

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

La fin de l'anonymat des cartes SIM prépayées

Lognoul, Michaël; Laes, Alexis

Published in:

Revue du droit des industries de réseau (RDIR)

Publication date:

2018

Document Version

le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

Lognoul, M & Laes, A 2018, 'La fin de l'anonymat des cartes SIM prépayées', *Revue du droit des industries de réseau (RDIR)*, numéro 2017/2-3, pp. 198-205.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

La fin de l'anonymat des cartes mobiles prépayées

Alexis LAES

Avocat au Barreau de Bruxelles

Michael LOGNOUL

Assistant à la Faculté de droit de l'Unamur et chercheur au CRIDS¹

TABLE DES MATIÈRES

Modifications apportées à l'article 127 de la LCE	199
L'arrêté royal d'exécution du 27 novembre 2016	200
Modifications apportées à l'article 16/2 de la LSRS	202
Conclusion	202

En Belgique, jusqu'à l'adoption de la loi du 1^{er} septembre 2016² et de son arrêté royal d'exécution du 27 novembre 2016³, il était possible d'acheter, d'activer et d'utiliser des cartes mobiles prépayées en tout anonymat.

Lors de l'adoption de la loi du 13 juin 2005 relative aux communications électroniques (LCE), le législateur avait en effet prévu une dérogation, pour les services de communications électroniques mobiles fournis sur la base d'une carte prépayée, à l'interdiction faite aux opérateurs d'offrir des services qui rendent difficile ou impossible l'identification de l'appelant (art. 127, § 3, de la LCE).

Cette dérogation, qui avait été justifiée par la nécessité de prévoir un régime transitoire afin de ne pas rendre la téléphonie mobile prépayée illégale du jour au lendemain (ce qui aurait eu pour effet d'entraver la pénétration de la téléphonie mobile en Belgique)⁴, n'avait pas vocation à durer puisque le législateur avait prévu que celle-ci serait abrogée lors de l'entrée en vigueur d'un arrêté royal fixant les modalités de l'identification des utilisateurs finals de cartes prépayées.

L'adoption d'une telle mesure a été une revendication de longue date des autorités judiciaires et des services de renseignement et de sécurité (depuis la fin des années nonante) étant donné que l'utilisation de cartes prépayées s'est largement répandue dans les milieux criminels en raison de l'anonymat qu'elle procure⁵.

Un tel anonymat compliquait en effet considérablement la mission de ces autorités dès lors que l'identification de l'utilisateur d'un service de communications électroniques constitue la première étape à franchir avant de pouvoir procéder, le cas échéant, à d'autres mesures d'enquête. Sans identification, ces autres mesures d'enquête perdaient dès lors une grande partie de leur utilité⁶.

Ainsi, en pratique, afin de pouvoir tout de même identifier l'utilisateur anonyme d'une carte prépayée, les autorités se voyaient contraintes de recourir à des techniques d'identification indirectes⁷, lesquelles s'avéraient non seulement plus longues et plus coûteuses mais également plus intrusives dans la vie privée qu'une simple identification lors de l'achat d'une carte prépayée⁸.

Ce n'est finalement qu'à la suite des attentats de Paris du 13 novembre 2015 que le Gouvernement a décidé, parmi les dix-huit mesures édictées pour lutter contre le terrorisme, la suppression de l'anonymat des cartes prépayées.

Pour atteindre cet objectif, le législateur a ainsi modifié l'article 127 de la LCE qui pose les principes en matière d'identification des utilisateurs finals de services de communications électroniques. Un arrêté royal d'exécution fixant les modalités de l'identification des utilisateurs finals de cartes prépayées a également été adopté. Enfin, des modifications ont également été apportées à l'article 16/2 de la loi organique des services de renseignement et de sécurité du 30 novembre 1998 (LSRS) afin de permettre à ces services de requérir le concours des banques et institutions financières pour procéder à l'identification des utilisateurs finals de cartes prépayées.

1. Les auteurs s'expriment à titre personnel et n'engagent pas les institutions auxquelles ils appartiennent. Ils remercient Pierre-Olivier de Broux pour ses commentaires pertinents.
2. Loi du 1^{er} septembre 2016 portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, *M.B.*, 7 décembre 2016.
3. Arrêté royal du 27 novembre 2016 relatif à l'identification de l'utilisateur final de services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée, *M.B.*, 7 décembre 2016.
4. *Doc. parl.*, Chambre, sess. 2004-2005, législature 51, doc. n^{os} 1425/001 et 1426/001, pp. 78 et 79.
5. *Doc. parl.*, Chambre, sess. 2015-2016, législature 54, doc. n^o 1964/001, p. 5.
6. *Ibid.*
7. De telles méthodes indirectes d'identification consistent à enquêter sur une carte prépayée en procédant par recoupement : analyse des numéros appelés à partir de cette carte prépayée, analyse des lieux à partir desquels les appels ont été émis (triangulation) et analyse des terminaux utilisés pour émettre lesdits appels (à partir des traces laissées par ces terminaux sur les réseaux).
8. *Doc. parl.*, Chambre, sess. 2015-2016, législature 54, doc. n^o 1964/001, p. 5.

Modifications apportées à l'article 127 de la LCE

Bien que la loi du 1^{er} septembre 2016 ait été adoptée pour mettre fin à l'anonymat des cartes mobiles prépayées, seule l'une de ses dispositions modificatives de l'article 127 de la LCE vise spécifiquement les services de communications électroniques mobiles fournis sur la base d'une carte prépayée, les autres modifications étant applicables à l'ensemble des services de communications électroniques⁹.

La modification relative aux services mobiles fournis sur la base d'une carte prépayée est contenue à l'article 127, § 3, de la LCE. Conformément au prescrit de cette disposition, la dérogation permettant l'anonymat des cartes prépayées a été abrogée à compter du 17 décembre 2016, date de l'entrée en vigueur de l'arrêté royal du 27 novembre 2016.

Concrètement, ceci signifie que les « nouvelles cartes prépayées » (c'est-à-dire celles qui ont été vendues à compter du 17 décembre 2016) sont donc soumises, d'une part, aux principes posés par l'article 127 de la LCE en matière d'identification des utilisateurs finals à l'instar des autres services de communications électroniques et, d'autre part, au régime d'identification spécifique mis en place par l'arrêté royal du 27 novembre 2016.

Pour les « anciennes cartes prépayées » (c'est-à-dire celles qui ont été vendues avant le 17 décembre 2016), un régime transitoire a été mis en place par l'article 127, § 3, alinéa 2, de la LCE : les utilisateurs finals non identifiés sont tenus de s'identifier dans le délai fixé par leur opérateur ou fournisseur, ce délai ne pouvant excéder six mois à partir de la publication de l'arrêté royal du 27 novembre 2016 (c'est-à-dire au plus tard le 7 juin 2017). À défaut de respecter ce délai, l'utilisateur final sera déconnecté du réseau sans indemnité (art. 127, § 5, LCE).

Il est nécessaire de préciser ici que puisque l'arrêté royal du 27 novembre 2016 n'a vocation à s'appliquer qu'aux services de communications électroniques mobiles fournis sur la base d'une carte prépayée, et puisqu'aucun pendant à ce texte réglementaire

n'existe dans l'ordre juridique belge à l'égard des autres services de communications électroniques¹⁰, les opérateurs et fournisseurs de ces autres services ne sont quant à eux pas tenus de suivre un régime d'identification spécifique similaire en ce qui concerne leurs utilisateurs finals (voir *infra*).

Les autres modifications apportées à l'article 127 de la LCE par la loi du 1^{er} septembre 2016 s'appliquent en revanche à l'ensemble des services de communications électroniques.

Premièrement, le champ d'application *ratione personae* de l'article 127 de la LCE a été élargi, incluant désormais les « canaux de vente de services de communications électroniques »¹¹ et les « entreprises fournissant un service d'identification »¹².

Deuxièmement, l'article 127, § 1^{er}, alinéa 2, de la LCE prévoit dorénavant que l'opérateur ou le fournisseur visé à l'article 126, § 1^{er}, alinéa 1^{er}, de la LCE¹³ est le responsable du traitement au sens de la loi vie privée du 8 décembre 1992¹⁴, qui sera remplacée en ses dispositions pertinentes par le Règlement général sur la protection des données lorsque celui-ci deviendra intégralement et directement applicable¹⁵.

Troisièmement, l'article 127, § 1^{er}, alinéa 3, de la LCE établit une présomption réfragable selon laquelle la personne identifiée est en principe l'utilisateur effectif du service de communications électroniques, et ce afin d'éviter qu'une personne ne s'identifie à la place de l'utilisateur réel et effectif du service pour cacher l'identité de ce dernier.

Quatrièmement, l'article 127, § 1^{er}, alinéas 4 à 8, de la LCE énumère une série de principes relatifs à la collecte et à la conservation des informations qui permettent l'identification de l'utilisateur final.

La loi ne prévoit pas quels sont les données et documents d'identification qui doivent être collectés, lesquels ont été déterminés par l'arrêté royal du 27 novembre 2016. La loi se limite à préciser que le numéro de registre national doit être collecté dans certaines circonstances, faisant en cela suite à l'avis y relatif rendu par la Commission pour la protection de la vie privée¹⁶.

9. *Ibid.*, p. 6.

10. IBPT, FAQ de l'IBPT sur les obligations des opérateurs en matière d'identification des utilisateurs finals de services de communications électroniques accessibles au public, 17 avril 2014, p. 1, disponibles à l'adresse suivante : www.bipt.be/public/files/fr/21251/FAQ_FR.pdf.

11. Cette notion vise non seulement les magasins des opérateurs mais également les canaux de vente indépendants, tels que les supermarchés, les librairies, les épiceries et les *night shops* (Doc. parl., Chambre, sess. 2015-2016, législature 54, doc n° 1964/001, p. 8 ; Doc. parl., Chambre, sess. 2015-2016, législature 54, doc n° 1964/002, p. 3).

12. Cette appellation recouvre, selon le Rapport au Roi de l'arrêté royal du 27 novembre 2016, les entreprises qui sont « tiers par rapport à l'utilisateur final, au point de vente et à l'entreprise concernée, qui entrent en contact avec l'utilisateur final et qui récoltent l'identité de ce dernier et la fournissent à l'entreprise concernée ».

13. C'est-à-dire les personnes qui fournissent au public des services de téléphonie, en ce compris par internet, d'accès à l'internet, de courrier électronique par internet, mais qui ne doivent pas se notifier comme opérateurs à l'IBPT.

14. La désignation du responsable du traitement au sens de la loi vie privée du 8 décembre 1992, par le texte de l'article 127 de la LCE, découle de l'avis rendu par la Commission pour la protection de la vie privée n° 54/2015 du 16 décembre 2015, point 10, p. 4.

15. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, J.O.U.E., 4 mai 2016, L 119, pp. 1 à 88. Conformément à son article 99.2, le Règlement (UE) 2016/679 sera applicable à compter du 25 mai 2018.

16. Avis de la Commission pour la protection de la vie privée n° 54/2015 du 16 décembre 2015, points 16 et 17, p. 6.

Pour la conservation des données, la loi établit une distinction entre les prestataires en fonction de leur rôle dans la chaîne de distribution du service.

S'agissant des canaux de vente, le principe est que ceux-ci ne conservent en principe pas de données ou de documents d'identification. Pour ce faire, la méthode préconisée par les travaux préparatoires est que les canaux de vente introduisent directement les données ou documents d'identification dans les services informatiques de l'opérateur, du fournisseur visé à l'article 126, § 1^{er}, alinéa 1^{er}, de la LCE ou de l'entreprise fournissant le service d'identification, sans devoir dès lors faire une copie de ces données ou documents¹⁷.

Ce n'est que dans l'hypothèse où une telle introduction directe n'est pas possible pour des raisons techniques (par exemple une panne dans les services informatiques) que les canaux de vente sont habilités à faire une copie du document d'identification, en ce compris la carte d'identité électronique belge. Cette copie devra toutefois être détruite au plus tard après l'activation du service de communications électroniques.

S'agissant de l'opérateur, du fournisseur visé à l'article 126, § 1^{er}, alinéa 1^{er}, de la LCE ou de leur sous-traitant (par exemple le fournisseur du service d'identification), la loi prévoit que ceux-ci sont tenus de conserver une copie des documents d'identification autres que la carte d'identité électronique belge (comme par exemple un passeport). Les travaux préparatoires de la loi justifient la conservation de ces autres documents pour deux raisons¹⁸. D'une part, étant donné que ces documents sont davantage susceptibles d'être falsifiés que la carte d'identité électronique, une copie de ceux-ci constituera généralement une piste pouvant permettre aux autorités de retrouver l'auteur du document falsifié. D'autre part, dès lors que ces documents ne peuvent en général pas être lus de manière électronique, une copie de ceux-ci permettra de vérifier s'il n'y a pas eu d'erreur lors de l'encodage de l'identité de l'utilisateur final dans les systèmes informatiques.

Enfin, la loi prévoit que les données et documents d'identification doivent être conservés conformément au prescrit de l'article 126, § 3, alinéa 1^{er}, de la LCE, qui régit la durée de conservation des données d'identification (douze mois à compter de la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé). Les travaux préparatoires de la loi précisent toutefois que les données d'identification conservées en vertu de

l'article 127 de la LCE sont soumises à l'ensemble des règles applicables à la conservation des données prévues par l'article 126 de la LCE, comme notamment celles relatives à l'accès aux données par la Cellule de coordination de l'opérateur ou encore à la liste exhaustive des autorités qui peuvent avoir accès aux données¹⁹.

L'arrêté royal d'exécution du 27 novembre 2016

L'arrêté royal d'exécution du 27 novembre 2016 (ci-après l'A.R.) met en place le régime concret d'identification des utilisateurs finals de cartes prépayées. Pour ce faire, l'A.R. impose des obligations spécifiques non seulement à l'utilisateur final mais également à l'« entreprise concernée »²⁰, au canal de vente et au fournisseur de service d'identification.

Premièrement, en ce qui concerne les utilisateurs finals, l'A.R. leur impose une obligation de collaboration en vertu de laquelle ces derniers sont tenus de s'identifier à la demande de leur opérateur ou fournisseur. Cette obligation de collaboration dans leur chef se décline aussi par le biais de l'obligation de notifier à leur opérateur ou fournisseur tout vol ou perte de leur carte prépayée, et ce dans un délai de vingt-quatre heures (art. 6).

L'A.R. établit également un régime limitant les hypothèses de cessions de cartes prépayées entre personnes physiques au cadre de la sphère familiale, sans quoi une nouvelle obligation de collaboration s'impose au cessionnaire. Dans un tel cas, ce dernier devra en effet procéder de sa propre initiative à son identification préalable auprès de l'entreprise concernée (art. 5).

Le même article dispose que les personnes morales qui attribuent des cartes prépayées à des personnes physiques effectuant des prestations pour leur compte (par exemple une société qui attribue des cartes prépayées à ses employés) sont également tenues à une obligation de collaboration consistant à conserver une liste actualisée faisant le lien entre ces cartes prépayées et lesdites personnes physiques.

Deuxièmement, s'agissant des entreprises concernées, l'A.R. leur impose l'obligation d'identifier leurs utilisateurs finals.

Pour les nouvelles cartes prépayées, l'article 7 de l'A.R. soumet l'activation de toute carte prépayée – et donc du service de communications électroniques

17. *Doc. parl.*, Chambre, sess. 2015-2016, législature 54, doc n° 1964/001, p. 10.

18. *Ibid.*, p. 11.

19. *Ibid.*, p. 12.

20. Cette notion est définie à l'article 2, 2°, de l'A.R. comme « l'opérateur ou l'entreprise étrangère visée à l'article 126, § 1^{er}, alinéa 1^{er}, de la loi, qui fournit à l'utilisateur final un service de communications électroniques publics mobiles sur la base d'une carte prépayée ».

mobiles y afférent – à l'identification de l'utilisateur final concerné au moyen d'une méthode d'identification valide.

En revanche, pour les anciennes cartes prépayées, les entreprises concernées disposent d'un délai maximal de six mois à compter de la publication de l'A.R. pour procéder à l'identification des utilisateurs finals non identifiés (c'est-à-dire au plus tard le 7 juin 2017), conformément au prescrit de l'article 127, § 3, alinéa 2, de la LCE examiné plus haut. Les entreprises concernées peuvent toutefois décider en interne de fixer un délai plus court. Quoi qu'il en soit, la sanction applicable aux utilisateurs finals en cas de non-respect de cette obligation reste la même : la déconnexion du réseau sans indemnité.

Dans un cas comme dans l'autre, l'A.R. institue l'obligation de rendre inutilisable toute carte prépayée qui aurait été notifiée comme volée ou perdue (art. 8).

Troisièmement, l'A.R. prévoit les différentes méthodes valides pour procéder à l'identification des utilisateurs finals (art. 14 à 19). Le texte précise également que la mise en œuvre d'une seule de ces méthodes par une entreprise concernée est suffisante (art. 13). Celles-ci sont :

- la vérification sur la base d'un document d'identification en présence de l'utilisateur final (art. 14) ;
- l'identification en ligne et la signature électronique par la carte d'identité électronique auprès de l'entreprise concernée (art. 15) ;
- la collaboration de fournisseurs de services d'identification (art. 16) ;
- l'extension ou la migration de produit (art. 18)²¹ ;
- la vérification par un moyen de communication électronique (art. 19)²² ;
- l'opération de paiement en ligne (art. 17)²³.

Pour l'application de la première des méthodes d'identification listées ci-avant, l'information d'identification minimale collectée est le numéro de registre national, en ce qui concerne les personnes physiques présentant un document d'identification belge. Les personnes morales, quant à elles, voient à tout le moins leur numéro d'identification de la Banque-carrefour²⁴ collecté.

Dans le même sens, la seconde de ces méthodes d'identification prévoit une obligation de collecte identique, à ceci près que les personnes morales n'y sont logiquement pas prises en compte.

En outre, dans ces deux premiers cas, lorsque le document utilisé pour s'identifier est une carte d'identité électronique belge, les opérateurs ou fournisseurs concernés sont tenus de vérifier que les « *documents d'identification valides* » le sont effectivement, tant *a priori* qu'*a posteriori* (art. 11).

Par ailleurs, en ce qui concerne les trois premières méthodes, et afin d'assurer au mieux le respect de la vie privée des utilisateurs finals en respectant (dans une certaine mesure) le principe de proportionnalité issu de la loi vie privée du 8 décembre 1992, l'A.R. prévoit en son article 10 que les différents intervenants en contact avec l'utilisateur final auront la possibilité de prélever plus d'informations à caractère personnel qu'il n'est strictement nécessaire – par exemple, ces intervenants pourront scanner une carte d'identité au complet, photo incluse et ce, dans le but d'éviter des problèmes organisationnels liés au fait de cacher certaines informations avant le scan – à la stricte condition que les informations superflues soient détruites avant l'activation de la carte prépayée.

Ainsi, seuls les organes étatiques compétents pourront retrouver lesdites informations dans leurs bases de données grâce aux données d'identification collectées conformément au texte de l'A.R., sans que celles-ci ne tombent entre les mains d'entreprises privées sous couvert d'une obligation légale.

Les informations à caractère personnel superflues dont il est ici question sont celles qui ne figurent pas sur la liste exhaustive des données pouvant faire l'objet de l'obligation de conservation conformément au prescrit de l'article 12 de l'A.R., auquel il est renvoyé pour le surplus. Il convient d'ajouter que cette liste est, plus largement, d'application pour chacune des méthodes d'identification instaurées par l'A.R.

Quatrièmement, un régime transitoire spécifique est prévu pour les cartes prépayées qui auraient été activées et distribuées aux canaux de vente des entreprises concernées avant l'entrée en vigueur de l'arrêté royal, mais vendues aux utilisateurs finals après cette même entrée en vigueur sans identification préalable, lorsque lesdites entreprises n'ont pas pu les désactiver avant leur vente finale pour des raisons techniques (art. 20). Dans un tel cas, l'entrée en vigueur de l'A.R. fait courir un délai de trois semaines, au bout duquel l'obligation d'identification des utilisateurs finals jouissant des cartes prépayées dont question entre à son tour en vigueur. Les cartes prépayées qui auraient

21. Cette extension ou migration doit se faire au sein de l'entreprise concernée, de telle sorte que cette dernière dispose au préalable des informations d'identification de l'utilisateur final soumis à l'obligation de s'identifier. Il est dès lors à la charge de l'entreprise de vérifier la véracité de l'extension ou de la migration, c'est-à-dire de s'assurer qu'il s'agit effectivement de l'individu identifié au préalable qui utilise la carte SIM prépayée.

22. L'utilisation de cette méthode implique la communication par canal électronique (formulaire en ligne, SMS, ...) de certaines données d'identification minimales à l'entreprise concernée par l'utilisateur final, qui seront contrôlées grâce à un outil de vérification de l'identité.

23. Ce type de méthode d'identification ne peut toutefois être utilisé que si le prestataire de services de paiement impliqué est soumis à loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, *M.B.*, 9 février 1993.

24. Il s'agit de la Banque-carrefour de la sécurité sociale, telle qu'instituée par la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, *M.B.*, 22 février 1990.

été vendues durant ces trois semaines devront quant à elles faire l'objet d'une identification de leur utilisateur final « *au plus tard le premier jour du mois qui suit l'expiration d'un délai de 6 mois prenant cours le jour suivant la publication du présent arrêté au Moniteur belge* », ce qui devrait correspondre au 1^{er} juillet 2017 au plus tard²⁵.

Comme mentionné ci-dessus, il n'existe pas d'équivalent à cet A.R. en ce qui concerne les opérateurs et fournisseurs de services de communications électroniques autres que ceux fournissant des services de communications électroniques mobiles sur la base d'une carte prépayée. Tant la liste exhaustive des données à caractère personnel qui peuvent être prélevées auprès de l'utilisateur final lors de son identification, à des fins de conservation, que la liste des méthodes valides d'identification pouvant être mises en œuvre pour atteindre cet objectif ne leur sont donc pas applicables²⁶.

Cela leur confère dès lors une plus grande latitude en ce qui concerne les méthodes pouvant être mises en œuvre afin de respecter le prescrit de l'article 127 de la LCE pour l'identification de leurs utilisateurs finals²⁷, ce qui peut poser question au regard du respect de la vie privée et du principe de l'égalité de traitement entre les différentes catégories d'utilisateurs finals de services de communications électroniques accessibles au public.

Ces autres opérateurs et fournisseurs doivent néanmoins respecter les dispositions de la loi vie privée du 8 décembre 1992 qui leur sont applicables (art. 127, § 1^{er}, al. 2, de la LCE), lesquelles seront remplacées par les dispositions pertinentes du Règlement général sur la protection des données lorsque celui-ci deviendra applicable.

Modifications apportées à l'article 16/2 de la LSRS

Afin de permettre l'application de la méthode valide d'identification des utilisateurs finals reposant sur les

opérations de paiement en ligne (art. 17 de l'A.R.), une modification de la LSRS était nécessaire pour permettre aux services de renseignement et de sécurité²⁸ de requérir le concours des banques et institutions financières.

En effet, dans le cas où la communication de l'identité d'un utilisateur final d'une carte prépayée serait requise par les pouvoirs publics, la présentation des informations bancaires collectées par l'opérateur de réseau ou le fournisseur de services de communications électroniques ne suffirait aucunement à déterminer l'identité de l'individu recherché. Dans un tel cas, seule la collaboration de l'institution bancaire ou financière impliquée peut permettre de relier des données de flux financiers à un individu particulier, titulaire d'un contrat avec ladite institution et identifié à ce titre.

Ce besoin de collaboration a dès lors été rencontré par le nouveau paragraphe deux de l'article 16/2 de la LSRS, qui donne désormais compétence aux services de renseignement et de sécurité pour requérir les informations d'identification pertinentes auxdites institutions.

Conclusion

La mise en place d'un régime d'identification obligatoire des utilisateurs finals de cartes mobiles prépayées par la loi du 1^{er} septembre 2016 et son arrêté royal d'exécution du 27 novembre 2016 s'inscrit dans une tendance observable sur le plan international depuis ces quinze dernières années.

Selon le livre blanc de la GSM Association (GSMA²⁹) relatif à l'enregistrement obligatoire des utilisateurs de cartes SIM prépayées, cette tendance a débuté en 2003 au Brésil, en Allemagne et en Suisse et n'a depuis lors cessé de se développer dans différents pays³⁰. Ainsi, suivant les statistiques de la GSMA, au 1^{er} juillet 2013, au moins 80 États avaient introduit dans leur législation un régime d'identification des utilisateurs de cartes mobiles prépayées ou envisageaient de le faire.

25. Le Rapport au Roi de l'A.R. indique toutefois que « *l'utilisateur final devra être identifié dans les 6 mois de la publication de l'arrêté royal, par analogie avec les règles applicables pour les anciennes cartes prépayées* », c'est-à-dire au plus tard le 7 juin 2017.

26. Ainsi, les FAQ de l'IBPT du 17 avril 2014 sur les obligations des opérateurs en matière d'identification des utilisateurs finals de services de communications électroniques accessibles au public (*op. cit.*, p. 1) précisent : « *La manière dont un opérateur doit identifier ses utilisateurs finals ou assurer que cet utilisateur est identifiable n'est pas définie par la loi. L'opérateur prend donc la responsabilité d'organiser cette identification de la manière qu'il juge la plus efficace, pour autant que les conditions suivantes soient remplies : Les données récoltées doivent être fiables. Ainsi, il n'est pas suffisant pour un opérateur de demander aux utilisateurs finals de remplir des champs sur un site Internet pour l'utilisation d'un service Wi-Fi, la véracité des informations n'étant pas garantie. Il est dès lors préférable de privilégier des solutions techniques qui ne peuvent pas être manipulées, telles que la réception de codes de sécurité par SMS ou la lecture de la carte d'identité électronique (...)* ».

27. Aux obligations découlant de cette disposition légale, s'ajoutent naturellement les obligations relatives à la conservation des données découlant de l'arrêté royal du 9 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques, *M.B.*, 8 octobre 2013.

28. Ces services sont les suivants : la Sûreté de l'État, et le Service général du renseignement et de la sécurité. Le premier est de nature civile tandis que le second est de nature militaire.

29. La GSMA est une association internationale représentant les intérêts d'environ 800 opérateurs de téléphonie mobile.

30. GSMA, *The Mandatory Registration of Prepaid SIM Card Users – White paper*, novembre 2013, p. 7 ; voir également GSMA, *Mandatory registration of prepaid SIM cards – Addressing challenges through best practice*, avril 2016. Ces deux documents sont disponibles à l'adresse suivante : www.gsma.com/publicpolicy/mandatory-registration-prepaid-sim-cards.

L'introduction d'un tel régime d'identification est généralement justifié par des raisons telles que la lutte contre la criminalité et la lutte contre le terrorisme, comme c'est le cas en Belgique. Il est vrai que les cartes SIM prépayées furent utilisées comme moyen de communication dans le cadre des attentats terroristes de Paris en 2015 et de Bruxelles en 2016, ou encore comme moyen permettant d'actionner à distance les détonateurs des bombes dans le cadre des attentats de Madrid en 2004.

Cela étant, de nombreuses voix considèrent qu'il n'existe aucune preuve empirique démontrant l'existence d'un lien direct entre l'identification des utilisateurs finals de cartes mobiles prépayées et le taux de criminalité. Vont notamment en ce sens le livre blanc précité de la GSMA³¹ ainsi qu'un rapport relatif à la réglementation de la téléphonie mobile prépayée et aux politiques d'enregistrement au sein de l'OCDE réalisé par le Centre de recherche stratégique sur les sciences et la technologie (CPROST) de l'Université Simon Fraser de Vancouver³².

Certains États sont également parvenus à la même conclusion.

À titre exemplatif, le Mexique, qui avait adopté en 2009 un régime d'identification obligatoire des utilisateurs finals de cartes mobiles prépayées, a décidé quelques années plus tard d'abroger ce régime à la lumière d'un rapport d'évaluation démontrant que cette mesure n'avait pas contribué à faciliter les enquêtes et la poursuite des infractions³³. De même, au Royaume-Uni, à la suite des attentats de Londres en 2005, un groupe d'experts composé de représentants des autorités judiciaires, des services de renseignement et de sécurité et des opérateurs mobiles avait examiné de manière détaillée l'opportunité d'introduire un régime d'identification obligatoire des utilisateurs finals de cartes mobiles prépayées et est parvenu à la conclusion qu'un tel régime n'apporterait aucun nouvel avantage significatif aux processus d'enquête³⁴.

Enfin, au sein de l'Union européenne, la Commission avait invité en 2012 les États membres à apporter des éléments de preuve démontrant les avantages réels ou potentiels liés à l'introduction d'un régime d'identification obligatoire des utilisateurs finals de cartes mobiles prépayées. À la lumière des réponses fournies par les États membres, Cecilia Malmström, l'ancienne

Commissaire européenne aux affaires intérieures, a souligné qu'il n'existait aucune preuve, en termes d'avantages pour les enquêtes pénales, quant à nécessité de proposer une approche commune de l'Union européenne dans ce domaine³⁵.

Ainsi, ces quelques exemples démontrent que l'opportunité d'introduire un régime d'identification obligatoire des utilisateurs finals de cartes mobiles prépayées aux fins de lutter contre la criminalité et le terrorisme est loin de faire l'unanimité.

Seuls le temps et la pratique permettront de déterminer si l'introduction d'un tel régime au sein de l'ordre juridique belge se révèle réellement efficace pour faciliter les tâches des autorités judiciaires et des services de renseignement et de sécurité, d'une part, et s'il existe un rapport de proportionnalité entre les avantages (potentiels) de ce nouveau régime et les effets restrictifs que celui-ci comporte, d'autre part.

Ce qui apparaît toutefois déconcertant de prime abord à la lumière du régime mis en place par la loi du 1^{er} septembre 2016 et son arrêté royal d'exécution du 27 novembre 2016, c'est que l'on est passé du rien au tout en matière d'identification des utilisateurs finals de cartes mobiles prépayées, à savoir d'une absence totale d'identification (anonymat) au régime d'identification le plus réglementé parmi les différents services de communication électroniques.

Au demeurant, les premières informations relatives à la mise en œuvre de ce nouveau régime ont été rendues publiques par l'IBPT.

Ainsi, dans un communiqué de presse du 8 juin 2017³⁶, l'IBPT a indiqué qu'à la date butoir fixée pour l'enregistrement des anciennes cartes prépayées (soit le 7 juin 2017), parmi les 3,1 millions de cartes SIM prépayées actives en Belgique, 2,7 millions de ces cartes ont été enregistrées (soit 87 %). Les 400 000 cartes SIM prépayées restantes, qui n'ont pas été enregistrées à cette date, devaient dès lors être bloquées par les opérateurs mobiles. L'IBPT a mené une première opération de contrôle le 8 juin 2017 auprès de tous les opérateurs mobiles afin de vérifier si ces cartes non enregistrées avaient bien été bloquées et si l'identification des utilisateurs finals avait été effectuée en conformité avec le nouveau régime mis en place. Lors de cette opération de contrôle, des infractions ont été

31. *Ibid.*, pp. 10 et 11.

32. CPROST, *Privacy Right and Prepaid Communication Services. A survey of prepaid mobile phone regulation and registration policies among OECD member states*, mars 2006, disponible à l'adresse suivante : www.sfu.ca/sfublogs-archive/departments/cprost/uploads/2012/06/0601.pdf.

33. www.senado.gob.mx/?ver=sp&mn=2&sm=2&id=28925 (uniquement disponible en espagnol).

34. www.theyworkforyou.com/wrans/?id=2007-07-16b.4.3&s=%22pay+as+you+go%22+mobile+phones.

35. www.europarl.europa.eu/sides/getAllAnswers.do?reference=P-2012-006014&language=EN.

36. www.ibpt.be/public/pressrelease/fr/140/CP_Cartes_SIM.pdf.

constatées dans le chef de quatre opérateurs mobiles. Il s'agit principalement d'opérateurs de type MVNO (*Mobile Virtual Network Operators*³⁷), les opérateurs de réseau mobile s'étant conformés à la nouvelle

réglementation. L'IBPT a déclaré qu'il continuera à effectuer de telles opérations de contrôle afin de s'assurer que les opérateurs mobiles respectent le prescrit du nouveau régime.

37. Contrairement à un opérateur de réseau mobile (*Mobile Network Operator* ou MNO), un opérateur de réseau mobile virtuel (MVNO) ne dispose ni d'un réseau d'accès radioélectrique propre ni d'une licence de spectre.