Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 136/2021 du 24 août 2021

Objet : Avis relatif à une proposition de résolution relative à la lutte contre la cyberfraude utilisant des mules bancaires (CO-A-2021-155)

Le Centre de Connaissances de l'Autorité de protection des données (ci-après "l'Autorité"), en présence de Mesdames Marie-Hélène Descamps et Alexandra Jaspar et de Messieurs Yves-Alexandre de Montjoye, Bart Preneel et Frank Robben ;

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 la "LCA") ;

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* (Règlement général sur la protection des données, ci-après le "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 "la LTD") ;

Vu la demande d'avis de Madame Éliane Tillieux, Présidente de la Chambre des représentants, reçue le 15/07/2021 ;

Vu le rapport d'Alexandra Jaspar ;

Émet, le 24 août 2021, l'avis suivant :

I. OBJET DE LA DEMANDE

1. Madame Éliane Tillieux, Présidente de la Chambre des représentants, recueille l'avis de l'Autorité sur une proposition de résolution relative à la lutte contre la cyberfraude utilisant des mules bancaires.

2. La résolution précise que les cybercriminels qui extorquent de l'argent via Internet ont généralement recours à des "money mules" (mules bancaires). Afin de ne pas se faire prendre eux-mêmes en faisant verser l'argent directement sur leur propre compte, par exemple, les escrocs font appel à des "mules bancaires". Ces personnes prêtent leur compte bancaire et/ou leur carte bancaire ainsi que leur code pin contre rémunération. L'argent volé peut ainsi être dépensé en ligne, être transféré sur un autre compte bancaire en Belgique ou à l'étranger ou être retiré à un distributeur de billets. Souvent, seule la mule bancaire peut être identifiée et condamnée alors que les donneurs d'ordre restent hors de portée.

3. Selon la résolution, ceci résulte du fait que les banques ne disposent pas de moyens pour attaquer le mal à la racine. Pour pouvoir démanteler les réseaux criminels, les échanges de données entre les banques devraient être beaucoup plus nombreux, par analogie avec le Risk Warning System (système de prévention des risques) aux Pays-Bas. Ce système permet aux banques d'entamer des enquêtes entre elles en cas de blanchiment d'argent. Les auteurs de la résolution insistent pour que le gouvernement élabore un cadre légal qui permette aux institutions financières d'échanger des informations sur les comptes suspects et les transactions suspectes, en cas de soupçon de blanchiment d'argent, afin de faciliter le démantèlement d'un éventuel réseau criminel.

II. EXAMEN DE LA DEMANDE

4. L'Autorité attire l'attention sur le fait que la recherche de criminels relève des services publics mandatés à cet effet. De telles enquêtes s'accompagnent en effet d'une immixtion dans la vie privée. La question se pose de savoir s'il appartient bien à des entreprises commerciales telles que des banques, qui sont finalement concurrentes les unes des autres, d'entamer, de leur propre initiative, des enquêtes entre elles sur leurs clients concernant le blanchiment d'argent et donc de mener au fond une enquête sur des infractions pénales et d'échanger des données sur des personnes dans ce cadre. Cela va bien au-delà par exemple d'une obligation de notification de transactions suspectes aux autorités judiciaires compétentes qui mènent des enquêtes pénales avec les garanties y afférentes pour les personnes concernées. Il en résulte en outre que les banques impliquées dans l'enquête (finalité d'enquête) entrent en possession de plus d'informations sur un client que ce dont elles disposent dans le cadre de leur relation commerciale (finalité commerciale) avec lui. Dès lors, le risque que les "informations d'enquête" soient ensuite utilisées à des fins commerciales est considérable.

5. Si l'on envisage d'attribuer à des entreprises commerciales un "rôle d'enquêteur", il faut chercher au maximum à assurer la minimisation des données par des « privacy enhancing technologies ». On peut penser ici à la technique de "Private Set Intersection" permettant aux banques d'établir chacune une "liste noire" reprenant les noms ou comptes susceptibles d'être impliqués par des "money mules" (mules bancaires) et de vérifier ensuite quels noms figurent également sur la "liste noire" d'autres banques sans divulguer la moindre information sur des données qui n'apparaissent qu'une seule fois.

6. Tant que rien de précis n'a été élaboré, l'Autorité n'est pas en mesure d'établir un point de vue. Elle se voit dès lors contrainte de se limiter à rappeler ci-après les principes essentiels qui doivent être respectés lors de la rédaction éventuelle d'une réglementation.

A. Test de nécessité

7. Tout traitement de données à caractère personnel instauré par une réglementation implique en principe une limitation du droit à la protection des données à caractère personnel. Lors de la préparation d'un projet de texte normatif qui encadre des traitements de données à caractère personnel, il faut donc d'abord analyser si la mesure visée est bel et bien nécessaire pour atteindre l'objectif légitime qu'elle poursuit. Ce test de nécessité implique que l'auteur d'un projet de texte normatif réalise une analyse préalable d'une part des faits qui justifient l'instauration de la mesure et d'autre part du degré d'efficacité de la mesure à la lumière de la finalité qu'elle poursuit. Dans le cadre de cette analyse, l'auteur doit également vérifier si son objectif peut éventuellement être atteint via une mesure moins intrusive du point de vue de la protection des données.

B. Base juridique et prévisibilité de la norme

8. Tout traitement de données à caractère personnel doit trouver une base juridique dans l'article 6.1 du RGPD. Les traitements de données instaurés via une mesure normative sont quasiment toujours basés sur l'article 6.1. c) ou e) du RGPD. En vertu de l'article 22 de la *Constitution*, de l'article 8 de la CEDH et de l'article 6.3 du RGPD, de tels traitements doivent être encadrés par une réglementation claire et précise, dont l'application doit être prévisible pour les personnes concernées. La réglementation doit donc définir de manière suffisamment précise sous quelles conditions et dans quelles circonstances le traitement de données à caractère personnel a lieu. En principe, les éléments suivants doivent dès lors y être repris :

a) le responsable du traitement,
b) la (les) finalité(s) du traitement,
c) le type de données nécessaires à la réalisation de cette (ces) finalité(s),

d) la durée de conservation des données,
e) les catégories de personnes concernées dont les données seront traitées,
f) les destinataires ou catégories de destinataires auxquels les données seront communiquées,
g) les circonstances dans lesquelles elles seront communiquées.

C. Traitement de données sensibles

9. L'Autorité attire l'attention sur le fait que le traitement de certaines catégories particulières de données à caractère personnel, telles qu'énumérées aux articles 9 et 10 du RGPD, est en principe interdit.

10. Il s'agit tout d'abord des catégories énumérées à l'article 9.1 du RGPD : les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques, les données biométriques aux fins d'identifier une personne physique de manière unique, les données concernant la santé et les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. L'article 9.2 du RGPD décrit les situations dans lesquelles des exceptions à cette interdiction de traitement s'appliquent. Si de telles catégories de données étaient traitées à la suite d'un projet de texte normatif, il serait donc nécessaire de vérifier si ce traitement trouve une base dans un des motifs d'exception de l'article 9.2 du RGPD.

11. Lors de la préparation d'un projet de texte normatif, l'exception reprise au point g) de l'article 9.2 du RGPD sera souvent pertinente : "*le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée*". Si l'auteur d'un projet de texte normatif veut faire reposer (partiellement) un traitement sur cet article 9.2.g) du RGPD, il doit donc démontrer l'intérêt public important qui nécessite le traitement de ces données. En outre, le projet de texte normatif doit prévoir des mesures spécifiques afin de veiller à la protection des droits et intérêts fondamentaux des personnes concernées.

12. L'Autorité fait par ailleurs remarquer que l'article 9 de la LTD impose des conditions complémentaires pour le traitement de ces catégories de données.

13. Une deuxième catégorie de données à laquelle une interdiction de traitement s'applique concerne les données relatives aux condamnations pénales et aux infractions (article 10 du RGPD). Le traitement de ce type de données ne peut être effectué que sous le contrôle de l'autorité publique

ou d'une autre personne si le traitement est autorisé par une loi (nationale ou européenne). Tout registre complet des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique. Enfin, l'article 10 de la LTD définit les personnes/organismes qui peuvent traiter ce type de données et sous quelles conditions cela doit se faire.

D. Utilisation du numéro de Registre national

14. Si le but est d'instaurer l'utilisation du numéro de Registre national pour des finalités déterminées via un projet de texte normatif, les prescriptions suivantes doivent être respectées.

15. L'article 87 du RGPD dispose que les États membres qui définissent un numéro d'identification national doivent veiller à ce que celui-ci ne soit utilisé que si des garanties appropriées pour les droits et libertés de la personne concernée sont prévues. De telles garanties impliquent que :

- l'utilisation d'un tel numéro soit limitée aux cas dans lesquels cela est strictement nécessaire et proportionnel, étant donné que cette utilisation engendre certains risques ;
- les finalités soient précisées clairement et explicitement afin que l'on puisse entrevoir les types de traitements visés ;
- la durée de conservation et les éventuelles communications à des tiers soient également encadrées ;
- les mesures techniques et organisationnelles encadrent adéquatement son utilisation sécurisée.

16. En outre, l'Autorité attire l'attention sur le fait que le numéro de Registre national ne peut être utilisé que dans la mesure où l' (les) instance(s) en question dispose(nt) de l'autorisation requise, en vertu de la loi du 8 août 1983 *organisant un registre national des personnes physiques* (article 8, § 1er). Conformément à cette disposition, une autorisation d'utilisation du numéro du Registre national n'est pas requise lorsque cette utilisation est explicitement prévue par ou en vertu d'une loi, un décret ou une ordonnance. Dans les autres cas, l'autorisation d'utiliser le numéro de Registre national est en principe octroyée par le ministre ayant l'Intérieur dans ses attributions, aux conditions énoncées aux articles 5 et 8 de la loi du 8 août 1983. Lorsque le Comité de sécurité de l'information doit émettre une délibération pour une communication de données à caractère personnel, il peut le cas échéant émettre dans le même temps une délibération pour l'utilisation du numéro de Registre national par les instances concernées, si cela s'avère nécessaire dans le cadre de la communication envisagée.

17. Si des données à caractère personnel sont transférées à des pays tiers ou à des organisations internationales, il convient de s'assurer soit que ce transfert ait lieu conformément aux instruments mentionnés aux articles 45 - 48 du RGPD, soit qu'une des situations particulières visées à l'article 49 du RGPD s'applique.

Pour le Centre de Connaissances,
(sé) Alexandra Jaspar, Directrice