitez vous inspirer de notre raisonnement pour répondre à la consultation, nous vous laissons choisir vos 1500 caractères.

****

Question 23 : **en tant que consommateur, souhaitez-vous, dans les cas indiqués ci-après, que l'on vous demande votre consentement préalable pour traiter vos données à caractère personnel et d'autres informations stockées sur vos appareils intelligents ? Veuillez sélectionner les options pour lesquelles vous voulez que votre consentement informé soit demandé (plusieurs réponses possibles) :**

X Identifiants placés/recueillis à des fins de publicité comportementale en ligne par un service de la société de l'information autre que celui que vous êtes en train de consulter

X Identifiants placés/recueillis par le service de la société de l'information que vous êtes en train de consulter, afin d'analyser le site web, de mesurer le nombre de visiteurs, d'analyser la navigation des utilisateurs sur le site, etc. (« cookies propres » ou technologies équivalentes)

X Identifiants placés/recueillis par le service de la société de l'information que vous êtes en train de consulter, afin de faciliter la navigation (cookies permettant de mémoriser la langue, p. ex.)

X Identifiants placés/recueillis par un service de la société de l'information afin de détecter les fraudes ?

X Identifiants placés/recueillis par un service de la société de l'information afin de mettre en place une limite de fréquence (nombre de fois où l'utilisateur voit une publicité)

X Identifiants recueillis et immédiatement rendus anonymes de manière que l'appareil de l'utilisateur soit impossible à identifier

Question 23 A : Veuillez préciser si nécessaire.

L'identifiant de l'utilisateur que comporte le cookie doit être considéré comme une donnée personnelle. Plus généralement l'intrusion dans la vie privée que les cookies représentent explique bien la nécessité d'encadrer son usage.
La réglementation actuelle n'est pas optimale car seuls les cookies liés aux opérations relatives à la publicité ciblée, les cookies des réseaux sociaux générés par les « boutons de partage de réseaux sociaux » et certains cookies de mesure d'audience nécessitent le consentement préalable des utilisateurs. Non seulement cela ne couvre qu'un champ restreint mais en plus dans la pratique l'obligation de fournir l'information est assez mal respectée puisque inintelligible ou invisible. Le consentement n'est donc bien souvent pas « éclairé » comme le RDGP l'impose.
Pour pallier ces lacunes, la CNIL a développé un guide de bonnes pratiques (pratiques qu'elle même applique) somme toute pertinent qu'il serait bon de considérer comme point de départ. Il importe en effet de ne plus présenter de façon indifférenciée cookies traceur et cookies de fonctionnement et afin que l'utilisateur, noyé sous un flot d'informations inintelligibles, n'accepte pas sans avoir réellement pris

connaissance des implications de sa décision.
(voir https://www.cnil.fr/fr/exemple-de-bandeau-cookie ainsi que la réponse à la question 23).

Question 24 : **il a été avancé que le fait de demander le consentement des utilisateurs pour stocker des informations/accéder à des informations stockées dans leurs appareils, notamment en installant des cookies traceurs, pouvait perturber la navigation sur internet. Pour faciliter la procédure et la capacité des utilisateurs à donner leur consentement, il faudrait mettre en place un nouvel instrument de protection de la vie privée dont les objectifs seraient les suivants (plusieurs réponses possibles) :**

X obliger les fabricants d'équipements terminaux, y compris de systèmes d'exploitation et de navigateurs, à commercialiser des produits dotés de paramètres de confidentialité par défaut (cookies tiers désactivés par défaut, p. ex.)

X adopter une législation (actes délégués, p. ex.) afin de définir des mécanismes permettant à l'utilisateur d'exprimer ses préférences en matière de pistage

X charger les organismes européens de normalisation de préparer des normes (« Ne pas pister », « Ne pas stocker/collecter », p. ex.)

X introduire des dispositions interdisant certains comportements abusifs, indépendamment du consentement de l'utilisateur (enregistrement audio/vidéo non sollicité par des appareils domestiques intelligents, p. ex.)

renforcer l'autorégulation

Question 24 A : Veuillez préciser si nécessaire.

Nous sommes tout à fait d'accord sur le fait que demander systématiquement un consentement et ce de la façon la plus explicite et éclairée possible est préférable au droit à l'opposition. Néanmoins ce régime de consentement préalable comporte dans la pratique certaines limites. Donner, non pas son simple accord par un clic mais un réel consentement éclairé et explicite demande non seulement du temps, de l'envie et certaines capacités pour pouvoir comprendre les enjeux liés à cette décision. Il convient donc de s'assurer que les utilisateurs sont informés de chaque traitement et qu'ils ont la possibilité de refuser ce traitement tout en ayant accès au service.
Plus généralement l'Union européenne doit tendre vers une législation qui garantit le régime le plus protecteur par défaut. Le règlement général sur la protection des données a amorcé cela avec son article 25. Mais on peut aller plus loin : l'idée de certains paramètres par défaut est intéressante si et seulement si cela assure une protection maximale. L'élaboration de normes protectrices par des organismes européens pourrait également être une piste à suivre.
Néanmoins, en l'état actuel des choses, tant que ces systèmes alternatifs protecteurs et non fondés exclusivement sur le consentement ne sont pas en vigueur, seul un régime basé sur le consentement préalable (opt-in) est acceptable, tout régime basé sur le droit à l'opposition (opt-out) devant être exclu.

****

Question 25 : **la directive « vie privée et communications électroniques » prévoit des protections spécifiques en matière de respect de la vie privée en ce qui concerne le traitement des données de trafic et de localisation, afin de garantir la confidentialité des communications. Elle dispose notamment que ces données doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication ou que l'utilisateur doit donner son consentement préalable à leur utilisation pour des services à valeur ajoutée (guidage routier, informations sur le trafic, prévisions météorologiques ou informations touristiques, p. ex.). Les dérogations existantes autorisent, en cas de nécessité, le traitement des données de trafic durant une période limitée, par exemple à des fins de facturation. Veuillez consulter le document de référence pour en savoir plus.**

Pensez-vous qu'il faudrait modifier les dérogations concernant le consentement préalable pour le traitement des données de trafic et de localisation? Vous pouvez choisir plusieurs réponses :

	les dérogations devraient être étendues afin d'inclure l'utilisation de ces données à des fins statistiques, moyennant des garanties appropriées
	les dérogations devraient être étendues afin d'inclure l'utilisation de ces données dans l'intérêt public (recherche, gestion de la circulation, etc.), moyennant des garanties appropriées
	les dérogations devraient permettre d'utiliser ces données à d'autres fins, mais uniquement si elles sont rendues entièrement anonymes.
X	les dérogations ne devraient pas être étendues
	la disposition relative aux données de trafic et de localisation devrait être supprimée.

****

II. 3. FACTURES NON DÉTAILLÉES, PRÉSENTATION DE L'IDENTIFICATION DE LA LIGNE APPELANTE, RENVOI D'APPEL AUTOMATIQUE ET ANNUAIRE DES ABONNÉS

Question 26 : donnez-nous votre avis sur les aspects suivants :

	Cette disposition est utile et devrait être maintenue	Cette disposition devrait être modifiée	Cette disposition devrait être supprimée	Autre
Factures non détaillées	X			

Présentation et restriction de l'identification des lignes appelante et connectée	X		
Renvoi d'appel automatique			X
Annuaires d’abonnés		X	

Question 26 A: Veuillez préciser si nécessaire.

N/A

Question 27 : pensez-vous que les États membres devraient garder la possibilité de choisir entre le consentement préalable (« opt-in ») et le droit d’opposition (« opt-out ») dans les cas suivants :

	Oui	Non	Je ne sais pas
Appels téléphoniques à des fins de prospection directe (avec interaction humaine) visant des particuliers		X	
Communications à des fins de prospection directe visant des personnes morales (systèmes d'appel automatisés, télécopieurs, courriers électroniques et appels téléphoniques avec interaction humaine)		X	

Question 28 : si vous avez répondu « Non » à une ou plusieurs des options ci-dessus, quel est le régime qui devrait s’appliquer dans les cas suivants?

	consentement préalable («opt-in»)	droit d’opposition («opt-out»)	je ne sais pas
Communications téléphoniques à des fins de prospection directe avec interaction humaine	X		
Protection des personnes morales	X		

Question 28 A : Veuillez préciser si nécessaire.

Comme nous l'écrivions à la question 8, la prospection par téléphone avec interaction humaine n'est pas moins envahissante que la prospection automatique ou par internet. Toutes sont une intrusion dans la vie privée si l'utilisateur n'a pas donné son consentement préalable. Donc dans tous ces cas de figure cités, que ce soit pour des personnes physiques ou morale, le consentement préalable - opt-in - est à privilégier face au droit à l'opposition - opt-out. Néanmoins, nous rappelons une nouvelle fois que le régime de l'opt-in n'est pas une solution optimale. Il est impensable que tous les utilisateurs puissent

donner systématiquement un consentement explicite ou au moins éclairé. Le consentement préalable est donc une fausse bonne idée qui peut-être utlisée en attendant de développer un solide système de protection maximale par défaut.

****

II.5. MISE EN ŒUVRE FRAGMENTÉE ET APPLICATION NON HARMONISÉE DE LA DIRECTIVE

Question 29 : estimez-vous qu'il est nécessaire de confier l'application de la directive à une autorité unique ?

Oui

Question 30: si vous avez répondu « Oui », quelle serait l'autorité la plus appropriée ?

Autorité nationale chargée de la protection des données

(Voir la justification à la question 33)

Question 30 A : Si vous avez répondu « Autre », veuillez préciser.

Nous n'avons pas répondu « Autre » mais nous allons tout de même détailler notre opinion.

Pour respecter une certaine cohérence avec le RGDP et favoriser l'harmonisation au sein de l'Union européenne, cette mission devrait revenir aux autorités de protection des données à caractère personnel telles que définies par le règlement (UE) 2016/679. Celles-ci ont été particulièrement actives dans l'élaboration du RGDP à travers le Groupe de travail Article 29 sur la protection des données. Elles sont d'ailleurs consacrées par ce règlement lorsque celui-ci crée un mécanisme cohérent de contrôle et de gestion des plaintes basé sur le « European data protection Board », lui-même exclusivement constitué d'autorités nationales de protection des données.

Néanmoins nous tenons à insister sur le fait que le texte qui remplacera la directive ePrivacy doit accentuer le principe d'indépendance de ces autorités. En effet, à l'heure actuelle les différentes autorités nationales n'ont pas la même indépendance vis-à-vis de leurs États d'appartenance. Cela a pu poser de gros problèmes, notamment en Croatie où le Gouvernement a fait pression sur l'autorité nationale de protection des données.

Qui plus est, il apparaît primordial de s'assurer que les autorités en question ont la capacité voire l'obligation aussi bien matérielle, procédurale que juridique d'agir à l'encontre des autorités publiques, lorsque celles-ci portent atteinte au principe de confidentialité des communications notamment.

****

Question 31 : le futur mécanisme de cohérence créé par le règlement général sur la protection des données devrait-il s'appliquer aux aspects transfrontières couverts par le futur instrument concernant la vie privée et les communications électroniques ?

Oui

Question 32 : pensez-vous que le nouvel instrument concernant la vie privée et les communications électroniques devrait inclure des amendes et des recours spécifiques en cas de violation de ses dispositions correspondantes (violation de la confidentialité des communications, p. ex.) ?

Non

Question 33 : Ces questions visent à obtenir une large consultation sur le fonctionnement et la révision de la directive « vie privée et communications électroniques ». Vous pouvez indiquer d'autres questions qui devraient être prises en considération. Veuillez également nous communiquer les données quantitatives, rapports ou études sur lesquels vous vous appuyez.

Concernant les services par contournement (OTT) :
Revenons tout d'abord sur la question des services par contournement pour lesquels nous n'avons pas pu développer notre opinion auparavant. Les OTT doivent rentrer dans le champ de la directive afin que les dispositions de l'article 4 sur la sécurité et de l'article 5 sur la confidentialité s'appliquent à eux.
Néanmoins ces services par contournement devraient avoir un statut propre et ainsi rentrer dans une nouvelle notion de fournisseurs de services de communication, distincte de celle « d'opérateurs », qui sont, eux, soumis à des obligations très spécifiques (déclaration aux ARNs, etc.) qui ne sont pas pertinentes pour les OTT.

Concernant les amendes :
Nous sommes en faveur de la mise en place d'amendes ambitieuses, déjà consacrées par le règlement général sur la protection des données, afin de faire respecter les dispositions de la directive. . Il serait non seulement redondant d'évoquer ces amendes dans la directive ePrivacy mais également dangereux car cela ouvrirait la porte à un potentiel affaiblissement de ces amendes.

Concernant les mesures supplémentaires en matière de sécurité :
Nous avons délibérément choisi de ne pas répondre à la question 21 car celle-ci est biaisée. Par exemple la première affirmation sur l'élaboration de normes minimales de sécurité n'a pas de sens. Les problèmes de sécurité qui ont des conséquences sur la protection des données personnelles ne viennent pas de « normes » au sens juridique (règlement européen, ISO, etc.), mais de manquements aux règles de l'art de et bonnes pratiques en matière de sécurité informatique (développement, conception, architecture des réseaux ou architecture des solutions logicielles, etc.). La création de normes pourrait présenter un intérêt, maissuit un processus très lent, rigide dans un domaine qui est très mouvant.

Par ailleurs, l'idée d'élargir la couverture des logiciels liés à la fourniture d'un service de

communication est une idée dangereuse, et ce pour deux raisons : d'une part cela met en danger la possibilité d'installer un logiciel libre (par exemple comme l'affirmation le suggère : système d'exploitation). En effet élargir la responsabilité pourrait se traduire par la mise en place d'une impossibilité pratique pour l'utilisateur final d'utiliser le logiciel de son choix sur le terminal qu'il possède. Ce verrouillage du couplage entre le matériel et le logiciel se traduit systématiquement par l'utilisation de solutions moins sécurisées, puisqu'elles ne peuvent plus faire l'objet de revue par les pairs, n'étant auditables qu'en interne chez les éditeurs/fabricants. En pratique les solutions réputées les plus sécurisées sont celles qui sont développées par des communautés ouvertes, permettant une revue du code par les pairs. Ce n'est pas par hasard si Tor, ou tous les mécanismes de chiffrement utilisés sur Internet s'appuient de manière directe ou indirecte sur des outils, des protocoles et des normes établis de manière ouverte.