Avis n° 10/2012 du 21 mars 2012

Objet : Projet de loi portant des dispositions diverses en matière de communications électroniques (CO-A-2012-009)

La Commission de la protection de la vie privée (ci-après "la Commission") ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après la "LVP"), en particulier l'article 29 ;

Vu la demande d'avis du Vice-Premier Ministre, Ministre de l'Économie, des Consommateurs et de la Mer du Nord, reçue le 27/02/2012 ;

Vu le rapport du Président ;

Émet, le 21 mars 2012, l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS

---

1. Le 27 février 2012, le Vice-Premier Ministre, Ministre de l'Économie, des Consommateurs et de la Mer du Nord a demandé à la Commission d'émettre un avis sur un projet de loi portant des dispositions diverses en matière de communications électroniques (ci-après le "projet de loi").

2. La Commission a également reçu, joint à la demande, un projet de loi portant modification de la loi du 17 janvier 2003 *concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges*. La Commission constate que ce texte n'implique aucun traitement de données à caractère personnel devant donner lieu à un avis de la Commission de la protection de la vie privée. Elle n'abordera dès lors pas davantage ce projet de loi.

3. Le projet de loi vise notamment la transposition en droit national de la Directive 2009/136/CE[1], faisant partie du nouveau Paquet télécoms européen de 2009. Cette directive comporte une modification (notamment) 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*.

4. La Commission est consultée sur ces aspects du projet de loi qui concernent la protection des données à caractère personnel. Elle souligne pour mémoire qu'elle a déjà formulé des opinions pertinentes sur plusieurs thèmes apparentés comme en ce qui concerne la rétention de données[2], la problématique de la cybersurveillance ou du contrôle de l'employeur de l'utilisation d'Internet et de la messagerie électronique par les travailleurs[3].

II. LÉGISLATION APPLICABLE

---

5. Le présent avis examine les articles du projet de loi relatifs à la protection de la vie privée.

---

[1] Directive *modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, 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 et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs.*

[2] Avis n° 20/2009 du 1er juillet 2009 *relatif à l'avant-projet de loi et au projet d'arrêté royal en matière de rétention de données et au projet d'arrêté royal relatif à l'obligation de collaboration*, publié sur le site http://www.privacycommission.be/fr/docs/Commission/2009/avis_20_2009.pdf.

[3] Voir la note exploratoire disponible sur le site www.privacycommission.be.

6. Ces articles sont confrontés aux principes de la LVP, à ceux de la Directive 2002/58/CE et aux points de vue des autorités européennes de protection des données concernant la transposition des Directives 2002/58/CE et 2009/136/CE, et les différents thèmes relatifs à la vie privée et aux communications électroniques.

7. Dès lors, la Commission se réfère ci-après à maintes reprises aux points de vue :
   - du Groupe de travail Article 29 (ci-après "le Groupe 29"[4]) ;
   - du Groupe de travail international sur la protection des données dans les télécommunications (ci-après "le Groupe de Berlin"[5]) ;
   - du Contrôleur européen de la protection des données (ci-après "CEPD"[6]).

III. EXAMEN GÉNÉRAL DU PROJET DE LOI

3.1. Aperçu des aspects relatifs à la protection de la vie privée

8. Le projet de loi se penche sur les différents aspects de la protection de la vie privée dans le cadre des communications électroniques. Les thèmes et articles suivants du projet de loi se révèlent pertinents pour la protection de la vie privée :

   - informations de localisation pour les services d'urgence (article 64 du projet de loi) ;
   - accès aux données téléphoniques sur la facture détaillée pour la personne concernée qui n'est pas l'abonné (article 67 du projet de loi) ;
   - compétence complémentaire de l'IBPT concernant la sécurité des réseaux et services (articles 74-76 du projet de loi) et concernant le fait de prendre connaissance des procédures internes des opérateurs pour les demandes d'accès à des données à caractère personnel (article 87) ;
   - obligation de notification d'une violation de la sécurité d'un service de communications électroniques accessible au public portant sur des données à caractère personnel (article 77 du projet de loi), ci-après "obligation de notification restreinte" – définition de violation de la sécurité d'un service de communications électroniques accessible au public portant sur des données à caractère personnel (article 14, 25° du projet de loi) ;

---

[4] http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm. Voir principalement l'avis 1/2009 *concernant les propositions modifiant la directive 2002/58/CE sur la protection de la vie privée dans le secteur des communications électroniques (directive "vie privée et communications électroniques")*, publié à l'adresse suivante : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp159_fr.pdf ainsi que l'avis 2/2010 *sur la publicité comportementale en ligne* ("online behavioural advertising"), publié à l'adresse suivante : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_nl.pdf.

[5] http://www.privacycommission.be/fr/international/berlin-telecom/index.html.

[6] http://www.CEPD.europa.eu/CEPDWEB/CEPD/CEPD?lang=fr.

- exceptions supplémentaires au secret des communications et télécommunications privées (articles 86 et 87 du projet de loi) ;
- règlement des cookies et autres fichiers ou logiciels espions (enregistrement d'informations ou obtention d'un accès à des informations déjà enregistrées sur des équipements terminaux d'un abonné ou d'un utilisateur) via l'exigence de consentement (article 88 du projet de loi), ci-après le "cookie consent" ;
- conditions pour la collecte et la publication de données des abonnés dans des annuaires (articles 65 et 115 du projet de loi) ;
- protection de l'utilisateur à l'égard de communications non souhaitées (article 123 du projet de loi).

3.2. Remarques générales :

3.2.1 Principe de complémentarité de la loi du 13 juin 2005 *relative aux communications électroniques* (ci-après "la loi du 13 juin 2005") à l'égard de la LVP – ancrage légal de la coopération entre l'IBPT et la Commission

9. La Commission souligne la possibilité que plusieurs dispositions du projet de loi portant sur la sécurité se chevauchent avec la LVP qui transpose la Directive 95/46/CE[7]. Elle souligne l'intention du législateur européen de compléter la Directive 95/46/CE avec la Directive 2002/58/CE[8]. Les dispositions de la loi du 13 juin 2005 et de la LVP peuvent dès lors se chevaucher, mais doivent plutôt être considérées comme complémentaires que comme portant préjudice à la LVP.

10. Concrètement, cela signifie par exemple que dans les cas où aucun consentement n'est requis pour utiliser certains cookies, la personne concernée devra quand même toujours être informée sur la base de la LVP par le webmaster ou le tiers concerné (voir ci-après la discussion des exceptions à l'article 88 du projet de loi et l'obligation générale d'information à l'article 9, §§ 1 et 2 de la LVP). Cela signifie aussi par exemple que les clients ou personnes concernées vis-à-vis desquels des communications électroniques sont utilisées via l'une ou l'autre technique (e-mail, fax, téléphone, cookies, …) conservent toujours leur droit d'opposition à l'égard de tous les traitements à des fins de marketing direct (par exemple aussi s'il n'y a pas de publicité, s'il s'agit de communications à des fins non commerciales, …) (article 12 de la LVP).

[7] Depuis l'entrée en vigueur le 1er décembre 2010 de la loi du 11 décembre 1998.
[8] Voir le considérant 10 et les différentes dispositions de la Directive 2002/58/CE "sans préjudice" à l'article 2 de cette Directive.

11. À l'instar de l'exemple néerlandais[9], la Commission recommande de rappeler de nouveau clairement dans l'Exposé des motifs cette complémentarité de la loi du 13 juin 2005 à l'égard de la LVP, et de reprendre les différents exemples à ce sujet dans le présent avis (voir également ci-après).

12. D'autre part, la Commission souhaite que le législateur fixe explicitement dans la loi du 13 juin 2005 une coopération plus étroite entre la Commission et l'IBPT[10] en ce qui concerne les thèmes où les compétences de contrôle réciproques se chevauchent, ce eu égard notamment à l'obligation légale de confidentialité reprise à l'article 33 de la LVP.

3.2.2. Neutralité de l'Internet et "Deep packet inspection" (inspection approfondie des paquets)

13. La Commission souhaite enfin attirer l'attention sur un autre aspect, bien qu'au sens strict, cela n'ait rien à voir avec la transposition de la Directive 2009/136/CE.

14. Elle estime que le législateur devrait également ancrer dans la loi du 13 juin 2005 le nouveau principe européen de neutralité de l'Internet[11], ce afin de limiter en temps utile les formes de deep packet inspection[12] les plus intrusives dans la vie privée que pratiquent les Internet Service Providers (fournisseurs d'accès à Internet, ci-après "ISP") belges et les autres acteurs du marché.

15. Elle se réfère au point de vue du CEPD[13] à cet égard et formulera une recommandation distincte sur ces thèmes.

---

[9] Voir la page 14 du rapport de TNO-IViR, publié à l'adresse suivante : http://www.tno.nl/downloads/rapport_opta_35473.pdf.
[10] Voir l'exemple néerlandais de 2009 : http://www.cbpweb.nl/downloads_pb/pb_20090915_samenwerkingsovereenkomst_at-cbp.pdf.

[11] Le concept de neutralité de l'Internet *"repose sur l'idée que les informations sur l'Internet doivent être transmises de manière impartiale, indépendamment de leur contenu, de leur destination ou de leur source, et que les utilisateurs doivent pouvoir décider d'utiliser les applications, les services et le matériel de leur choix. Cela implique que les FSI ne peuvent hiérarchiser ou ralentir arbitrairement l'accès à certains services ou applications tels que le poste à poste (P2P), etc.*".

[12] Le DPI est en fait une technique connue depuis déjà longtemps par laquelle on inspecte automatiquement (quasiment) en temps réel certains paquets de données dans le trafic sur le réseau. Si on expliquait la technique de DPI au moyen de la circulation classique du courrier, cela signifierait que (au moins) le nom de l'expéditeur, du destinataire, le type d'enveloppe ou de message, etc. seraient traités par le service postal pour différentes finalités avant de remettre le courrier. La prise de connaissance du contenu de la communication n'est pas toujours présente dans toutes les formes de DPI, mais en constitue toutefois une possibilité technique (bien qu'illégale).

[13] Avis du 7 octobre 2011 du Contrôleur européen de la protection des données *sur la neutralité de l'internet, la gestion du trafic et la protection de la vie privée et des données personnelles*, JO, C34/1, 8 février 2012, publié à l'adresse suivante : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:034:0001:0017:FR:PDF.

IV. EXAMEN DES ARTICLES DU PROJET DE LOI

4.1. Informations de localisation pour les services d'urgence (article 64 du projet de loi)

16. L'article 64 du projet de loi modifie l'article 107 de la loi du 13 juin 2005. Un § 1er/1 est inséré dans cet article. Il permet aux opérateurs de collaborer avec des entreprises qui fournissent des réseaux publics de communications électroniques afin de permettre la localisation des utilisateurs qui téléphonent aux services d'urgence, même s'ils téléphonent via un service VoIP nomade[14], c'est-à-dire un service déconnecté du réseau original et qui n'est pas associé à un réseau déterminé (par exemple Skype).

17. Le nouveau projet de loi permet à l'IBPT de déterminer la manière dont cet accès sera octroyé. Il est possible que l'opérateur VoIP soit obligé de collecter des informations sur ses clients, notamment au sujet de leurs informations de localisation exactes, afin de pouvoir remplir leurs obligations.

18. La Commission souligne que l'opérateur VoIP est tenu de respecter l'obligation d'information de l'article 9 de la LVP dans le cadre de cette collecte d'informations au sujet des utilisateurs finaux. Cette collecte d'informations doit avoir pour seul but de procéder à la localisation pour les services d'urgence, et non pour d'autres finalités (pour des services commerciaux par exemple).

4.2. Accès aux données téléphoniques sur la facture détaillée pour la personne concernée qui n'est pas l'abonné (article 67 du projet de loi et article 10 de la LVP)

19. Au niveau des versions spécifiées des factures de base, la Commission se demande si l'abonné qui n'est pas (toujours) l'utilisateur final peut également demander une facture détaillée sans l'accord de l'utilisateur final ou sans en informer ce dernier. La Commission souligne le point de convergence avec le droit d'accès de la personne concernée (article 10

---

[14] On entend ce qui suit par nomadicité : "*caractéristique d'un service de communications électroniques qui permet à ce service d'être utilisé à partir de pratiquement n'importe quelle connexion à un réseau de communications électroniques*" (article 1, 14° de l'arrêté royal du 27 avril 2007 *relatif à la gestion de l'espace de numérotation national et à l'attribution et au retrait des droits d'utilisation de numéros*). Voir la communication relative à l'interprétation du concept "*numéros géographiques nationaux E.164 spécifiques réservés à l'Institut pour une utilisation nomade*", visé à l'article 43, quatrième alinéa de l'arrêté royal du 27 avril 2007 *relatif à la gestion de l'espace de numérotation national et à l'attribution et au retrait des droits d'utilisation de numéros*, M.B. du 5 décembre 2007.

de la LVP) et pense par exemple au scénario fréquent d'un employeur qui paie les factures et qui demande le détail de ces factures. La jurisprudence antérieure à la loi du 13 juin 2005 acceptait souvent la production de telles factures.

20. Le législateur peut peut-être préciser dans l'Exposé des motifs les cas dans lesquels la loi permet à l'abonné qui n'est pas l'utilisateur final de prendre connaissance du détail des factures et, le cas échéant, d'autoriser l'utilisateur final à prendre également connaissance du détail des factures qu'il a indirectement générées mais qu'il n'a pas payées.

21. Enfin, il serait intéressant d'ajouter ce qui suit dans l'en-tête de l'article 110, § 1 de la loi du 13 juin 2005 : "Sans préjudice de l'application de l'article 10 de la loi du 8 décembre 1992 (…)", clarifiant ainsi également le fait que la personne concernée peut toujours accéder à ses données téléphoniques auprès de l'opérateur, même si elle n'est pas l'abonné.

4.3. Compétence complémentaire de l'IBPT concernant la sécurité des réseaux et services (articles 74-76 du projet de loi) et concernant le fait de prendre connaissance des procédures internes des opérateurs pour les demandes d'accès à des données à caractère personnel (article 87 du projet de loi)

22. Les articles 74 à 76 inclus concernent les mesures de sécurité que doivent prendre les entreprises qui offrent des réseaux publics de communications électroniques et les entreprises qui fournissent des services de communications électroniques accessibles au public.

23. Plusieurs compétences sont confiées à l'IBPT pour déterminer les informations à communiquer, les mesures de sécurité à prendre ou pour contrôler les actions des différents acteurs. Comme déjà mentionné au point 3.2.2. ci-avant (complémentarité), il est clair que certaines compétences de l'IBPT découlant du projet de loi peuvent coïncider avec les compétences de la Commission découlant de la LVP, dans la perspective où les deux aspects se rapportent à la sécurité des données à caractère personnel.

24. Ainsi, le nouvel article 113, § 6, 2° permet à l'IBPT de fournir des informations sous une forme normalisée via les entreprises concernant les *"moyens de protection contre les risques d'atteinte à la sécurité individuelle, à la vie privée et aux données à caractère personnel lors de l'utilisation des services de communications électroniques.*"

25. Le nouvel article 113/1, alinéa 2 octroie à l'IBPT la compétence de superviser "*la détection, l'observation et l'analyse des problèmes de sécurité"* et de *"fournir aux utilisateurs des informations en la matière.*"

26. L'article 114, § 2, dernier alinéa prévoit que l'IBPT peut vérifier les mesures prises par les entreprises et peut émettre des recommandations "*sur les meilleures pratiques concernant le degré de sécurité que ces mesures devraient permettre d'atteindre*". On précise que cela vaut "*Sans préjudice de la loi du 8 décembre 1992* (…)".

27. Outre l'intervention de l'IBPT en cas de violation de la sécurité d'un service de communications électroniques accessible au public concernant des données à caractère personnel (voir ci-après), le nouvel article 114/1, § 4 permet à l'IBPT d'adopter des lignes directrices et d'édicter des instructions précisant les circonstances dans lesquelles les entreprises fournissant des services de communications électroniques accessibles au public sont tenues de notifier une violation de données à caractère personnel. Le format applicable à cette notification et son mode de transmission peuvent également être définis dans ce cadre.

28. L'article 87 du projet de loi donne à l'IBPT la compétence de prendre connaissance des procédures internes des opérateurs relatives aux demandes d'accès à des données à caractère personnel (nouvel article 127, § 6 de la loi du 13 juin 2005).

29. Vu la complémentarité de la loi du 13 juin 2005 et de la LVP, la Commission estime que pour toutes les compétences et tous les points de vue de l'IBPT relatifs à la protection des données à caractère personnel (article 16 de la LVP) et à l'exercice du droit d'accès aux données à caractère personnel (article 10 de la LVP), il faudrait tenir compte des points de vue de la Commission, du Groupe 29 et du CEPD en la matière.

30. Comme mentionné ci-avant, une coopération plus étroite entre la Commission et l'IBPT s'impose, ce que pourrait encourager le projet de loi, en prévoyant plus systématiquement l'avis préalable de la Commission lorsque l'IBPT exerce une des compétences réglementaires précitées (type d'information normalisée, lignes directrices, instructions), sans préjudice de la possibilité de formaliser la collaboration via un protocole de coopération pour les autres aspects.

31. La Commission se penche ci-après sur la différence avec la "large obligation de notification" qui introduira une notification à l'égard de toutes les commissions vie privée pour les

violations de la sécurité relatives aux données à caractère personnel, même si elles ne concernent pas un service de communications électroniques accessible au public.

4.4. L'obligation de notification d'une violation de la sécurité d'un service de communications électroniques accessible au public relative à des données à caractère personnel (article 77, § 3 du projet de loi), ci-après "obligation de notification restreinte" – définition de violation de la sécurité d'un service de communications électroniques accessible au public portant sur des données à caractère personnel (article 14, 25° du projet de loi)

32. L'article 77 § 3 du projet de loi dispose ce qui suit "*En cas d'atteinte à la sécurité d'un service de communications électroniques accessible au public en matière de données à caractère personnel, l'entreprise fournissant des services de communications électroniques accessibles au public avertit sans délai*" l'IBPT "*de la violation de données à caractère personnel".*

33. L'article 77, § 3 du projet de loi introduit ce que l'on a coutume d'appeler dans la littérature une "obligation de notification restreinte", ce en complément d'une obligation d'information aux abonnés déjà existante des "*risques particuliers liés à une violation de la sécurité du réseau*"[15]. Les termes "obligation de notification restreinte" réfèrent surtout à la limitation de l'obligation de notification, à savoir l'application restreinte dans le secteur des télécommunications (seule la sécurité d'un service de communications électroniques accessible au public fait l'objet de l'obligation de notification).

34. La Commission constate que le législateur opte pour la possibilité de désigner l'IBPT au lieu de la Commission comme instance à qui il faut adresser la notification. Elle estime qu'il s'agit d'une pondération d'opportunité logique, vu l'expertise existante de l'IBPT, indépendamment de la possibilité, en vertu de la Directive 2009/136/CE, de désigner une commission vie privée en tant qu' "autorité nationale compétente", ce qui était déjà le cas dans certains États membres[16].

35. La Commission demande toutefois au législateur de se pencher sur deux problèmes qu'entraînera le choix de l'IBPT.

---

[15] Article 114 de la loi du 13 juin 2005 (article 4.1. de la Directive 2002/58/CE).

[16] Voir par exemple la France, où il faut procéder à une notification à la CNIL. http://www.cnil.fr/la-cnil/actualite/article/article/transposition-du-paquet-telecom-renforcement-des-droits-des-internautes-et-signalement-des-fail/.

36. Vu la complémentarité de la LVP avec la loi du 13 juin 2005 en ce qui concerne la protection des données à caractère personnel (voir ci-avant), il existe d'ores et déjà un risque de discordance dans l'intervention de deux instances dans la même matière (protection des données à caractère personnel). Pour éviter des contradictions dans les points de vue, il faudra, comme déjà mentionné, une coopération accrue avec l'IBPT.

37. Par ailleurs, il faudra de toute façon tenir compte à plus long terme de la discussion européenne en cours sur la large obligation de notification[17] aux commissions vie privée. Dans la Directive 2009/136/CE, la Commission européenne a déjà expliqué que l'introduction d'une large obligation de notification (c'est-à-dire applicable à tous les secteurs) devait être considérée comme une priorité[18]. Le Groupe 29[19] s'est également prononcé en faveur d'une large obligation de notification.

38. La Commission prie le législateur de considérer d'ores et déjà les éventuels problèmes que pourra poser à terme le maintien en parallèle de la large obligation de notification et de l'obligation de notification restreinte. Bien que la Commission préfère la possibilité d'introduire de concert la large obligation de notification et l'obligation de notification restreinte, le législateur devra veiller à ce que cela se fasse de manière coordonnée (modalités d'obligation de notification analogues). La Commission demande également que le législateur appuie déjà explicitement une collaboration plus étroite entre l'IBPT et la Commission dans la loi du 13 juin 2005.

39. La Commission estime que les modalités de l'obligation de notification restreinte de l'article 77, § 3 ne sont pas encore assez claires. Quoi qu'il en soit, les risques à notifier devront être mieux définis. Tout notifier et traiter ne constitue en effet pas une option ; une formalisation intégrale du processus de notification est contre-productive. La Commission est dès lors favorable à des dispositions d'exécution qui apportent des précisions. Après avis de la Commission, le Roi pourrait fixer les modalités de l'obligation de notification.

---

[17] Voir l'article 31 de la proposition de règlement européen sur la protection des données de la Commission européenne du 25 janvier 2012, publié à l'adresse suivante : http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf.

[18] Considérant 59 de la Directive 2009/136/CE : "*Cependant, la notification des violations de sécurité traduit l'intérêt général des citoyens à être informés des violations de sécurité qui pourraient se traduire par la perte ou la violation de leurs données à caractère personnel, ainsi que des précautions existantes ou souhaitables qu'ils pourraient prendre pour minimiser les pertes économiques ou dommages sociaux éventuels pouvant découler de ces violations. L'intérêt des utilisateurs à être informés ne se limite pas, à l'évidence, au secteur des communications électroniques, et il convient dès lors d'introduire de façon prioritaire, au niveau communautaire, des exigences de notification explicites et obligatoires, applicables à tous les secteurs. Dans l'attente d'un examen, mené par la Commission, de toute la législation communautaire applicable dans ce domaine, la Commission, après consultation du contrôleur européen de la protection des données, devrait prendre les mesures appropriées pour promouvoir, sans retard, l'application, dans l'ensemble de la Communauté, des principes inscrits dans les règles relatives à la notification des violations des données contenues dans la directive 2002/58/CE (directive "vie privée et communications électroniques"), quel que soit le secteur ou le type de données concerné.*"

[19] Page 5 de l'avis suivant : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp159_fr.pdf.

40. La Commission souligne plusieurs éléments positifs dans la transposition de l'article 2, 4, c) de la Directive 2009/136/CE. L'avis du Groupe 29 est ainsi suivi sur un point. Alors que le Groupe 29 plaidait pour une notification immédiate[20], cela s'est traduit par l'expression "sans délai".

41. Par ailleurs, elle s'interroge quant à l'interprétation de "l'exception technique" à l'obligation de notification de l'article 77, § 3[21]. Cette exception revient à dire que si les données à caractère personnel sont codées, il n'y a plus besoin d'une obligation de notification.

42. La Commission rejoint ici le point de vue du Groupe 29, qui s'est prononcé contre cette exception[22] de l'article 4, c) de la Directive 2009/136/CE qui manque totalement l'objectif de l'obligation de notification. La protection ou non de données à caractère personnel au moyen du cryptage ou d'autres méthodes ne constitue qu'une modalité. L'objectif principal de l'obligation de notification est justement de pouvoir informer de manière qualitative et utile la personne concernée s'il y a un risque suffisamment élevé pour ces citoyens. Supposer qu'il n'y a pas de risque si des données à caractère personnel codées sont compromises est une hypothèse erronée et devrait plutôt soulever d'autres questions telles que le mode de codage (end to end ou non), ou le fait de savoir s'il s'agit ou non de données à caractère personnel sensibles au sens de la LVP.

43. Bien que l'article 77, § 3 du projet de loi constitue une transposition littérale de l'article 4, c) de la Directive 2009/136/CE, la Commission est dès lors favorable à un modèle de notification qui se base davantage sur le risque.

4.5 Exceptions supplémentaires au secret des communications et télécommunications privées (articles 86 et 87 du projet de loi)

44. À l'article 125, § 1 de la loi du 13 juin 2005, le projet de loi prévoit deux exceptions supplémentaires à l'interdiction d'intercepter des communications électroniques. Dans la liste des services auxquels ne s'appliquent pas les dispositions de l'article 124 de la loi du 13 juin 2005 et des articles 259*bis* et 314*bis* du Code pénal, on ajoute :

---

[20] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp159_fr.pdf.

[21] "*La notification d'une violation des données à caractère personnel à l'abonné ou au particulier concerné n'est pas nécessaire si le fournisseur a prouvé, à la satisfaction de l'autorité compétente, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation. De telles mesures de protection technologiques rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.*"

[22] Page 7 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp159_fr.pdf : *"Une telle disposition réduirait considérablement la qualité et l'utilité des informations fournies aux personnes concernées. Les utilisateurs touchés ne pourront faire le nécessaire pour réduire les risques auxquels ils sont confrontés que s'ils ont été correctement informés. Par conséquent, le groupe insiste sur l'importance du format de la notification et de l'évaluation des risques pour déterminer si les particuliers doivent être avertis, indépendamment des mesures techniques prises pour protéger leurs données.*"

- exception supplémentaire pour les agents habilités par le Ministre qui a l'Économie dans ses attributions (dans le cadre de leurs missions légales de recherche) ; et
- exception supplémentaire pour les actes de la Commission d'éthique et de son secrétariat (dans le cadre de leurs missions légales de recherche[23]).

45. La Commission n'a pas de remarque particulière quant à ces exceptions supplémentaires, pour autant qu'elles soient fondées sur une base légale claire et soient utilisées pour une mission de recherche spécifique (article 22 de la Constitution et article 8 de la CEDH).

46. La Commission constate que l'actuelle exception pour l'IBPT est adaptée en ce sens : *"4° lorsque les actes sont accomplis par l'Institut sur ordre d'un juge d'instruction et/ou dans le cadre de sa mission générale de surveillance et de contrôle*". On peut se poser diverses questions quant à l'utilité de cette adaptation. Bien que l'intervention d'un juge d'instruction peut certainement être considérée comme une protection renforcée de la vie privée des personnes concernées, la Commission s'interroge quand même sur la formulation imprécise (les termes "et/ou" laissent entendre que l'ordre du juge d'instruction n'est pas nécessaire si l'IBPT agit dans le cadre de sa mission générale). La raison de ne pas imposer une condition similaire ("sur ordre du juge d'instruction") au service de médiation pour les télécommunications (article 125, § 1, 5°) soulève des questions de logique. L'Exposé des motifs ne comporte aucune explication à ce sujet. En outre, les modalités d'une collaboration entre l'IBPT et les juges d'instruction ne sont pas claires, et cette disposition crée une différence dans les différentes procédures administratives.

47. La Commission demande dès lors de supprimer la condition supplémentaire de l'article 88 du projet de loi.

4.6 (Exception à l') exigence de consentement, différents types de cookies et autres formes de stockage ou de consultation d'informations (article 88 du projet de loi)

48. Des logiciels destinés à contrôler secrètement les actes de l'utilisateur ou à influencer le fonctionnement des équipements terminaux de l'utilisateur au profit de tiers ("spyware") constituent, tout comme les virus, une menace grave pour la vie privée de l'utilisateur[24]. L'article 5.3. modifié de la Directive 2002/58/CE a dès lors renforcé la protection des utilisateurs de réseaux électroniques en exigeant le consentement avant que des

[23] Voir les articles 134 et 134/1 de la loi du 13 juin 2005. Les autres réglementations de la Commission d'éthique sont disponibles sur son site Internet http://www.telethicom.be (publications officielles > législation).
[24] Considérant 65 de la Directive 2009/136/CE.

informations telles que les cookies soient enregistrées ou consultées sur les équipements terminaux de l'utilisateur (ou de l'abonné).

49. Ce consentement n'est toutefois pas toujours requis pour toutes les informations enregistrées ou consultées sur les équipements terminaux de l'utilisateur (ou de l'abonné). L'article 5.3. de la Directive 2002/58/CE accepte une exception s'il s'agit d'un des critères suivants (1) s'il s'agit d'un "*stockage ou à un accès techniques visant exclusivement à effectuer ou à faciliter la transmission d'une communication par la voie d'un réseau de communications électroniques*" ou (2) le deuxième critère est "*strictement nécessaires au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur*".

50. Les cookies qui répondent ou non à un des deux critères devraient être définis par le législateur (par exemple dans l'Exposé des motifs). Les travaux préparatoires au sein du Groupe 29 concernant un point de vue quant aux cookies et une étude néerlandaise à la demande de l'OPTA[25] dans un rapport de TNO-IViR indiquent d'ores et déjà que la liste de cookies, pour lesquels aucun consentement n'est requis et impliquant peu de problèmes de vie privée et de protection des données, est assez limitée.

51. Les cookies pour lesquels il y a dispense de l'obligation de consentement sont principalement les cookies "first party"[26] et en majeure partie ceux du type "user input session cookies", c'est-à-dire des cookies placés par l'utilisateur lui-même et qui retiennent des choix linguistiques et préférences personnelles dans un magasin en ligne (par exemple une identification du client et un panier virtuel).

52. Par ailleurs, certains cookies ne sont clairement pas concernés par la dispense de l'obligation d'information. La littérature renvoie aux formes de cookies les plus intrusives et les plus récentes par le biais de diverses dénominations qui sont parfois utilisées simultanément comme "cookies persistants", "flash cookies", "supercookies" et "evercookies"[27]. Les caractéristiques de tels cookies sont inouïes. Il s'agit de cookies qui ne sont clairement pas demandés explicitement par l'utilisateur, qui restent parfois sur les équipements terminaux après les avoir effacés (ce qu'on appelle le respawning[28]), et sont utilisés pour des finalités diverses ou indéterminées. Il s'agit souvent de cookies "third party" faisant

---

[25] http://www.tno.nl/downloads/rapport_opta_35473.pdf.

[26] Si l'éditeur du site Internet place lui-même des cookies, on appelle cela "first party cookie". Voir la page 16 du rapport de TNO-IViR précité.

[27] On trouve une bonne explication de cela à la page 8 du rapport de l'ENISA du 2 février 2011, Bittersweet cookies. Some security and privacy considerations, publié à l'adresse suivante : http://www.enisa.europa.eu/activities/identity-and-trust/library/pp/cookies.

[28] D'après la page 3 du rapport de TNO-IViR, un cookie supprimé (http) est rétabli par un autre cookie (flash).

l'objet de très peu ou d'aucune information de la part des responsables, et qui requièrent une expertise et un logiciel spécifiques pour les supprimer.

53. Tout comme d'autres autorités de protection des données, la Commission constate en la matière un manque de précision à l'article 5.3 modifié de la Directive 2002/58/CE qui est rédigé en des termes très abstraits et techniques, de sorte que la personne non initiée peut difficilement évaluer l'impact de ces dispositions. Selon l'étude susmentionnée de TNO-IViR, il s'avère que très peu d'utilisateurs en savent suffisamment pour pouvoir se protéger efficacement. Bien que le terme "cookies" soit connu, les cookies ne sont pas forcément associés à de la publicité comportementale en ligne ("online behavioural advertising" ou "OBA"), et faire une distinction entre les divers types de cookies et leur utilisation possible dépasse la plupart des utilisateurs. Dans la majorité des cas, l'information sur les cookies avancés et l'établissement de profils s'est avérée inexistante. Les utilisateurs moyens ont également des compétences limitées. Ainsi, pour Monsieur et Madame Tout le Monde, bloquer les cookies flash est tout à fait impossible[29].

54. Le projet de loi et l'Exposé des motifs sont tout aussi imprécis puisqu'ils n'expliquent nulle part de quoi il s'agit concrètement.

55. La Commission estime que l'article 88 du projet de loi est une pure transposition technique du principe de "cookie consent" qu'elle juge, en soi, insuffisante en tant que disposition légale pour délimiter et légitimer efficacement tous les types et formes de cookies (d'intrusions via des cookies) et pour protéger efficacement les personnes concernées.

56. La Commission sollicite l'attention du législateur quant à divers problèmes qui démontrent qu'une telle transposition technique est tout à fait insuffisante pour réaliser la finalité européenne de protection des personnes concernées.

Problème 1 : terminologie

57. La Commission constate qu'en ce qui concerne la terminologie, une discussion européenne est toujours en cours à propos de l'interprétation de notions telles que "équipements terminaux", "cookies", des exceptions à l'exigence de consentement selon le type de cookie et selon les finalités d'utilisation du cookie, de la manière dont le consentement peut être apporté et des autres techniques de stockage et de consultation des informations. Le législateur doit dès lors au moins suivre cette discussion afin de donner un cadre plus

[29] Voir la page 3 de l'étude TNO-IViR susmentionnée.

légal et plus clair aux diverses formes de "consultation des informations" et à la notion d' "équipements terminaux".

58. Un problème typiquement terminologique réside dans le fait que l'article 88 du projet de loi ne parle que d' "abonné ou utilisateur final" alors que la LVP parle toujours de la notion plus large de "personne concernée". La Commission renvoie à nouveau à sa remarque relative à la complémentarité (voir le point 3.2.2. ci-avant). Cela signifie que si l'abonné n'est pas l'utilisateur (par exemple l'employeur en tant qu'abonné), la personne concernée (donc l'utilisateur) doit toujours être informée, éventuellement en plus de l'abonné (sur la base de l'application conjointe de l'article 10 de la LVP et de la loi du 13 juin 2005).

Problème 2 : hypothèses inexactes : le paramétrage du navigateur ne peut pas faire office de consentement, un consentement avec un pop-up gênant et davantage de données à caractère personnel stockées n'est pas requis pour chaque cookie

59. Le problème est également que trop souvent, les représentants des entreprises intéressées partent de suppositions erronées et d'arguments incorrects dans les débats comme la quasi solution de "faire du paramétrage du navigateur par l'utilisateur un élément déterminant dans le contexte de la question de savoir si l'utilisateur a donné le consentement requis pour l'installation et la lecture de cookies"[30]. Les acteurs économiques peuvent toutefois continuer à installer tranquillement des cookies car les trois principaux navigateurs (Internet Explorer de Microsoft, Mozilla Firefox et Google Chrome) ont pour paramétrage standard qu'ils acceptent tous les cookies automatiquement[31]. Les entreprises intéressées donnent également à tort l'idée que pour chaque cookie, un consentement distinct devrait être demandé, ce qui aurait pour conséquence un écran de pop-ups extrêmement gênant. Ce faux argument a néanmoins convaincu le législateur néerlandais qui a affirmé dans l'Exposé des motifs de la loi Télécoms néerlandaise : "*Selon les réactions recueillies, la conséquence est que l'utilisation d'Internet n'est pas conviviale, que dans la pratique, l'utilisateur donnera toujours son consentement sans prendre conscience de l'objet de son consentement et davantage de données à caractère personnel doivent être enregistrées par celui qui est responsable des cookies*" [traduction libre réalisée par le Secrétariat de la Commission, en l'absence d'une traduction officielle]. Il s'agit ici aussi d'une vision tronquée, dès lors que la Directive et l'article 88 du projet de loi ajoutent des exceptions pour lesquelles le consentement n'est pas requis, rendant le consentement limité aux applications les plus intrusives via des cookies (principalement les cookies de tiers) et dans le cadre de

[30] Voir les travaux parlementaires de la loi Télécoms néerlandaise.

[31] Voir la page 2 du courrier du 14 mars 2011 dans lequel le Président du Collège néerlandais de Protection des Données à caractère personnel (College Bescherming Persoonsgegevens), qui est également Président du Groupe 29, réagit contre ces arguments. Voir http://www.cbpweb.nl/downloads_med/med_20110422_cookies_brief.pdf.

l'application normale du droit européen, le nombre de pop-ups gênants diminuera avec le temps[32] (ce qu'on appelle le "processus d'apprentissage" sur la base d'un consentement accordé précédemment, certes pour autant qu'il soit requis).

Problème 3 : des études étrangères indiquent une négligence collective de l'obligation d'information par le secteur et aucune solution ou fausse solution n'est proposée qui n'implique pas de consentement.

60. Il ressort d'une étude aux Pays-Bas[33] et en Angleterre[34] que les entreprises qui installent des cookies négligent collectivement la simple obligation d'information (article 9 de la LVP). Le président néerlandais du College Bescherming Persoonsgegevens a donc réagi vis-à-vis de la Deuxième Chambre : "*Les entreprises intéressées n'ont entrepris aucune initiative au cours des dernières années pour informer les personnes et leur offrir des choix via des "best practices" ou d'autres formes d'autorégulation*" [traduction libre réalisée par le Secrétariat de la Commission, en l'absence d'une traduction officielle].

61. L'étape suivante, le consentement basé sur une information préalable ("informed consent") n'est dès lors pas non plus proposée par les entreprises. Dans la même réaction, le président néerlandais affirme que les entreprises concernées pensent pouvoir se contenter de "constructions opt-out"[35] et d'une icône commune pour remplir l'obligation d'information. Il s'agit d'un problème européen. Il y a une discussion perpétuelle entre les autorités de protection des données européennes[36] d'une part et des représentants de l'industrie de la publicité en ligne[37] (IAB Europe et EASA) d'autre part concernant les "solutions" élaborées jusqu'à présent via une autorégulation relative à l'utilisation de cookies pour la publicité comportementale en ligne ("online behavioural advertising" ou "OBA"). Le Groupe 29 a insisté à cet égard sur l'exigence d'une manifestation concrète de volonté des personnes concernées. En effet, tous les cookies ne sont pas utilisés pour de l'OBA. Mais l'OBA suscite

---

[32] Voir la page 3 du courrier du Groupe 29 d'août 2011, publié http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/20110803_letter_to_oba_annexes.pdf.

[33] Voir le point 5 de la page 5 de l'étude susmentionnée TNO-IViR (http://www.tno.nl/downloads/rapport_opta_35473.pdf) : "Plus de la moitié des parties participant à l'enquête avouent ne pas informer l'utilisateur" [traduction libre réalisée par le Secrétariat de la Commission, en l'absence d'une traduction officielle].

[34] Voir le rapport de l'ENISA du 2 février 2011, Bittersweet cookies. Some security and privacy considerations, publié à l'adresse suivante : http://www.enisa.europa.eu/activities/identity-and-trust/library/pp/cookies.

[35] Axées sur le "IAB Europe OBA Framework". Voir http://www.iabeurope.eu/news/self-regulation-framework.aspx.

[36] Voir l'avis 2/2010 *sur la publicité comportementale en ligne*

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_fr.pdf.

[37] Voir les courriers du Groupe 29 http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/20110803_letter_to_oba_annexes.pdf et http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/20111215_letter_oba_industry_en.pdf concernant notamment la solution de l'icône "i" de l'IAB.

diverses questions parce que plusieurs parties peuvent être impliquées[38], il s'agit d'un profilage[39] extrême des utilisateurs, ce qui rend encore plus prioritaire le traitement efficace de ce type d'utilisation des cookies.

Problème 4 : la responsabilité de l'obligation d'information dans le cadre de l'OBA

62. Vu le grand nombre de parties[40] pouvant être impliquées dans l'utilisation de certains cookies "third party" comme en cas d'OBA, le législateur doit délimiter très clairement sur qui repose l'obligation d'information. Il faut prévoir (par exemple dans la politique en ligne en matière de respect de la vie privée sur la base de l'article 9 de la LVP) plus de transparence vis-à-vis des utilisateurs concernant les conditions de collaboration entre ces parties, informations sur la base desquelles la (co)responsabilité de chacune des parties concernées peut être établie à l'égard des personnes concernées.

63. En vertu des raisons et arguments susmentionnés, la Commission se range derrière l'appel de son homologue néerlandais d'exiger à l'article 88 du projet de loi le consentement ***indubitable*** des utilisateurs et des abonnés pour les cookies les plus intrusifs dans la vie privée (pour être clair, pas pour les cookies pour lesquels la dispense susmentionnée de consentement s'applique).

64. La Commission incite aussi le législateur à permettre des informations complémentaires :

- en faisant référence à la possibilité pour l'IBPT[41] ou le Roi de prendre, après avis de la Commission, une décision sur quel type de cookies peut faire partie des exceptions, avec quelle finalité (utilisation), ce à l'aide des précisions supplémentaires que la Commission attend de l'Europe sur ce point[42] ou des listes de FAQ[43] qui sont rédigées ailleurs par l'instance nationale compétente ;

---

[38] Des éditeurs de sites Internet, des publicitaires, des réseaux de publicité, des fournisseurs de statistiques, … Voir l'enquête néerlandaise publiée sur http://www.tno.nl/downloads/rapport_opta_35473.pdf.

[39] Voir la recommandation CM/Rec(2010)13 du 23 novembre 2010 du *Comité des Ministres aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage*, publiée à l'adresse suivante : https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2010)13&Language=lanFrench&Ver=original&Site=CM&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864# et l'Exposé des motifs publié à l'adresse suivante : https://wcd.coe.int/ViewDoc.jsp?Ref=CM(2010)147&Language=lanFrench&Ver=add3final&Site=CM&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864.

[40] Voir la page 12 de l'avis 02/2010 du Groupe 29 sur la publicité comportementale en ligne, cité en page 15 de l'étude susmentionnée ("destinataires de la norme"), publié à l'adresse suivante : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_fr.pdf. Le Groupe 29 distingue les réseaux de publicité, les publicitaires, les bureaux de médias et les statistiques en ligne.

[41] Voir la compétence analogue de l'IBPT pour déterminer les séries de numéros en matière de communication par téléphone et par SMS.

[42] La Commission s'attend à ce que le Groupe 29 publie en 2012 un avis complémentaire qui précisera le type de cookies qui peut relever de l'exception à l'exigence de consentement.

- en prévoyant de manière similaire la possibilité de définir pour quel type de cookies le consentement est requis ;
- en prévoyant l'obligation d'information complémentaire à l'égard de l'utilisateur et de l'abonné qui, vu la nature spécifique du traitement, est nécessaire pour protéger efficacement la personne concernée (article 9, § 1, d) *in fine* de la LVP), comme des informations claires sur quels types de cookies sont utilisés avec quelles finalités, et de quelle façon on peut principalement supprimer ou bloquer les cookies de tiers, via le navigateur ou par un autre moyen.

65. L'Exposé des motifs de l'article 88 du projet de loi pourrait apporter un peu plus de précisions pratiques en stipulant qu'il s'agit de la réglementation de l'utilisation de cookies (entre autres) sur les ordinateurs personnels et que les paramètres standard des principaux navigateurs ne peuvent à l'heure actuelle impliquer aucun consentement, à moins qu'ils ne refusent et rejettent par défaut les cookies tiers, que l'utilisateur ait le choix d'accepter ou non les cookies au cas par cas, également sur des équipements mobiles, …

4.7. Les conditions pour collecter et publier dans des annuaires des données des abonnés (articles 65 et 115 du projet de loi)

66. Les noms, adresses et numéros de téléphone de personnes physiques sont des données à caractère personnel au sens de la LVP. Leur publication dans un annuaire sur Internet constitue un traitement, ce qui implique l'application de la LVP.

67. Sous le régime de la LVP, un traitement n'est autorisé que dans un certain nombre de cas. Un de ces cas est défini à l'article 5, c) : "*lorsqu'il est nécessaire au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance*". Une telle base légale se retrouve à l'article 45, § 2 de la loi du 13 juin 2005 *relative aux communications électroniques*. Cette disposition prévoit notamment que "*Les personnes qui offrent des services téléphoniques publics aux abonnés mettent les données-abonnés nécessaires à la disposition des personnes qui ont effectué une déclaration* [auprès de l'Institut belge des services postaux et des télécommunications] *(…)*", et ce en vue de distribuer un annuaire.

68. Selon la Directive 2009/136/CE, "*les clients devraient être informés de leurs droits concernant l'utilisation de leurs données à caractère personnel dans des annuaires d'abonnés, et en particulier des fins auxquelles sont établis ces annuaires, ainsi que de leur*

---

[43] Voir par exemple la liste de FAQ de la CNIL et principalement la question n° 4 ("4. Tous les cookies sont-ils concernés ?", publiée sur http://www.cnil.fr/en-savoir-plus/fiches-pratiques/fiche/article/ce-que-le-paquet-telecom-change-pour-les-cookies/).

droit de ne pas figurer dans un annuaire public d'abonnés, et ce gratuitement, conformément à la directive 2002/58/CE (directive "vie privée et communications électroniques"). Les clients devraient aussi être informés quant aux systèmes permettant d'inclure des informations dans la base de données de l'annuaire sans les divulguer auprès des utilisateurs de services d'annuaire[44]." Cette disposition concerne l'article 12 de la Directive 2002/58/CE.

69. En outre, la loi *relative aux communications électroniques* stipule également ce qui suit : "*Sans coût pour les abonnés, les personnes qui offrent des services téléphoniques publics aux abonnés isolent les données relatives aux abonnés qui ont demandé à ne pas figurer dans un annuaire, de manière à ce que ces abonnés puissent recevoir l'annuaire sans que leurs données y figurent*" (article 45, § 3).

70. La Commission estime que le droit de suppression prévu à l'article 12.2 de la Directive 2002/58/CE[45] n'a pas encore été tout à fait transposé en droit belge à l'heure actuelle.

71. Selon la loi du 13 juin 2005, une réglementation spécifique devait prévoir les conditions pour effacer les données de l'annuaire. L'arrêté royal qui devrait fixer ces conditions en exécution de l'article 133, § 2[46] de la loi du 13 juin 2005 n'a toutefois pas encore été adopté de sorte que la réglementation belge ne tient pas encore compte aujourd'hui de la Directive 2009/136/CE. La formulation actuelle de l'article 133, § 2 est également inutilement formaliste (arrêté royal, avis de la Commission et de l'IBPT) et confronte les personnes concernées et la Commission à des problèmes dans divers dossiers, de sorte que certains éditeurs d'annuaires en Belgique pensent actuellement ne devoir donner aucune suite aux demandes de suppression. Les opérateurs renvoient à l'obligation imposée par l'article 45, § 2 de la loi du 13 juin 2005[47].

---

[44] Considérant 33 de la Directive 2009/136/CE.

[45] "*2. Les États membres veillent à ce que les abonnés aient la possibilité de décider si les données à caractère personnel les concernant, et lesquelles de ces données, doivent figurer dans un annuaire public, dans la mesure où ces données sont pertinentes par rapport à la fonction de l'annuaire en question telle qu'elle a été établie par le fournisseur de l'annuaire. Ils font également en sorte que les abonnés puissent vérifier, corriger ou supprimer ces données. La non-inscription dans un annuaire public d'abonnés, la vérification, la correction ou la suppression de données à caractère personnel dans un tel annuaire est gratuite."*

[46] Article 133, § 2 de la loi du 13 juin 2005 : "*Tout abonné a le droit de consulter les données à caractère personnel le concernant conformément aux conditions fixées par ou en vertu de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.*

Tout abonné a en outre le droit de faire corriger ou de faire supprimer gratuitement de l'annuaire ou du service de renseignements téléphonique, les données à caractère personnel le concernant selon les procédures et aux conditions fixées par le Roi après avis de la Commission de la protection de la vie privée et de l'Institut."

[47] Article 45, § 2 de la loi du 13 juin 2005 : "*Les personnes qui offrent des services téléphoniques publics aux abonnés mettent les données-abonnés nécessaires à la disposition des personnes qui ont effectué une déclaration conformément au § 1er, dans des conditions techniques, financières et commerciales équitables, raisonnables et non discriminatoires*."

72. La Commission demande au législateur belge de faire une priorité de la définition des conditions d'effacement des données de l'annuaire. Concrètement, elle demande au législateur d'adapter le dernier alinéa de l'article 133, § 2 de la loi du 13 juin 2005 de manière à ce que la disposition "*selon les procédures et aux conditions fixées par le Roi après avis de la Commission de la protection de la vie privée et de l'Institut*" soit remplacée par "selon la procédure prévue à l'article 12, § 1, dernier alinéa de la loi du 8 décembre 1992".

4.8. Protection de l'utilisateur contre les communications non sollicitées (article 123 du projet de loi)

73. Le projet de loi modifie l'article 100 de la loi du 6 avril 2010 *relative aux pratiques du marché et à la protection du consommateur*. Le but est de transposer l'article 2 de la Directive 2009/136/CE qui modifiait l'article 13 de la Directive 2002/58/CE ("Communications non sollicitées").

74. Selon le nouvel article 13 de la Directive 2002/58/CE, le législateur national doit notamment énumérer clairement, pour les abonnés ou les utilisateurs, les possibilités (notamment en matière d'opt-out) entre le consentement et le droit d'opposition qui s'appliquent dans les cas qui ne relèvent pas des premier et deuxième paragraphes de l'article 13. Dans la pratique, il s'agit surtout de gérer le télémarketing (ce qu'on appelle le "cold calling")[48], dans la mesure où la personne concernée n'est pas cliente.

75. La Commission estime que la manière dont l'article 123 du projet de loi met en œuvre cette mission n'est pas suffisamment claire.

76. Tout d'abord, le législateur doit faire un choix motivé de manière plus claire entre le principe du consentement préalable ("opt-in") ou d'opposition en cas de télémarketing ("opt-out"). Si le législateur choisit ensuite l'opt-out, il doit motiver ce choix. Une possibilité réside dans le fait que l'Exposé des motifs renvoie à l'évolution attendue dans le droit européen de protection des données[49] pour défendre le choix de l'opt-out. Une autre possibilité est que le

[48] En cas d'utilisation d'autres moyens que les systèmes automatisés d'appel, le courrier électronique ou le télécopieur.

[49] Article 19 de la proposition de Règlement européen de protection des données de la Commission européenne du 25 janvier 2012, publiée à l'adresse suivante : http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

législateur renvoie au nombre limité d'États membres[50] qui ont fait le choix de l'opt-in en matière de télémarketing.

77. Si le législateur choisit l'opt-out, il doit également insister davantage sur la qualité de l'information concernant les possibilités d'opposition déjà existantes pour les abonnés et les utilisateurs à l'heure actuelle. Un problème qui ressort des questions et plaintes que la Commission reçoit actuellement concernant cette thématique n'est pas le manque de techniques pour exercer le droit d'opposition mais plutôt le manque d'informations claires fournies aux personnes concernées par les sous-traitants (le call center ou l'agent de télémarketing) et le responsable du traitement au nom de qui la communication est transmise (le publicitaire/le donneur d'ordre) à propos des différentes formes possibles d'opposition.

78. Bien que le projet de loi ne fasse pas mention de la situation où la personne concernée est cliente de l'émetteur, le régime de base en matière de protection des données s'applique ici, notamment le droit d'opposition à l'égard de tous les traitements à des fins de marketing direct (article 12, § 1er, troisième alinéa de la LVP[51]). L'Exposé des motifs pour l'article 123 du projet de loi peut peut-être expliquer cet aspect par souci d'exhaustivité.

79. L'article 123 du projet de loi n'évoque pas du tout non plus un certain nombre de formes d'opposition :

- l'article 123 du projet de loi ne renvoie pas à l'article 12 de la LVP. L'article 14 (b) de la Directive 95/46/CE sur lequel se base cet article contient néanmoins la base juridique générale en Belgique pour le droit d'opposition contre tous les traitements à des fins de marketing direct, même pour les communications électroniques[52]. Il importe de noter que la forme et la technique du droit d'opposition restent ici non définies et que les États membres doivent veiller à que ce que les personnes concernées soient informées de l'existence de ce droit ;
- le droit de ne pas être repris dans les annuaires (voir ci-avant). Actuellement, les personnes concernées s'adressent souvent aux éditeurs d'annuaires et la Commission

[50] En Italie, la commission vie privée a décidé d'instaurer le principe de l'opt-in. En Allemagne, en Autriche, au Portugal (pour le télémarketing vis-à-vis des consommateurs), en Espagne et en Lettonie, l'exigence du consentement pour le télémarketing est également en vigueur.

[51] "*Article 12, § 1er (…)*

Lorsque les données à caractère personnel sont collectées à des fins de direct marketing, la personne concernée peut s'opposer, gratuitement et sans aucune justification, au traitement projeté de données à caractère personnel la concernant. (…)"

[52] Voir les considérants 10 et suivants de la Directive 2002/58/CE.

doit souvent renvoyer ces dernières vers les opérateurs à défaut d'une collaboration des éditeurs d'annuaires ;

- la possibilité de se faire enregistrer dans d'innombrables fichiers repoussoirs et dans des registres "do not call me" dont la liste Robinson Phone de l'Association belge de marketing direct (ci-après "la BDMA") constitue peut-être le registre le plus connu :
- la possibilité pour les personnes concernées de s'inscrire sur d'autres listes que celles de la BDMA (par ex. des associations étrangères, des fichiers repoussoirs d'entreprises, …) ;
- le droit (qui n'est pas transposé en droit belge) pour les personnes concernées de faire supprimer leurs données des annuaires (vu que les annuaires sont souvent utilisés à des fins de télémarketing).

80. En outre, la constitution de ce fichier repoussoir ou "registre de blocage" suscite également de nombreuses questions restées sans réponse comme :

- le législateur instaure-t-il pour les call centers, les agents de télémarketing, les publicitaires et leurs donneurs d'ordre une obligation légale d'utiliser ce registre avant de lancer des actions de télémarketing ? Actuellement, l'utilisation de la liste Robinson Phone n'est pas obligatoire en Belgique (cela s'applique uniquement aux membres de la BDMA), alors qu'un nombre important de pays[53] le prévoient déjà. L'utilisation obligatoire de ce registre pour mettre sur pied une action de télémarketing peut représenter une garantie importante en cas de plainte de la personne concernée, si des professionnels supportent une grande part de la charge de la preuve car ils doivent pouvoir prouver qu'ils utilisent le fichier repoussoir dans leurs actions de marketing ;
- quelles sont les garanties de gestion neutre du registre "do not call me" ? Ce n'est pas un hasard si dans de nombreux États membres, ce registre est placé sous gestion indépendante[54] ou même sous gestion de l'autorité publique[55], les coûts devant être supportés par les utilisateurs professionnels (les call centers ou les agents de

---

[53] Le Danemark, le Royaume-Uni, la Hongrie, la Norvège, l'Autriche, la Suède, l'Irlande. Dans les pays anglo-saxons aussi, il s'agit d'une obligation établie pour les communications aux consommateurs (l'Australie, le Canada, la Nouvelle-Zélande et les États-Unis). Source : http://ddma.nl/wp-content/uploads/2011/04/TMBlokkaderegisters09.pdf.

[54] Aux Pays-Bas, la fondation "Infofilter" (https://www.bel-me-niet.nl/) est le gestionnaire légal désigné du registre "Bel-me-niet".

[55] En Italie, le registre d'opposition pour le télémarketing (http://www.registrodelleopposizioni.it/) a été créé par la "*Fondazione Ugo Bordoni*", une institution qui travaille sous le contrôle du Ministère du développement économique.

En Islande, en vertu de l'article 28(2) de la loi vie privée islandaise, le bureau statistique d'Islande gère ce registre. Au Danemark, les citoyens peuvent officiellement faire enregistrer leurs préférences concernant le marketing direct auprès de la commune dans le système civil d'enregistrement (voir la section 29, point (3) de la loi danoise en matière de système civil d'enregistrement, à consulter à l'adresse suivante : http://www.cpr.dk/cpr/site.aspx?p=194&ArticleID=4326). D'autres pays quant à eux (par ex. le Portugal) ont une liste de type "Robinson" organisée par un groupement d'intérêt du secteur du marketing direct.

télémarketing, les publicitaires/les donneurs d'ordre) via un système de licence[56]. La question est de savoir si le législateur a d'abord envisagé ces options, comme la mise en place de ce registre au sein de l'IBPT, le médiateur télécoms ou une ASBL sous le contrôle indépendant des pouvoirs publics. Une indépendance structurelle vis-à-vis du secteur du marketing direct présente assurément des avantages en matière de gestion indépendante et de communication correcte concernant toutes les possibilités d'opposition et leur base juridique (article 12 de la LVP) ;

- en cas de gestion privée par un groupement d'intérêt du secteur du marketing direct, la question est de savoir s'il y a une gestion interne distincte au sein de cette organisation (ce qu'on appelle les "Chinese walls") ou si, au contraire, le registre est géré par des personnes ayant une tâche journalière fixe dans le secteur du marketing direct. Il faut également savoir si la communication vis-à-vis des personnes concernées est claire ou compliquée, neutre ou tendancieuse, s'il y a un site Internet distinct et clair pour le registre, … ;
- qu'en est-il des moyens mis en œuvre et de la qualité des données ? Le service de gestion est-il uniquement joignable par voie électronique ou également via d'autres canaux ?
- ce nouveau registre "do not call me" sera-t-il simplement une reprise du registre "Robinson Phone" existant, géré par la BDMA ou un nouveau fichier sera-t-il créé avec les mêmes ou de nouvelles caractéristiques et limitations, y a-t-il un règlement transitoire, etc. ?
- quelles caractéristiques et limitations aura ce registre ? Y a-t-il une limitation dans la durée en matière d'inscription[57] ou l'inscription est-elle permanente ? À l'étranger, on a choisi d'intégrer plusieurs limitations. Dans le registre néerlandais "bel-me-niet", la limitation sert à protéger le consommateur du marketing (pas le marketing "b2b") et il existe un système à la carte ou système de blocage partiel dans lequel les consommateurs peuvent cocher ou décocher certaines options selon leur préférence, comme lorsqu'on souhaite encore être contacté pour des propositions commerciales, non commerciales ou caritatives, plutôt que d'instaurer un blocage téléphonique total pour de tels appels ou des blocages partiels pour certains types de communications non sollicitées ;
- une obligation de notification est-elle d'application en cas de violation de la sécurité au niveau de ce registre ? Si oui, à quelle instance (SPF Économie, IBPT, Commission, …) faut-il s'adresser ?

---

[56] Voir les explications relatives aux tarifs et aux conditions à l'adresse suivante : https://www.bel-me-niet.nl/faq/3.

[57] Auparavant, une limitation de trois ans s'appliquait dans le cadre de la liste Robinson Phone. Cette limitation serait supprimée entre-temps.

- quelles sont les mesures en matière de cohérence avec d'autres sources au niveau national, européen et international, compte tenu du fait que le respect du droit d'opposition dans les États membres peut différer fortement ? La personne concernée est-elle renvoyée vers l'enregistrement de ses données dans des sources similaires (modèle réactif où le service du gestionnaire est minimal) ou le gestionnaire professionnel responsable prend-il lui-même l'initiative (modèle proactif où le gestionnaire aide la personne concernée et intervient éventuellement en tant que conciliateur) ?

81. La Commission ne souhaite pas *a priori* se prononcer pour ou contre la mise en place d'un registre "do not call me" entre les mains d'une organisation privée ou de droit public (par ex. au sein de la BDMA ou de l'IBPT), étant donné qu'elle estime qu'il s'agit d'un choix d'opportunité. Elle juge plus opportun que le législateur accorde d'abord et surtout de l'attention aux garanties efficaces que chaque registre d'opposition reconnu comme officiel doit offrir en matière de gestion neutre et de communication, en plus des nombreuses alternatives similaires nationales et étrangères pour les personnes concernées.

82. La Commission demande dès lors que l'article 123 du projet de loi (le passage concernant la modification de l'article 100, § 3 de la loi du 6 avril 2010) soit réécrit. Elle demande que la disposition "*un registre tenu par la Belgian Direct Marketing Association dont le numéro d'entreprise est le 0452.664.950*" soit supprimée. Elle demande aussi que la disposition soit complétée par "Le Roi détermine par arrêté délibéré en conseil des ministres et après avis de la Commission, l'identité du gestionnaire, les exigences et caractéristiques de la gestion du registre, l'accès au registre, les exceptions à l'utilisation obligatoire du registre, l'administration, les moyens et le fonctionnement du registre, ainsi que les mesures pour assurer la transparence du registre vis-à-vis des utilisateurs. Le registre traite les données conformément aux exigences de la loi du 8 décembre 1992 et le gestionnaire fait rapport annuellement sur son fonctionnement."

V. DÉCISION

Le projet de loi et le droit belge ne parviennent pas encore, sur certains points, à transposer correctement, d'un point de vue technique, le droit à la protection des données européen en matière de communications électroniques (droit de suppression des annuaires, diverses options en matière de télémarketing, …).

Ce sont surtout la complexité de la législation en matière de communications électroniques et la technique sous-jacente complexe qui se dégagent, ainsi que la complexité engendrée par la complémentarité de la LVP vis-à-vis de la loi du 13 juin 2005 (terminologie et points de convergence dans les compétences de l'IBPT et de la Commission en matière de sécurité, d'obligation de notification pour les violations de la sécurité et droit d'accès).

Cette complexité est de nature à compliquer l'exercice des droits des personnes concernées. Pour la plupart des utilisateurs, l'infrastructure d'Internet et les flux de données en matière de marketing direct et d'annuaires sont majoritairement invisibles. L'expérience de l'utilisateur est souvent limitée et commence et se termine souvent au point final (sur les équipements terminaux ou lors d'un appel téléphonique commercial). Pourtant, la plupart des risques relatifs aux données à caractère personnel se situent au niveau de la technologie et de l'infrastructure et de l'utilisation en arrière-plan des équipements terminaux ou des usages dans le monde professionnel.

L'absence d'une communication claire et concrète par les acteurs économiques privés, conformément au droit européen sur les techniques utilisées, les finalités et les possibilités de la personne concernée empêche une bonne compréhension de la plupart des utilisateurs du fonctionnement et de l'impact de formes plus complexes d'usage de différentes sortes de cookies, Deep Packet Inspection, publicité comportementale en ligne, … Des recherches montrent que le respect de l'obligation d'information est collectivement négligé actuellement, alors qu'à l'aide de ces techniques, un nombre indéterminé d'instances suivent de manière intensive le comportement de navigation sur plusieurs sites Internet et établissent automatiquement le profil des utilisateurs dans certaines catégories. Des décisions automatiques sur la base de tels intérêts supposés et d'un comportement prétendu peuvent conduire à ce que les utilisateurs soient traités, dans le contexte d'échanges commerciaux ou en dehors, autrement que d'autres ou même qu'ils soient exclus de certains produits ou services, alors que le secteur néglige de fournir une information de base plus claire et de procéder à une transposition effective de l'exigence de consentement.

Le projet de loi et l'Exposé des motifs doivent dès lors accorder une priorité claire à une communication plus claire sur ces éléments complexes aux personnes concernées, aux garanties effectives (le consentement indubitable pour les cookies les plus intrusifs en matière de vie privée qui contournent les navigateurs, un registre d'opt-out de qualité qui doit être obligatoirement utilisé lors d'actions de télémarketing, …) et à l'objectif d'une meilleure collaboration entre la Commission et l'IBPT, une cohérence dans l'application de la LVP et de la loi du 13 juin 2005.

PAR CES MOTIFS,

la Commission de la protection de la vie privée émet un avis favorable sur le projet de loi, sous réserve du respect des remarques mentionnées dans le présent avis et dans la décision.

Vu la matière complexe et son importance, la Commission se tient à disposition pour toute éventuelle concertation ultérieure, révision et/ou exécution des dispositions du projet de loi.

L'Administrateur ff, Le Président,

(sé) Patrick Van Wouwe (sé) Willem Debeuckelaere