Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 141/2023 du 29 septembre 2023

Objet: Demande d'avis concernant un projet d'arrêté royal portant modification de l'arrêté royal du 27 novembre 2016 relatif à l'identification de l'utilisateur final de services de communications électroniques accessibles au public fournis sur la base d'une carte prépayée (CO-A-2023-331)

Version originale

Le Centre de Connaissances de l'Autorité de protection des données (ci-après « l'Autorité »),
Présent.e.s : Mesdames Cédrine Morlière, Nathalie Ragheno et Griet Verhenneman et Messieurs Bart Preneel et Gert Vermeulen;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après « LCA »);

Vu l'article 25, alinéa 3, de la LCA selon lequel les décisions du Centre de Connaissances sont adoptées à la majorité des voix ;

Vu le 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* (ci-après « RGPD »);

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après « LTD »);

Vu la demande d'avis de Madame Petra De Sutter, vice-Première ministre et ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste (ci-après « la demanderesse »), reçue le 14 juillet 2023;

Émet, le 29 septembre 2023, l'avis suivant :

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. La demanderesse a sollicité l'avis de l'Autorité concernant un projet d'arrêté royal portant modification de l'arrêté royal du 27 novembre 2016 relatif à l'identification de l'utilisateur final de services de communications électroniques accessibles au public fournis sur la base d'une carte prépayée[1] (ci-après « le projet »).

2. L'avant-projet de loi visant à modifier les §§1er et 3 de l'art. 127 de la loi du 13 juin 2005 *relative aux communications électroniques en vue de mettre fin à l'anonymat pour les services de communications électroniques publics mobiles auxquels il est souscrit avec des cartes prépayées*, avait été soumis à la Commission pour la protection de la vie privée (ci-après « CPVP ») le 4 décembre 2015[2], c'est-à-dire dans les semaines qui ont suivi les attentats de Paris[3] et la loi a été promulguée le 1er septembre 2016[4], soit moins de 6 mois après les attentats de Bruxelles.

3. Cette disposition habilitait le Roi à déterminer les données d'identification que les points de vente doivent collecter et les documents d'identification dont la force probante peut être admise, ce qu'il a fait dans l'AR que le projet à l'examen entend à présent modifier et au sujet duquel la CPVP avait rendu un avis pour le moins critique[5].

4. Par son arrêt n° 158/2021 du 18 novembre 2021, la Cour constitutionnelle a annulé la disposition de la loi du 1er septembre 2016 modifiant l'art. 127 de la loi relative aux communications électroniques (tout en maintenant temporairement ses effets) au motif que cette disposition ne déterminait pas les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération. En d'autres termes, la Cour constitutionnelle a rappelé, dans cet arrêt, que le principe de légalité consacré par l'article 22 de la Constitution impose au législateur de déterminer, lui-même, les données et les documents d'identification qui doivent être conservées par les opérateurs, étant donné que ces données et documents d'identification constituent un élément essentiel du traitement de données à caractère personnel.

5. Suite à cet arrêt d'annulation, l'art. 127 de la loi relative aux communications électroniques a été remplacé par la loi du 20 juillet 2022 relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture

---

[1] MB 7.12.2016

[2] Voy. l'avis 54/2015 du 16 décembre 2015 qui relève notamment que « *le législateur a omis d'intégrer plusieurs éléments essentiels dans le texte légal* » (point 10) (https://www.autoriteprotectiondonnees.be/publications/avis-n-54-2015.pdf); voy. également les avis de la section de législation du Conseil d'Etat n° 58.750/4 du 18 janvier 2016 http://www.raadvst-consetat.be/dbx/avis/58750.pdf) et 59.423/4 du 15 juin 2016 (http://www.raadvst-consetat.be/dbx/avis/59423.pdf)

[3] 13 novembre 2015

[4] MB 7.12.2016

[5] Avis 54/2016 du 21 septembre 2016 (https://www.autoriteprotectiondonnees.be/publications/avis-n-54-2016.pdf)

de ces données aux autorités[6]. L'Autorité a rendu l'**avis 108/2021**[7] au sujet de ce projet de loi et l'**avis 66/2022**[8] au sujet des amendements modifiant ce projet de loi, dans lesquels des observations sont formulées concernant l'augmentation considérable de l'ingérence dans les droits et libertés résultant de l'extension de l'obligation d'identification des utilisateurs finaux des services de communications électroniques et du recours à la technologie de la reconnaissance faciale ainsi que concernant le fait que l'identification de l'abonné à un service de communications électroniques ne permet pas nécessairement d'identifier l'utilisateur effectif de ce service. **Il est renvoyé à ces avis pour tout ce qui n'est pas expressément mentionné dans le présent avis**.

6. A noter que plusieurs recours en annulation totale ou partielle[9] ont été introduits auprès de la Cour constitutionnelle, en janvier et février 2023, à l'encontre de la loi du 20 juillet 2022 ou de certaines de ses dispositions (et notamment la disposition modifiant l'art. 127 de la loi relative aux communications électroniques).

7. Aux termes du rapport au Roi du projet, les modifications qui y sont prévues visent, premièrement, à supprimer les règles qui à la suite de la loi conservation des données de 2022 sont dorénavant reprises dans l'article 127 de la loi relative aux communications électroniques, deuxièmement, à refléter les règles et les concepts repris dans la loi relative aux communications électroniques après modifications par la loi du 21 décembre 2021 *portant transposition du code des communications électroniques européen et modification de diverses dispositions en matière de communications électroniques* et par la loi conservation des données de 2022 et, troisièmement, à « *améliorer* » l'AR de 2016 « *sur base de l'expérience acquise* ».

8. En vertu du projet à l'examen, l'AR de 2016 ne portera plus sur l'identification de la personne physique qui demande l'activation d'une carte prépayée, mais « *sur les cartes prépayées qui permettent d'utiliser un service de communications électroniques accessible au public* ». L'Autorité émet des réserves quant au caractère adéquat de ce libellé, dès lors que le projet ne se limite pas à une règlementation technique des cartes prépayées, mais à encadrer leur activation.

9. L'Autorité a été informée du fait que la section de législation du Conseil d'Etat ne s'était pas estimée en mesure de se prononcer sur le projet à l'examen dans le délai imparti et que la demande a par conséquent été rayée du rôle. L'Autorité estime que l'importance de l'ingérence pour les droits et libertés des personnes concernées, induite par le projet, implique que la plus grande attention soit

[6] MB 8.08.2022

[7] Voy. en particulier le considérant 104 de cet avis du 28 juin 2021 (https://www.autoriteprotectiondonnees.be/publications/avis-n-108-2021.pdf)

[8] Voy. en particulier les considérants 41 et suivants de cet avis du 1er avril 2022 (https://www.autoriteprotectiondonnees.be/publications/avis-n-66-2022.pdf)

[9] Affaires n°7907, 7929, 7930, 7931 et 7932

réservée à l'accomplissement des formalités préalables à son adoption. L'Autorité estime donc que le projet adapté suite aux observations formulées ci-après doit nécessairement être représenté, pour avis, à la section de législation du Conseil d'Etat.

II. EXAMEN DU PROJET

1. Prévisibilité, effectivité et importance de l'ingérence

10. L'Autorité constate que les dispositions du projet, dans la mesure où elles prévoient des traitements de données à caractère personnel, touchent *de facto* aux droits et libertés fondamentaux, dont la Constitution confie particulièrement la garantie au législateur. Or, conformément à l'article 8 de la Convention européenne des droits de l'homme, l'article 22 de la Constitution ainsi que l'article 6.3 du RGPD, lu à la lumière du considérant 41 du RGPD, toute norme prévoyant un traitement de données à caractère personnel (et donc une ingérence dans les droits et libertés des personnes concernées) doit être **claire et précise**. En outre, son **application doit être prévisible** pour les personnes concernées. Il en va d'autant plus ainsi lorsque l'ingérence revêt un caractère particulièrement important, comme c'est le cas en l'espèce.

11. Le projet à l'examen est l'occasion pour l'Autorité d'attirer l'attention de la demanderesse sur le fait que, comme le rappelle un récent rapport au Haut-Commissaire des Nations-Unies aux Droits humains, s'inquiétant des menaces que la surveillance fait peser sur les démocraties : « *les Etats négligent trop souvent de démontrer l'efficacité des systèmes de surveillance qu'ils mettent en œuvre* »[10]. Par conséquent, afin d'éviter qu'à l'avenir il puisse être reproché à la Belgique de ne pas démontrer l'efficacité des systèmes de surveillance qu'elle met en œuvre, l'Autorité estime qu'il convient de prévoir par une disposition du projet que des statistiques seront réalisées par services de police, aux **fins de la publication d'un rapport d'évaluation** (selon une périodicité à déterminer dans le projet, mais qui ne devrait pas être inférieure à tous les 3 ans) mettant à tout le moins en évidence la fréquence de consultation des données d'identification et de quel arrondissement judiciaire cette demande d'identification émane[11]. En outre, l'Autorité estime qu'il convient de prévoir les modalités de consultation, par la personne concernée, des informations relatives aux accès à ses propres données d'identifications, auprès des opérateurs[12].

---

[10] Rapport du 4 août 2022, The right to privacy in the digital age, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf?OpenElement, point 54

[11] Sur le modèle de ce qui a été réalisé par la société civile allemande en matière de rétention des données (voy. https://www.statewatch.org/media/documents/news/2011/jan/dret-working-party-report-on-germany.pdf)

[12] L'art. 17, al. 5 de la loi du 8 août 1983 organisant un registre national des personnes physiques (MB 21.04.1984) peut servir de modèle à cet égard

12. L'Autorité relève au passage que l'identification obligatoire pour l'activation d'un moyen de communication électronique n'est pas généralisée en Europe[13].

2. Observations particulières

13. L'Autorité constate qu'alors que l'intitulé (modifié) de l'arrêté se réfère à « *l'utilisateur final* », cette notion disparaît du contenu de l'arrêté au profit des notions « *d'abonné* », de « *personne qui s'identifie auprès de l'opérateur* » et des « *personnes qui peuvent utiliser une carte prépayée* ».

14. Le rapport au Roi ne précise pas pourquoi il serait nécessaire de maintenir la notion d'utilisateur final dans l'intitulé, mais justifie la suppression de cette notion dans le corps de l'AR en ces termes :

« *Les notions d'abonné (la personne qui conclut le contrat avec l'opérateur), de personne qui s'identifie après de l'opérateur et de personne qui utilise la carte prépayée sont plus précises que la notion d'utilisateur final, qui, selon la loi relative aux communications électroniques (voir article 2, 12° et 13°), vise tant la personne physique ou morale qui utilise un service de communications électroniques accessible au public que celle qui demande un tel service.*».

15. L'Autorité estime que l'abandon de la notion d'utilisateur final (y compris dans l'intitulé de l'AR modifié par le projet) se justifie par le fait que l'identification de l'abonné à un service de communications électroniques ne permet pas nécessairement d'identifier l'utilisateur effectif de ce service.

16. Afin de justifier le recours à la notion d'abonné, le rapport au Roi cite les travaux préparatoires de la loi de 2022, qui précisent que « *la notion d'abonné (ou le client de l'opérateur) doit s'entendre au sens large et couvre également les personnes qui souscrivent aux services de l'opérateur à l'aide d'une carte prépayée ou qui souscrivent à un service d'un opérateur qui fournit des services de communications interpersonnelles non fondés sur la numérotation* »[14].

17. L'Autorité estime à cet égard que la justification mentionnée dans le rapport au Roi ne doit pas (uniquement) se référer aux travaux préparatoires de la loi de 2022, mais à la Convention de Budapest sur la cybercriminalité et à son deuxième protocole additionnel ainsi qu'au considérant 13 de la directive ePrivacy.

---

[13] Voy. https://www.comparitech.com/blog/vpn-privacy/sim-card-registration-laws/

[14] Projet de loi relatif à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités, amendement n° 6, Ch., 2021-2022, n°2572/002 p. 74.

18. De plus, si la finalité liée à la possibilité de faire le lien entre une carte prépayée et la personne physique à laquelle cette carte a été attribuée peut être considérée comme légitime, l'Autorité ne perçoit pas en quoi elle serait de nature à justifier le traitement des mêmes **catégories de données** (et en particulier du recours à une comparaison biométrique) lorsqu'il est question de personnes agissant pour le compte d'une personne morale. Il en va d'autant plus ainsi que ladite personne morale est elle-même contrainte de conserver une liste actualisée permettant de faire le lien entre une carte prépayée et la personne physique à laquelle cette carte a été attribuée.

19. L'Autorité estime par conséquent qu'il convient de prévoir qu'à l'égard des personnes agissant pour le compte d'une personne morale, les traitements de données doivent se limiter à une comparaison visuelle entre les statuts ou un mandat *ad hoc* identifiant la personne habilitée à effectuer un acte juridique au nom de la personne morale et une pièce d'identité. En revanche, sauf à en démontrer le caractère nécessaire et proportionné, la conservation de ces données devra être expressément proscrite. Pour autant que besoin, l'Autorité précise que la comparaison visuelle devra être humaine et non algorithmique.

20. De plus, l'Autorité estime que **l'inapplicabilité de l'art. 5 à certaines catégories de personnes concernées** (en l'occurrence les collaborateurs des services de police et des services de renseignement) **doit être réévaluée** ou à tout le moins davantage justifiée. En effet, les mesures visant à lutter contre la criminalité grave et organisée seront facilement contournées par les personnes qu'elles ciblent si des complicités à l'intérieur des organisations chargées de poursuivre ces infractions ne peuvent être identifiées en raison d'un régime dérogatoire trop favorable. Or, comme en témoigne le rapport annuel 2022 de la Police Fédérale, de tels cas de corruption ne sont pas exceptionnels au sein de ce type d'institutions, puisqu' « *une trentaine d'enquêtes ont ainsi été ouvertes sur des fonctionnaires (de la police, de la douane, des services publics fédéraux et des administrations locales) soupçonnés de corruption* »[15].

21. Sans préjudice des compétences du COC et du Comité R pour les services qui relèvent de leur compétence exclusive, l'Autorité estime donc qu'il convient de conserver une trace de l'acquisition d'une telle carte pour tout type de personne morale, en ce compris les autorités publiques et de leur appliquer indistinctement l'obligation de principe[16] de conserver une liste actualisée, en interne, permettant de faire le lien entre une carte prépayée et la personne physique à laquelle cette carte a été attribuée.

---

[15] https://rapportannuel.policefederale.be/securite/securite-citoyen/

[16] Figurant à l'art. 5 de l'AR

22. L'Autorité ne voit pas de raison valable de ne pas également imposer cette obligation aux services de police et de renseignement. Le commentaire de l'art. 2 du projet justifie cette dérogation en précisant qu' « *il est en effet nécessaire de protéger les enquêtes effectuées par ces autorités* ». L'Autorité comprend cet argument de même que la nécessité de protéger plus largement la sécurité nationale et la sécurité des membres du personnel de certaines autorités commandent de prévoir des mesures dérogatoires. Cependant, si certains services, en ce compris les services de police et de renseignement estiment que les conditions de traitement et de conservation des données prévues par le projet sont susceptibles de constituer un risque pour la sécurité de leurs agents ou la sécurité nationale, l'Autorité estime que ces risques doivent être mentionnés dans le rapport au Roi et que, le cas échéant, il convient de démontrer pourquoi les garanties actuellement prévues devrait être considérées comme de nature à rendre ce risque admissible lorsqu'il s'agit de traiter les données à caractère personnel d'autres personnes concernées[17]. A cet effet, une analyse d'impact relative à la protection des données pourrait être réalisée dès le stade de la rédaction de la présente norme réglementaire. Une telle analyse pourrait en effet permettre d'envisager des moyens présentant à la fois un risque inférieur et un degré d'ingérence moindre, tout en permettant d'atteindre la finalité visée. De tels moyens pouvant éventuellement être généralisés au profit de l'ensemble des catégories de personnes concernées ou à tout le moins aux catégories de personnes qui ont des raisons tout aussi valables de craindre que l'ingérence occasionnée les affecte de manière disproportionnée (par exemple, dans une affaire du type de celle dite des « *princesses du Conrad* »[18], le système actuellement en vigueur n'aurait-il pas dissuadé les victimes de traite des êtres humains de se procurer un moyen de communication et de contacter des associations d'aide aux victimes, voire les services de secours ?).

23. La nouvelle version de l'art. 1er de l'AR de 2016 ne prévoit plus que l'arrêté porte sur l'identification des personnes demandant l'activation d'une carte prépayée, mais sur les cartes prépayées elles-mêmes. L'Autorité estime cependant que cette formulation a pour effet de scinder l'AR de la mesure qu'il entend préciser ou mettre en œuvre.

24. Le commentaire de l'art. 1er du projet précise en substance que la référence à la délégation au Roi figurant à l'art. 127, §11, al. 2 de la loi relative aux communications électronique a été omise car cette délégation vise les services de communications électroniques mobiles et qu'il a été décidé de ne plus restreindre l'AR aux services mobiles de communications électroniques « *afin d'éviter qu'il ne soit argumenté que le présent arrêté n'est pas applicable au motif que le service de communications électroniques utilisé ne serait pas mobile* ».

---

[17] L'Autorité rappelle au passage que les véhicules des forces de l'ordre (et même ceux des services de renseignement) sont immatriculés, comme les autres.

[18] https://www.lalibre.be/belgique/2017/06/23/bruxelles-15-mois-de-prison-avec-sursis-pour-les-princesses-du-conrad-L5NWFT3TYFCU7FGEBGOEEVS7CA/

25. A cet égard, l'Autorité estime que cette modification implique une **extension des catégories de personnes concernées par le traitement de leurs données** et que, s'agissant d'un élément essentiel, elle doit nécessairement figurer dans une norme de rang législatif. Un fois que cette modification aura été admise par le législateur, l'intégration dans le projet d'une référence aux mesures techniques et administratives qui sont imposées aux opérateurs en vue de permettre l'identification de la personne souhaitant activer une carte prépayée permettant l'accès à des services de communications électroniques devra être envisagée.

26. Par dérogation à l'AR modifié, les opérateurs peuvent **déterminer librement les modalités d'identification** des « abonnés » aux cartes prépayées permettant exclusivement des applications la technologie machine à machine (M2M) ou des applications relatives à l'internet des objets (IoT), pour autant que ces applications ne permettent pas d'utiliser un service d'accès à internet ou un service de communication interpersonnelle d'un opérateur. Cette dérogation est justifiée dans le rapport au Roi par « *la demande des opérateurs* ».

27. Dans la mesure où l'obligation d'identification reste applicable aux cartes permettant ce type d'applications, il ne fait aucun doute que des données à caractère personnel devront être traitées par des opérateurs pour respecter l'obligation légale à laquelle ils sont soumis. Dans cette optique, dans le respect du principe de minimisation des données, en l'état, cette disposition ne peut en aucun cas permettre aux opérateurs de justifier d'exiger la production d'une carte d'identité officielle, l'accès à des sources authentiques et encore moins la comparaison de données biométriques.

28. L'art. 5 nouveau de l'AR interdit – sauf les cas d'exceptions qu'il énumère - la **cession (et la cession ultérieure) d'une carte prépayée active**, par une personne qui s'identifie, à une autre personne.

29. Le caractère excessif de cette ingérence est renforcé par l'absence de définition de la « cession ». L'Autorité estime donc qu'il convient à tout le moins d'exclure, dans le rapport au Roi, l'applicabilité de cette disposition à l'usage occasionnel par un tiers.

30. La modification de l'art. 11 de l'AR **étend la vérification systématique** (jusqu'alors limitée au vol et à la fraude) au cas où la carte d'identité belge est connue des autorités publiques comme volée, perdue, périmée, non valide ou n'a pas été émise.

31. L'Autorité estime que le caractère nécessaire et proportionné de cette extension doit être démontré dans le rapport au Roi. A cette occasion, une attention toute particulière devra être accordée à la justification de la vérification du caractère périmé de la carte d'identité. En effet, s'agissant d'une

identification et non d'un contrôle de la régularité d'un document (ni des conditions de séjour), la finalité prévue par le projet ne semble pas compatible avec une interdiction absolue d'activation ou avec un signalement aux autorités du caractère périmé de la carte. Lorsqu'une demande l'activation d'une carte prépayée au moyen d'une carte d'identité périmée, l'Autorité estime qu'il convient de prévoir expressément la possibilité de s'identifier au moyen d'autres documents et/ou, du moins en l'absence de doute sur la ressemblance, de prévoir une activation temporaire, d'une durée raisonnable, pour permettre à la personne d'obtenir ou de se procurer le document requis[19].

32. A défaut d'être en mesure de démontrer le caractère nécessaire et proportionné de cette extension, l'Autorité estime qu'il y a lieu de revenir aux conditions de refus d'activation prévalant jusqu'à présent, à savoir le signalement par les autorités que la carte d'identité utilisée a été volée ou a fait l'objet d'une fraude.

33. Le même article 11, qui prévoyait jusqu'à présent **« *l'identification fiable* » de l'utilisateur**, se réfère à présent à la « *condition que l'outil informatique puisse être considéré comme fiable* ». L'ancienne formulation permettait de rencontrer cette condition de fiabilité en ayant recours à une identification sur base de données commerciales, de checkdoc.be, via paiement électronique ou d'autres méthodes de vérification électroniques. Afin d'éviter tout doute quant à l'interprétation de ce qui peut être considéré comme fiable ou non, l'Autorité estime qu'il convient de préciser les conditions permettant de considérer un outil informatique comme fiable. L'Autorité précise toutefois que ces conditions ne peuvent être strictes au point d'avoir pour effet de privilégier la comparaison biométrique par rapport à d'autres outils.

34. Le dernier alinéa de l'art. 11, §1er nouveau de l'AR dispose que « *l'autorisation visée à l'alinéa 1er est accordée après avis de l'Institut, qui se* ***concerte au préalable*** *avec les services de renseignement et de sécurité et le NTSU, à savoir le National Technical et Tactical Support Unit des unités spéciales de la police fédérale* ».

35. L'Autorisation en question semble porter le recours à un « *autre outil informatique autorisé par le ministre de la Justice et le ministre* » (sic), pour la vérification de la carte d'identité du demandeur d'activation. Le commentaire de cet article n'apporte pas d'avantage d'explications. Par comparaison, le commentaire de l'article modifiant l'art. 19 de l'AR (dont le libellé est similaire), précise qu' « *il convient notamment d'éviter que cet outil ne récolte des données sur des abonnés et que ces données ne fuitent ensuite vers des pays tiers et ce, dans la mesure où ces dernières risqueraient d'être utilisées, entre autres, à des fins d'espionnage et/ou de recoupement avec d'autres informations. Ceci est*

[19] Voy. par analogie l'art. 41 de la loi du 15 décembre 1980

particulièrement le cas lorsque les abonnés précités travaillent dans des secteurs sensibles reliés à la sécurité nationale (services de renseignement et de sécurité, services de police, etc.) ».

36. L'Autorité estime qu'une précision similaire doit illustrer le dernier alinéa de l'art. 11, §1er nouveau de l'AR. L'Autorité s'interroge par ailleurs sur le périmètre de la concertation prévue. En effet, si cette concertation est limitée à l'outil, il convient de démontrer que des tests ont démontré que l'outil autorisé ne présentait aucune faille susceptible d'être exploitée par un utilisateur mal intentionné[20]. Si, en revanche, la concertation devait également porter sur les exploitants des points de vente, voire leurs préposés, il conviendrait de démontrer de manière détaillée, en quoi la comparaison de données biométriques, voire la possibilité de lire les données figurant sur les cartes d'identité des citoyens offre un bénéfice à ce point supérieur à l'ingérence dans les droits et libertés des personnes appelées à être les sujets d'une concertation avec les services de renseignement et de sécurité et le NTSU. En d'autres termes, à la lumière des potentielles dérives, **il convient de démontrer qu'il est bien adéquat, nécessaire et proportionné, de permettre la vérification de données issues de sources authentiques (et a fortiori de données biométriques) par des préposés d'opérateurs privés**.

37. L'Autorité constate que le commentaire de l'art. 15 (modifiant l'art. 11 de l'AR) précise qu' « *il n'y a plus d'**obligation de la part des opérateurs d'informer les autorités compétentes** de détection d'anomalies ou du caractère incorrect des données, ce qui ne les empêche pas de le faire si cela est pertinent* ». L'Autorité en prend acte.

38. L'Autorité constate en outre qu'en l'absence de réidentification, après détection d'une anomalie, l'art. 11, §2, 3° nouveau dispose que la carte est rendue inutilisable « *sauf ordre contraire des autorités judiciaires ou des services de renseignement et de sécurité* » et que le §3 nouveau de ce même article dispose que « *lorsque la carte prépayée a déjà été activée et que par la suite l'opérateur constate ou est informé, par exemple par une autorité, que l'identification de la personne qui s'identifie est frauduleuse, il rend immédiatement inutilisable la carte prépayée, sauf ordre contraire reçu des autorités judiciaires ou des services de renseignement et de sécurité* ». L'Autorité présume que les mesures techniques et organisationnelles destinées à assurer la sécurité, l'intégrité et le caractère confidentiel des données communiquées par les services de police et de renseignement aux opérateurs téléphoniques sont applicables en l'espèce. Sous cette réserve, l'Autorité n'a pas d'observations à formuler à cet égard.

[20] On peut effet légitimement supposer qu'un pays ayant la capacité d'ouvrir des commissariats de police clandestins dans l'Union européenne (https://fr.euronews.com/2022/10/27/la-chine-a-t-elle-ouvert-54-postes-de-police-illegaux-en-europe-et-dans-le-monde), pourrait être en mesure de contrôler des points de vente de cartes de téléphonie pour, par exemple, accéder aux données biométriques d'opposants réfugiés sur le territoire national

39. L'art. 19 du projet modifie l'art. 14 de l'AR en mettant notamment en œuvre l'**identification optionnelle par comparaison faciale,** prévue à l'art. 127, §5, al. 4, 1° de la loi relative aux communications électroniques. L'art. 14, al. 2 nouveau de l'AR dispose que « *lorsque l'opérateur a été autorisé à mettre en œuvre un outil de comparaison faciale* (…) *et que la personne y consent, il peut l'identifier à l'aide de cet outil* ».

40. Le libellé de cette disposition, lu en combinaison avec l'art. 13 nouveau de l'AR qui dispose que « *l'opérateur doit proposer au moins une méthode d'identification visée dans la présente section à la personne qui s'identifie* ». Ce n'est en effet qu'à la lecture du rapport au Roi qu'il apparaît clairement qu' « *une personne doit toujours avoir à sa disposition une alternative par rapport à l'outil de comparaison faciale (article 127, § 5, alinéa 4, 2°, de la loi relative aux communications électroniques). Elle peut par exemple demander qu'elle ne soit pas identifiée par cet outil mais par un membre du personnel du point de vente* ».

41. L'Autorité estime donc que l'art. 13 nouveau de l'AR doit mentionner explicitement que l'opérateur doit proposer au moins une méthode d'identification visée dans la présente section, « *autre que l'outil de comparaison faciale* », à la personne qui s'identifie.

42. En outre, il convient de reformuler l'art. 14, al. 2 nouveau de l'AR en prévoyant que lorsque l'opérateur a été autorisé à mettre en œuvre un outil de comparaison faciale, « *il ne peut identifier une personne à l'aide de cet outil que moyennant le consentement de cette personne* ».

43. Le dernier alinéa du commentaire de l'art. 19 du projet précise que « *dans ce cas,* ***il reviendra au membre du personnel du point de vente de s'assurer*** *que la personne qui se présente correspond bien à la personne dont la photo est reprise sur le document d'identité.* ***Pour éviter de devoir faire ce contrôle*** *et lorsque la personne présente une carte d'identité électronique belge, le point de vente peut choisir de lui demander d'introduire le code PIN lors de la lecture de cette carte d'identité belge* ».

44. Cet alinéa semble comporter des éléments prescriptifs tout en étant formulé d'une manière permettant « *au point de vente* » de déterminer discrétionnairement les traitements de données auxquels il sera procédé. Si la demanderesse souhaite la déplacer vers le projet, l'Autorité l'invite à en revoir fondamentalement la formulation et en tenant compte des deux observations fondamentales suivantes : tout d'abord, « *éviter de devoir faire ce contrôle* », ne peut en aucun cas être une finalité admissible pour un traitement de données à caractère personnel. Et ensuite, pour qu'il y ait une

obligation légale au sens de l'article 6.1.c) du RGPD, il faut que le responsable du traitement (à savoir, en l'occurrence les points de vente) n'ait pas le choix de se conformer ou non à l'obligation[21].

PAR CES MOTIFS,
L'Autorité
estime que :

- en ce qui concerne les éléments essentiels figurant dans la loi relative aux communications électroniques, il y a lieu de tenir compte de ses avis 108/2021 et 66/2022 ;
- il convient de prévoir la réalisation de statistiques aux fins de la publication d'un rapport chiffré (point 11) ;
- il convient de prévoir les modalités de consultation, par la personne concernée, des informations relatives aux accès à ses propres données d'identifications, auprès des opérateurs (point 11) ;
- la justification relative à l'abandon de la notion d'utilisateur final, de même que celle relative à la notion d'abonné doivent être adaptées (points 13 à 17) ;
- il convient de prévoir qu'à l'égard des personnes agissant pour le compte d'une personne morale, les traitements de données doivent se limiter à une comparaison visuelle entre les statuts ou un mandat *ad hoc* identifiant la personne habilitée à effectuer un acte juridique au nom de la personne morale et une pièce d'identité et, sauf à en démontrer le caractère nécessaire et proportionné, que la conservation de ces données est interdite (point 19) ;
- la proportionnalité des moyens doit être évaluée dans le rapport au Roi, au regard d'une analyse détaillée des risques liés aux conditions de traitement et de conservation des données prévues par le projet (points 20 à 22) ;
- l'extension des catégories de personnes concernées doit être prévue dans une norme de rang législatif (points 24 et 25) ;
- la liberté de détermination des moyens d'identification des « abonnés » aux cartes prépayées permettant exclusivement des applications la technologie machine à machine (M2M) ou des applications relatives à l'internet des objets (IoT) ne peut fonder la consultation de données issues de sources authentiques et encore moins le recours à une comparaison biométrique (points 26 et 27) ;
- la notion de « cession » figurant à l'art. 5 de l'AR doit expressément exclure l'usage occasionnel par un tiers (point 29) ;
- le caractère nécessaire et proportionné de l'extension de la vérification aux cas où la carte d'identité belge est connue des autorités publiques comme volée, perdue, périmée, non valide

[21] Groupe de travail « Article 29 » sur la protection des données (prédécesseur du Comité européen de la protection des données), Avis n° 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, adopté le 9 avril 2014, WP 217, p. 21-22 ; voy. également la décision 34/2022 de la Chambre contentieuse de l'Autorité

ou n'a pas été émise, doit être démontré (points 30 à 32) ;

- il convient de préciser les conditions permettant de considérer un outil informatique comme fiable (point 33) ;
- le périmètre de la concertation prévue à l'art. 11 de l'AR doit être précisé et justifié (points 35 et 36) ;
- les art. 13 et 14 nouveaux de l'AR doivent être reformulés en ce qui concerne le recours à la reconnaissance faciale moyennant le consentement de la personne concernée (points 41 et 42) ;
- le commentaire de l'art. 19 du projet doit être reformulé et éventuellement déplacé dans le projet (point 44).

Pour le Centre de Connaissances,
(sé) Cédrine Morlière, Directrice