noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienna
Austria

Autorité de protection des données
Rue de la Presse 35
1000 Bruxelles
par e-Mail: [redacted]

Vienne, 23 juin 2023

noyb Case-No: C-063

Plaignants: [redacted], domicilié à [redacted]
[redacted] domicilié [redacted]
[redacted], domiciliée [redacted]
[redacted], domicilié [redacted]
[redacted], domicilié [redacted]
[redacted], domicilié [redacted]
[redacted], domicilié [redacted]
[redacted], domicilié [redacted]
[redacted]

Représentés par: *noyb* – European Center for Digital Rights
Goldschlagstraße 172/4/3/2, 1140 Vienne, Autriche, en vertu de l'article 80 du RGPD

Contre:

BICS SA
Boulevard du Roi Albert II 27, 1030 Bruxelles

TELESIGN
13274 Fiji Way Suite 600, Marina del Rey CA 90292, Etats-Unis
ayant un représentant au sens de l'article 27 du GDPR en la personne de TeleSign Netherlands B.V., société enregistrée au Pays-Bas.

PROXIMUS
Boulevard du Roi Albert II 27, 1030 Bruxelles.

Et toute autre personne, responsable du traitement ou sous-traitant qui serait identifiée dans le cadre de la procédure.

PLAINTE

1. REPRESENTATION

1. *noyb* – European Center for Digital Rights est une association sans but lucratif active en matière de protection des données des personnes. Ses bureaux sont situés Goldschlagstraße 172/4/2, 1140 à Vienne en Autriche, et est enregistrée sous le numéro ZVR: 1354838270 (ci-après: *« noyb »)* (Pièce 1).

2. *noyb* représente les plaignants qui lui ont donné mandat à cet effet en vertu de l'article 80 du RGPD (Pièces 2).

2. CONTEXTE DE LA PLAINTE

2.1 Introduction

3. Comme développé dans la présente plainte (voir section 2.3), un article du journal *Le Soir* révélait en mars 2022 que BICS, filiale de Proximus, transférait les données transitant par ses services à une autre filiale de Proximus aux USA, la société TeleSign.

4. L'article du Soir expliquait que TeleSign attribuait un « score de réputation » aux numéros de téléphone de millions d'utilisateurs finals, et nourrissait ses algorithmes avec les données de télécommunications reçues par BICS. Ce score de confiance est revendu aux clients de TeleSign (comme Skype, LinkedIn, ou Microsoft) qui l'utilisent également sans en informer leurs utilisateurs. TeleSign annonce utiliser ces données à des fins -assez vagues- de « détection de la fraude ».

5. Suite à cette révélation, plusieurs utilisateurs de services de communications résidant dans différents pays de l'Union européenne ont introduit une demande d'information auprès de leur fournisseur de téléphonie, de BICS et de TeleSign, pour savoir si et à quelles conditions leurs données étaient envoyées et traitées par TeleSign.

6. Il ressort des réponses reçues que TeleSign recevait bien les données des utilisateurs pour les profiler et leur attribuer un score de réputation. TeleSign a d'ailleurs communiqué à ces utilisateurs le score qui leur était attribué. Il s'avère donc que des millions d'utilisateurs de service de communications se sont vu profilés par une société américaine avec laquelle il n'ont jamais eu de contact, dont ils ne connaissaient même pas l'existence, et qui ne les jamais informés de l'existence, de l'objectif et des conditions de ce traitement, alors qu'elle disposait précisément de leurs numéros de téléphones pour ce faire. TeleSign confirme elle-même vérifier plus de cinq

milliards de numéros de téléphone par mois, ce qui représente la moitié des abonnées de téléphonie mobile dans le monde.[1]

7. Vu la part de marché de BICS, il semble même que TeleSign a collecté les données de plus de la moitié des utilisateurs du globe, ce qui génère un revenu considérable, sans base légale et sans les en informer. TeleSign utilise en outre un algorithme pour adopter automatiquement un score sur la base duquel l'accès aux services de ses clients peut être refusé. Il s'agit donc de décisions automatisées illégales au sens du RGPD. Enfin, TeleSign étant soumis aux lois de surveillance américaines, le traitement de ces données est contraire aux règles relatives aux transferts de données édictées par le RGPD, et aux arrêts *Schrems I* et *Schrems II* de la Cour de justice.

8. Outre le traitement illégal mis en œuvre par TeleSign, cette plainte concerne également l'absence de réponse à la demande d'accès introduite par deux plaignants auprès de Proximus. Cette plainte concerne également le détournement de finalités des données traitées par BICS, qui partage ses données pour des finalités qui sont interdites à la fois par le RGPD mais également par la loi sur les communications électroniques. La plainte soulève également l'illégalité du transfert de données opéré par BICS vers TeleSign aux Etats-Unis, transfert organisé et encadré par un contrat entre les deux sociétés et qui prévoit l'envoi systématique et massif des données de communications par BICS vers TeleSign.

9. Enfin, vu les réponses vagues, voire obscures, et même parfois contradictoires fournies par TeleSign, il reste difficile de comprendre avec précision ce que cette société fait exactement avec les données des utilisateurs, où elle les collecte, et avec qui elle les partage. TeleSign invoque la « lutte contre la fraude » comme objectif dans ses réponses aux demandes d'accès. Cependant, si la lutte contre la fraude est une finalité autorisée par la loi pour l'utilisation des données de communications électroniques par les opérateurs, TeleSign n'est pas supposée recevoir ou utiliser lesdites données de communications électroniques, même à des fins de prévention de fraude, comme cela est développé dans la présente plainte. Dans tous les cas, il est plus que douteux que l'utilisation desdites données par TeleSign reflète un tel objectif de détection de la fraude qui réponde au prescrit de la loi. Le service d'inspection de l'APD que ne manquera pas d'éclairer les plaignants sur ces traitements de données, dont l'existence aurait encore été un secret sans les révélations d'une presse bien informée.

2.2 Présentations des différentes entités concernées par la plainte : BICS, TeleSign et Proximus

2.2.1 BICS

10. BICS (« Belgacom International Carrier Services ») est le premier opérateur dans le domaine des communications internationales, l'un des principaux opérateurs voix et le premier fournisseur de services de données mobiles au monde.[2]

---

[1] https://www.telesign.com/press/telesign-unveils-new-brand-identity-reflecting-companys-transformation-and-commitment-to-making-the-digital-world-more-trustworthy-for-everyone.

[2] Rapport annuel 2022 de Proximus http://www.proximus.com/dam/jcr:7cf6d111-cf0b-4c3d-a764-201c9bd93283/proximus-rapport-annuel-integre-2022_fr.pdf, p. 12.

11. BICS est une filiale du Groupe Proximus. La société a été fondée en 1997 et son siège est situé à Bruxelles, avec des bureaux à Dubaï, Singapour, Berne, San Francisco et New York. BICS fournit ses services dans plus de 200 pays, intervient dans la moitié du trafic mondial de roaming[3], permet la mobilité globale de plus de 150 millions de terminaux et a conclu un partenariat avec plus de 500 opérateurs mobiles.[4] BICS a transmis 20,5 milliards de messages à travers le globe, et 26 milliards de minutes via 550 connexions directes.

12. BICS offre également des services de protection contre différentes formes de fraude aux télécommunications. Ces services incluent la prévention à la fraude SMS, à la voix, au roaming, et à la sécurité des interconnexions IPX.[5]

2.2.2 TeleSign

13. TeleSign se présente comme un leader dans l'identité digitale et les communications programmables.[6] TeleSign est *« un leader en pleine croissance spécialisé dans les solutions d'identité digitale et de communications programmables. Partenaire de confiance des entreprises dans le monde entier, Telesign compte parmi ses clients huit des dix plus grandes sociétés du digital au monde et fournit des services dans plus de 230 pays et territoires »*.[7]

14. TeleSign « fournit des *solutions de sécurité, d'authentification, de détection des fraudes, de gestion de la conformité et des scores de réputation et de communications sécurisées* ».[8] En combinant services d'identité digitale et solutions globales de communications, *« TeleSign aide les entreprises à se connecter, à se protéger et à interagir avec leurs clients, tout en permettant à ces derniers de communiquer en toute sécurité sur leurs plateformes digitales préférées ».* [9]

15. TeleSign offre notamment un outil de prévention des fraudes appelé « Intelligence API » (et autrefois appelé « Score »). Cet outil se base sur un « score de fiabilité » que TeleSign attribue à chaque numéro de téléphone dans sa base de données et basé sur « les informations concernant les numéros de téléphone, les habitudes de trafic, le machine learning et un consortium mondial de données ».[10] Toujours selon TeleSign, les informations utilisées par TeleSign utilisent deux bases de données mondiales pour détecter et identifier les fraudes : TeleBureau, la base de données de TeleSign permettant de mesurer la réputation d'un numéro de téléphone, mais aussi de la base de données de BICS (BICS Global Telco Fraud Data).[11]

---

[3] https://www.bics.com/global-roaming/

[4] https://www.bics.com/wp-content/uploads/2021/07/BICS-Roaming-brochure.pdf

[5] https://www.bics.com/wp-content/uploads/2022/02/Telco-Fraud-Whitepaper.pdf

[6] https://www.telesign.com/company

[7] Rapport annuel 2022 de Proximus, http://www.proximus.com/dam/jcr:7cf6d111-cf0b-4c3d-a764-201c9bd93283/proximus-rapport-annuel-integre-2022_fr.pdf, p. 12.

[8] Rapport annuel 2021 de Proximus http://www.proximus.com/dam/jcr:7ee0f496-f68e-4161-aa09-c2df5f16f1d0/Proximus-rapport-annuel-integre-2021_fr.pdf, p. 11.

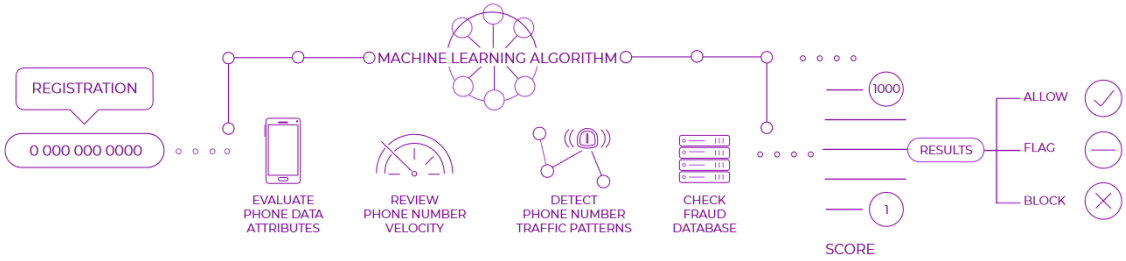
[9] Rapport annuel 2021 de Proximus, p. 12.

[10] https://ts.telesign.com/hubfs/Product-Datasheets/Score-Datasheet.pdf

[11] https://ts.telesign.com/hubfs/Product-Datasheets/Score-Datasheet.pdf

16. TeleSign dit exploiter les informations de plus de 5 milliards de numéros de téléphones uniques, combinés avec 2200 signaux d'identité numérique (adresse IP, numéro d'identification de l'appareil).[12] TeleSign affirme vérifier plus de 5 milliards de numéros de téléphone par mois, ce qui représente la moitié des utilisateurs de mobile dans le monde.[13] TeleSign compte 8 des 10 plus grandes sociétés mondiales du digital parmi ses clients, comme SalesForce, Skype, Ubisoft ou ByteDance (laquelle fournit la plateforme TikTok).

17. Le schéma ci-dessus permet de résumer le processus en place pour la solution de score de fiabilité fournie par TeleSign aux dits clients:



18. Dans un premier temps, TeleSign évalue les attributs des numéros de téléphone, à savoir toute une série d'informations relatives au numéro de téléphone, comme le type de téléphone (ligne fixe, mobile, VOIP), l'opérateur de téléphonie, l'adresse de l'utilisateur, le statut du téléphone, la location géographique, et le code du pays de l'opérateur. Ces informations permettent, selon TeleSign, de repérer d'éventuels hauts risques (« red flags »).

19. TeleSign évalue également la vélocité du numéro (« phone number velocity »). Cela concerne l'usage et l'activité associée à un numéro de téléphone, par exemple si ce numéro a été vu plusieurs fois sur un ou plusieurs sites web endéans une période de temps relativement courte.

20. TeleSign détecte ensuite les comportements inhabituels et procède à une vérification de l'historique des fraudes sur un numéro de téléphone.

21. TeleSign délivre enfin un score consistant en un niveau de risque et une recommandation relative au numéro. Ce score varie de 0 à 1000 et aide à les applications web ou mobile (les clients de TeleSign) dans leur processus de décision de bloquer, d'autoriser ou de marquer un utilisateur dans la procédure de création de compte. Si le score permet de considérer que l'utilisateur devrait être vérifié, TeleSign peut alors vérifier l'utilisateur au moyen d'un code envoyé par SMS ou au moyen d'un appel.

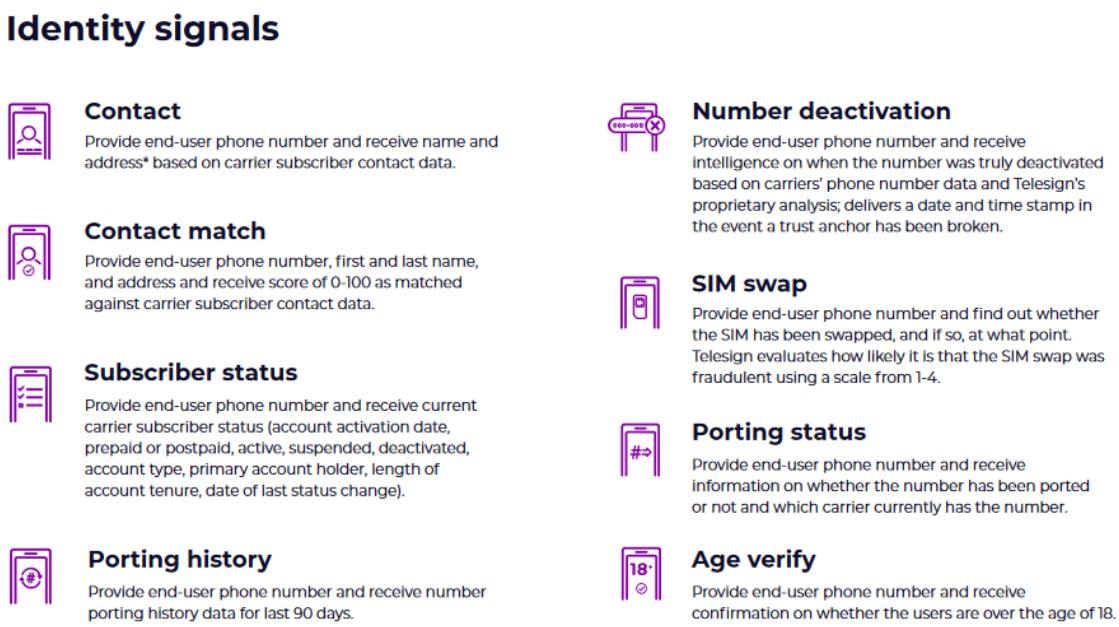
22. Outre ce service « Intelligence API », TeleSign offre également, parmi d'autres services, des informations concernant les utilisateurs des clients de TeleSign au moyen d'un numéro de téléphone, comme le montre l'extrait ci-dessous. TeleSign offre ce service « Identity signal » via son service Phone ID API.[14]

---

[12] https://www.telesign.com/products/intelligence

[13] https://www.telesign.com/press/media-alert-telesign-demonstrates-comprehensive-line-of-digital-identity-solutions-at-money-20-20-amsterdam

[14] « Phone ID identity signals allow you to find out many kinds of information associated with a phone number » : voir https://developer.telesign.com/enterprise/docs/phone-id-get-started-with-identity-attributes. Voir également Pièce 12, accédée le 20 mars 2022.



23. Comme le montre le descriptif, TeleSign peut, à la demande de ses clients (le fournisseur de l'application mobile ou web, comme TikTok, Skype, ou Salesforce) :
    - fournir le nom de l'utilisateur ;
    - vérifier si le nom, le numéro de téléphone et l'adresse de l'utilisateur correspondent aux données détenues par TeleSign, qui délivre dans ce cas un score de 0 à 100 ;
    - déterminer quel est le statut de l'utilisateur sur le réseau : actif, désactivé, suspendu, durée d'activation du numéro ; et
    - déterminer si l'utilisateur a plus de 18 ans ou non.

24. TeleSign fournit également d'autres services, lesquels seraient, toujours selon TeleSign, liés à la prévention de la fraude, comme le service de vérification, qui permet notamment la prévention de la fraude « IRSF » (International Revenue Share Fraud) ou un service de vérification des utilisateurs par envoi d'un mot de passe par SMS.

2.2.3 Proximus

25. En octobre 2017, BICS a fait l'acquisition de TeleSign pour 230 millions de dollars. En 2021, Proximus a acquis la totalité des parts de BICS pour une valeur de 569 millions d'euros. BICS et TeleSign sont donc des filiales entièrement contrôlées par Proximus.

26. Proximus est l'opérateur historique en Belgique et fournit des solutions de communication en Belgique (via Proximus, Scarlet et Mobile Vikings), en Europe (via Tango, Telindus) et dans le monde entier au travers de ses filiales BICS et Telesign.

27. Avec 11634 employés, le groupe Proximus a réalisé un chiffre d'affaires de 5,909 milliards d'euros en 2022.[15]

2.3 Les traitements faisant l'objet de la plainte

28. Un article de presse dans le journal *Le Soir* du 22 mars 2022 a révélé que Proximus transférait les données de ses clients à sa filiale américaine TeleSign, via son autre filiale BICS (Pièce 3).

29. Selon *Le Soir*, et comme cela est confirmé ci-dessus, TeleSign utilise un algorithme pour attribuer un score à chaque numéro de téléphone et ainsi mesurer la fiabilité de ces numéros de téléphone.

30. Suite à ces articles, les plaignants, résidant dans différents pays de l'Union Européenne, ont introduit des demandes d'accès sur la base de l'article 15 du RGPD auprès de leur opérateur mobile, de BICS et de TeleSign, pour obtenir des informations sur les traitements en question. Les paragraphes qui suivent exposent de manière synthétique les informations obtenues par les plaignants concernant les traitements dont ils ont fait –et font probablement toujours- l'objet. Ces traitements concerner principalement (ou uniquement ?) le service « Intelligence API » (anciennement « score ») comme le montrent les réponses fournies par TeleSign aux demandes d'accès des plaignants.

2.3.1 Réponse de Proximus

31. Proximus a répondu aux plaignants [redacted] et [redacted] qu'elle ne transmettait pas directement de données à TeleSign mais bien à BICS pour les besoins d'interconnexion (Pièces 4).

32. Proximus a en outre envoyé aux plaignants concernés une copie de clauses contractuelles types (« SCC ») qu'elle aurait signées avec un autre responsable du traitement ou sous-traitant aux Etats-Unis (Pièce 5), après avoir pris soin de noircir les champs relatifs à la description des données transférées, au noms des parties, aux pays où les données sont transférées, ou encore le nom de l'autorité compétents auprès de laquelle les personnes concernées pourraient exercer leurs droits. Proximus s'est retranchée à cet effet derrière un prétendue confidentialité d'informations commerciales à cet égard.

33. Suite à une relance de la part des plaignants, Proximus s'était engagée à revenir vers eux au mois de juin 2022 pour satisfaire à leur demande d'accès, mais ces derniers sont restés sans nouvelles depuis.

2.3.2 BICS

34. Les réponses données par BICS aux plaignants dans le cadre de la demande d'accès permettent de relever les points qui suivent (Pièces 6).

[15] Rapport annuel 2022 de Proximus, p. 19.

35. BICS confirme être le responsable du traitement en cause. BICS confirme également transférer à sa filiale TeleSign certaines informations spécifiques pertinentes pour le contrôle et la détection des fraudes. BICS envoie, parmi ces informations, le numéro de téléphone des utilisateurs, lesquels sont cryptés et hachés avant l'envoi. BICS envoie également à TeleSign « quelques informations spécifiques qui sont pertinentes dans le cadre des efforts de BICS pour le contrôle et la détection de la fraude ».[16]

    BICS déclare se baser sur « un intérêt légitime à détecter et combattre les cas de fraude dans les télécommunications ». Selon BICS, les données proviennent uniquement des opérateurs mobiles des plaignants, si ces derniers ont décidé d'utiliser BICS pour les besoins de routage des appels.[17]

36. BICS déclare également mettre en place les mesures supplémentaires suivantes entourant le transfert des données vers TeleSign aux Etats-Unis, pour se conformer aux termes de l'arrêt *Schrems II* de la Cour de justice de l'UE :
    - minimisation des données ;
    - pseudonymisation ;
    - encryptage ;
    - transfert via un protocole SFTP ;
    - stricte politique d'accès aux données ; et
    - accès aux fichiers et droits d'audit. [18]

37. Les transferts de BICS à TeleSign sont encadrés par des SCCs, lesquelles auraient –toujours selon BICS- été adaptées peu avant sa réponse pour utiliser les nouvelles SCCs adoptées par la Commission Européenne (Pièce 7). Ces SCCs ont été communiquées aux plaignants et sont décrites ci-dessous.

38. Les SCCs utilisent le module 1 « responsable du traitement à responsable du traitement » et le module 2 « responsable du traitement à sous-traitant » et datent du 1er décembre 2021. Aucune version des SCCs en vigueur avant cette date n'ont été transmises aux plaignants. Ces SCCs sont signées en tant qu'addendum à « un ou plusieurs accords principaux », en ce inclus le « Data processing agreement » (voir page 1 des SCCs, Pièce 7).

39. Le **module 1** concerne le transfert de données de BICS (en tant que responsable du traitement) à TeleSign (en tant que responsable du traitement) à des fins d'exécution des « divers accords entre sociétés tels que décrits dans la table » de l'Annexe I.B du module 1. La dernière ligne de ladite table se réfère uniquement à un « Schedule 9 » sans autre explication, et déclare porter sur les « données des utilisateurs finals » à des fins « d'amélioration du service de scoring de TeleSign ».

40. Le **module 2** concerne le transfert de données de BICS (en tant que responsable du traitement) à TeleSign (en tant que sous-traitant). Le module 2 se contente de dire que l'importateur des données (TeleSign) peut traiter les données en accord avec les finalités décrites dans l'accord principal, et plus généralement à la fourniture dudit service à l'exportateur des données (BICS)

[16] Voir par exemple réponse à [redacted], Pièce 6.3. BICS confirme également envoyer le numéro de téléphone des personnes concernées, avec les informations spécifiques dérivées des activités observées sur le réseau de BICS : voir par exemple réponse donnée à [redacted], Pièce 6.10.

[17] Voir par exemple Pièce 6.3.

[18] Voir par exemple Pièce 6.3.

et la détection et réduction des fraudes. Les personnes concernées n'ont pas reçu cet accord principal auquel se réfère le module 2 et ne sont pas au courant d'autres finalités qui seraient poursuivies.

41. Les deux modules désignent l'autorité belge de protection des données comme autorité compétente (voir Annexes I.C des deux modules des SCCs, Pièce 7).

2.3.3 TeleSign

42. Les plaignants ont également adressé des demandes d'accès à TeleSign, auxquelles cette dernière a répondu (Pièces 8). Ces réponses sont résumées ci-dessous.

a) Données traitées

43. TeleSign a confirmé traiter le numéro de téléphone des plaignants lors de la demande d'accès, et avoir généré un score lié à ce numéro (Pièces 8). Pour l'une des plaignantes, les données traitées incluaient également le type de numéro de téléphone (mobile), le nom de l'opérateur et le pays de cette dernière (voir Pièce 8.1, réponse à [redacted]).

44. À titre d'exemple, la plaignante [redacted] a reçu le score qui lui était attribué ainsi que les informations suivantes de la part de TeleSign (voir Pièce 8.1, réponse à [redacted]):

> *Scores = Ranging between 1 - 300*
>
> *Reason codes = Ranging from:*
>
> • *low activity; pp: low number of completed calls, irregular call duration, no long-term activity, no range activity*
>
> • *low activity; p2p: low number of completed calls, regular call duration, no long-term activity, no range activity*
>
> • *low activity; p2p: low number of completed calls, regular call duration, sparse long-term activity, no range activity*
>
> • *low activity; p2p: very low number of completed calls, irregular call duration, no long-term activity, no range activity*
>
> • *low activity; p2p: very low number of completed calls, irregular call duration, sparse long-term activity, no range activity*
>
> • *low regular activity; p2p: low number of completed calls, regular call duration, no long-term activity, no range activity, low successful outgoing traffic*
>
> • *low regular activity; p2p: regular number of completed calls, regular call duration, no long-term activity, no range activity, low successful incoming traffic*
>
> • *regular activity; p2p: high number of completed calls, regular call duration, sparse long-term activity, no range activity*
>
> • *regular activity; p2p: low number of completed calls, regular call duration, sparse long-term activity, no range activity*

• regular activity; p2p: regular number of completed calls, regular call duration, no long-term activity, no range activity

• regular activity; p2p: regular number of completed calls, regular call duration, sparse long-term activity, no range activity

In translation, this means that the Phone Number was recommended as "medium - low" risk level.

45. En outre, la plaignante [redacted] a été informée que les données additionnelles suivantes la concernant ont été traitées, dans le cadre d'un service SMS de Amazon, pour lequel la plaignante en question n'a pas reçu plus d'informations.

To support the Telesign Customer, Amazon Services LLC's request for SMS Services, the following additional data points (see source below) were generated:
o Phone type = Mobile
o Carrier Name = T-Mobile Austria GmbH
o Country = AustriaThe access requests

b) Transferts opérés

46. **TeleSign confirme avoir reçu les données en question de BICS** (le numéro de téléphone étant haché). TeleSign a également informé les plaignants qu'elle utilisait les SCCs de la Commission européenne pour les transferts avec BICS (vers laquelle elle semble également envoyer des données) en tant que client de TeleSign ayant demandé le score, pour la prévention des fraudes par BICS.

47. Dans ses réponses aux plaignants, TeleSign confirme en outre **partager les données avec Amazon Web Services (AWS) en tant que sous-traitant de TeleSign**, et utiliser des SCCs à cet effet. TeleSign ajoute que les données sont partagées avec AWS dans le contexte des services de prévention des fraudes en temps réel fourni aux clients de TeleSign via son algorithme de réputation des numéros de téléphone mobile.

48. TeleSign a communiqué aux plaignants les SCCs datées du 12 décembre 2016 entourant le transfert de données vers AWS (Pièce 9).

- Ces SCCs sont celles adoptées par la Commission européenne dans sa décision 2010/87 du 5 février 2010, laquelle a été abrogée en date du 26 septembre 2021. En outre, le document ne précise pas si l'exportateur des données, TeleSign ici, agit en tant que responsable du traitement, de sous-traitant, ou à ces deux titres.
- La Clause 2 se réfère aux opérations de traitement suivantes : « Compute, Storage and Content Delivery on the AWS Network » sans autre précision.
- L'Appendix 2 renvoie à des mesures de sécurité décrites dans un addendum non transmis aux plaignants.

49. En ce qui concerne les données de [redacted] et de [redacted], **TeleSign ajoute que leurs données sont également partagées avec Microsoft**, en tant que client de TeleSign, « pour des

services de détection et de prévention des fraudes » (Pièce 8.4 et 8.7). TeleSign a conclu des SCCs avec Microsoft concernant ce transfert (Pièce 11).

- Ces dernières reproduisent les SCCs de la décision 2010/87 précitée, laquelle a été abrogée en septembre 2021. La Clause 9 détermine le droit applicable en fonction de l'Etat Membre où l'exportateur est établi, à savoir Microsoft, lequel est établi à Redmond aux USA (qui n'est jusqu'à preuve du contraire pas un Etat membre de l'UE).
- Le point 6 de l'Appendix 1 se réfère aux opérations de traitement couverts par les SCCs et stipule notamment que Microsoft, exportateur des données, interroge les services de TeleSign pour accéder un ou plusieurs services de prévention des fraudes. Le reste de la description des opérations de traitement est noirci et rendu illisible sans explication.
- Concernant la description des mesures de sécurité appelées à figurer dans l'Appendix 2 des SCCs : le texte les décrivant est également noirci.

50. Quant à la plaignante [redacted], TeleSign indiquait que **son numéro de téléphone avait également été communiqué par Amazon Services LLC** pour les services SMS, et que les données additionnelles la concernant provenaient de Telcordia Technologies Inc.

51. TeleSign a également fourni une copie des SCCs encadrant les transferts avec la société Amazon Services LLC (Pièce 10). Toutefois, le document joint est une pure copie des SCCs de la Commission européenne, sans avoir été aucunement rempli, signé, daté, et sans même avoir indiqué quels modules étaient pertinents ou qui était l'exportateur et l'importateur des données. À ce jour, la plaignante n'a pas reçu davantage d'informations quant à ce transfert.

c) Intérêt légitime et destinataires des informations collectées par TeleSign

52. TeleSign a également indiqué qu'elle invoquait l'intérêt légitime au sens de l'article 6(1)(f) du RGPD pour traiter les données, à des fins spécifiques de *« prévention de la fraude, de protection contre le spamming ou le phishing, les abus de promotions, les faux comptes, l'usurpation de comptes et autres attaques onéreuses »* (voir par exemple réponse à [redacted], voir Pièce 8.3).

53. TeleSign n'a pas informé les plaignants du nom des clients avec lesquels elle aurait partagé le numéro des plaignants. TeleSign précise toutefois –sans plus d'explications- que si les numéro n'ont pas été partagés avec d'autres entités, ils sont néanmoins susceptibles d'être envoyés vers des clients de TeleSign auxquels les plaignants souscriraient et qui demanderait à TeleSign leur score dans ce contexte.[19]

[19] "Data has not been disclosed further but the Score in relation to your Phone Number could be transferred to other TeleSign customers to which you would subscribe and who would in this context request our Score for your number for fraud prevention".

3. FONDEMENTS DE LA PRESENTE PLAINTE

3.1 Violation par Proximus du droit d'accès des plaignants et de son obligation de transparence (articles 12, 13 et 15 du RGPD)

54. Comme mentionné ci-dessus, les plaignants [redacted] et [redacted] ont tous les deux introduit une demande d'accès sur la base de l'article 15 du RGPD auprès de Proximus concernant les données envoyées aux Etats-Unis, et notamment quelles bases légales et garanties appropriées étaient utilisées (Pièces 4).

55. Proximus a répondu à ces deux plaignants que les données étaient envoyées en vertu de SCCs attachées à l'email de réponse et en indiquant une liste des catégories de destinataires localisés aux Etats-Unis vers lesquelles les données « pourraient » être transférées. Proximus indique également que selon elle *« le RGPD permet de se limiter à des catégories de destinataires et n'impose pas à Proximus de dévoiler des informations confidentielles, telles son réseau de fournisseurs, vous trouverez en annexe une copie d'un exemple concret de SCC (en l'espèce, les nouvelles SCC) pour un transfert de données aux États-Unis, dans laquelle diverses informations ont été masquées. »*

56. **Premièrement**, il convient d'observer que Proximus fait une lecture erronée du RGPD. En effet, conformément à la jurisprudence de la CJUE, il convient de communiquer à la personne concernées la liste concrète des destinataires de ces données, afin qu'ils puissent vérifier qui sont les destinataires ayant reçu les données, mais également exercer leurs droits auprès de ces destinataires. [20] En outre, on constatera que le libellé de l'article 15.1.c du RGPD se réfère spécifiquement aux destinataires établis dans un pays tiers.

57. **En second lieu**, la première réponse de Proximus aux deux plaignants en question se réfère à quatre bases légales sans préciser les données traitées pour chaque base légale et pour quelles finalités précises. Cela rend impossible une compréhension entière des traitements de données faisant l'objet des transferts.

58. La CJEU a pu rappeler à cet égard que au nombre des principes de l'article 5 du RGPD *« figure le principe de transparence visé à l'article 5, paragraphe 1, sous a), du RGPD, qui implique, ainsi qu'il ressort du considérant 39 de ce règlement, que la personne concernée dispose d'informations sur la manière dont ses données à caractère personnel sont traitées et que ces informations soient aisément accessibles et compréhensibles »*.[21] Force est de constater que tel n'est pas le cas en l'espèce : il est impossible de comprendre quelles données sont effectivement transférées, à quelles finalités et ce sur quelle base légale précise au sens de l'article 6 du RGPD. Ce faisant, Proximus viole dès lors son obligation de transparence et à tout le moins les articles 13 et 15 du RGPD.[22]

59. **De plus**, Proximus se retranche derrière l'excuse selon laquelle *« les clauses communiquées étaient des exemples de clauses signées dans le cadre d'autres d'activités de traitement ».* Or, la

[20] Arrêt *RW* c. *Österreichische Post AG*, C-154/21 du 13 janvier 2023.

[21] Arrêt *RW* c. *Österreichische Post AG*, C-154/21 du 13 janvier 2023, § 35.

[22] A ce sujet, voir notamment la décision 4/2022 de l'EDPB du 5 décembre 2022 concernant Instagram, et plus particulièrement les §§234 et 346.

demande faite à Proximus concerne bien les transferts de données ayant effectivement eu lieu vers les Etats-Unis, et les garanties adoptées dans ce cadre, et non des transferts hypothétiques ou qui pourraient éventuellement concerner les données des plaignants concernés.[23] Ce faisant, Proximus a notamment violé l'article 15 du RGPD et plus particulièrement son §1 (c).

60. **En outre**, on ne voit aucunement à quelle obligation de confidentialité Proximus serait tenue et qui l'empêcherait de communiquer les éléments essentiels des transferts couverts par les SCCs, comme la description des traitements concernés, les destinataires des données, ou l'autorité de contrôle compétente auprès de laquelle se plaindre. En résumé, Proximus a noirci tellement d'informations dans les SCCs communiquées qu'il est impossible pour les plaignants de comprendre ce qu'il advient de leurs données et comment elles sont protégées par les SCCs. Proximus ne peut se retrancher derrière une obligation de confidentialité -qu'elle n'a d'ailleurs ni justifiée ni explicitée[24]- pour communiquer des SCCs qui apparemment ne couvriraient pas les transferts des données des plaignants mais concerneraient « d'autres activités de traitement ». L'exception de confidentialité ne s'applique d'ailleurs qu'à la fourniture de la copie des données en vertu de l'article 15.4 du RGPD, mais non aux informations relatives au traitement.[25]

61. **Enfin**, malgré l'engagement du 3 juin 2022 de Proximus de revenir vers les deux plaignants susmentionnés « avec plus d'informations endéans les délais légaux applicable à leur nouvelle requête », ces deux derniers n'ont jamais reçu de retour de la part de Proximus. Le délai maximum pour répondre à une telle requête étant d'un mois en vertu de l'article 12(3) du RGPD. Ce délai est donc largement dépassé sans aucune justification de la part de Proximus.

62. Pour les raisons qui précèdent, Proximus a notamment violé:

- l'article 12 du RGPD en ne répondant pas aux plaignants concernant leur demande additionnelle d'informations dans les délais légaux, mais également en ne leur fournissant pas une information concise, transparente, compréhensible et aisément accessible, comme il est démontré ci-dessus ; et

- ses obligations de transparence au sens des articles 5.1.a, 13 et 15 du RGPD, en ne soumettant pas toutes les informations prescrites par ces dispositions, et notamment celles portant sur les transferts opérés hors de l'Union Européenne.

63. Au vu de ce qui précède, il est demandé à l'APD d'ordonner à Proximus, sans préjudice d'autres mesures correctrices en ce inclus une amende, de fournir les informations aux questions des plaignants concernant le transfert de leurs données aux Etats-Unis sur la base des articles 13 et 15 du RGPD.[26]

---

[23] Voir les Lignes directrices du WP29 du 29 novembre 2017 endossées par l'EDPB le 11 avril 2018, §13 : l'utilisation du conditionnel, comme dans le cas d'espèce, rend difficile voire impossible pour les personnes concernées de savoir sir leurs données sont effectivement ou non traitées de la manière décrite.

[24] Voir les Questions Réponses de la Commission européenne concernant les SCCs, qui confirment que les personnes concernées ont non seulement le droit d'obtenir copie des clauses, mais également le détail des transferts qu'elles couvrent, et que la confidentialité ne peut être soulevée qu'à des conditions strictes et justifiées : https://commission.europa.eu/system/files/2022-05/questions_answers_on_sccs_en.pdf, question 32.

[25] Voir Lignes directrices 01/2022 de l'EDPB du 18 janvier 2022, notamment § 166.

[26] Pour le bon ordre, les informations demandées ne concernent que les transferts aux Etats-Unis.

3.2 Le traitement de données opéré par BICS

64. BICS confirme dans ses réponses aux plaignants (Pièces 6) que BICS agit en tant que responsable du traitement et envoie les données à sa filiale TeleSign pour le contrôle et la détection des fraudes (« fraud monitoring and detection »).

65. Les SCCs signées avec TeleSign et mentionnées plus haut (voir Section 2.3.2, Pièce 7) se réfèrent quant à elles aux finalités suivantes :

- amélioration du produit Score de TeleSign (« improvement of TeleSign's score product ») pour lesquelles les données sont transférées à TeleSign qui agit en tant que responsable du traitement ;
- assistance aux capacités de BICS pour la prévention et la détection des fraudes (« assistance to BICS's fraud prevention capabilities ») pour lesquelles les données sont transférées à TeleSign qui agit en tant que sous-traitant de BICS.

3.2.1 Manquement à l'obligation d'information

66. BICS n'a jamais informé les utilisateurs du traitement de leurs données ni de l'existence d'un transfert de leurs données à TeleSign. En ne fournissant aucune information aux utilisateurs, BICS n'a pas rempli ses obligations de transparence, et notamment celles prévues à l'article 14 du RGPD, notamment en n'informant pas les abonnés :
- de son identité ;
- de l'identité de son DPO ;
- des finalités du traitement et la base juridique ;
- des catégories de données traitées et envoyées à TeleSign ;
- du ou des destinataires des données, en ce compris TeleSign ; et
- de l'existence d'un transfert de données hors de l'UE, et des garanties appropriés utilisées.

67. Par conséquent, BICS a violé son obligation d'information et de transparence et notamment les articles 5.1.a et 14 du RGPD.

3.2.2 Utilisation illicite des données et détournement de finalité

a) Rappel du cadre légal concernant l'utilisation des données de communications électroniques

68. BICS, tout comme Proximus, sont des opérateurs soumis à la loi du 13 juin 2005 relative aux communications électroniques. Cette loi transpose notamment en droit national la directive « vie privée et communications électroniques »[27] et définit de manière stricte les conditions auxquelles les données de communications peuvent être traitées par les opérateurs de communications électroniques.

69. L'article 122 §1 de la loi du 13 juin 2005 dispose que *« Les opérateurs suppriment les données de trafic concernant les abonnés ou les utilisateurs finaux de leurs données de trafic ou rendent ces données anonymes, dès qu'elles ne sont plus nécessaires pour la transmission de la communication ».*

[27] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

70. L'article 122 prévoit quelques dérogations limitées à l'interdiction du §1, et qui permet aux opérateurs de conserver les données en question sans préjudice du RGPD et du devoir d'informer les utilisateurs du type de données traitées, des objectifs précis et de la durée du traitement:

    - aux seules fins de facturation et de paiement de l'interconnexion, (voir article 122 §2 de la loi du 13 juin 2005),
    - à des fins de marketing et de proposer un meilleur plan tarifaire aux utilisateurs, avec leur consentement (voir article 122§3 de la loi du 13 juin 2005),
    - aux fins de prendre des mesures appropriées, proportionnées, préventives et curatives, compte tenu des possibilités techniques les plus récentes, de manière à détecter les fraudes et utilisations malveillantes sur leurs réseaux et services et éviter que les utilisateurs finaux ne subissent un préjudice ou ne soient importunés (article 122 §4 *juncto* article 121/8 §1 de la loi du 13 juin 2005),
    - aux fins de permettre d'établir la fraude ou l'utilisation malveillante du réseau ou du service ou d'identifier son auteur et son origine, et pour autant qu'il les traite ou les génère dans le cadre de la fourniture de ce réseau ou de ce service (article 122 §4 de la loi du 13 juin 2005).

71. Dans tous les cas, l'article 122 §5 dispose que *« les données énumérées dans le présent article ne peuvent être traitées que par les personnes chargées par l'opérateur de la facturation ou de la gestion du trafic, du traitement des demandes de renseignements des abonnés, de la lutte contre les fraudes ou l'utilisation malveillante du réseau, de la sécurité du réseau, du respect de ses obligations légales, du marketing des services de communications électroniques propres ou de la fourniture de services qui font usage de données de trafic ou de localisation ».*

72. Notons également que l'article 123 de la même loi prévoit que les opérateurs de réseaux mobiles peuvent conserver des données de localisation autres que des données de trafic dans les cas suivants:
    - lorsque cela est nécessaire pour le bon fonctionnement et la sécurité du réseau ou du service, les données étant conservées le temps nécessaire à cette fin ;
    - lorsque cela est nécessaire pour détecter ou analyser les fraudes ou l'utilisation malveillante du réseau, les données étant conservées le temps nécessaire à cette fin ;
    - lorsque les données ont été rendues anonymes ;
    - lorsque le traitement s'inscrit dans le cadre de la fourniture d'un service à données de trafic ou de localisation et que l'abonné ou, le cas échéant, l'utilisateur final, y a donné son consentement ;
    - lorsque le traitement est nécessaire pour répondre à une obligation légale dans le chef de l'opérateur .

73. La loi 20 juillet 2022 entrée en vigueur le 18 août 2022 définit d'ailleurs la notion de « fraude » comme *« un acte malhonnête fait dans l'intention de tromper en contrevenant à la loi, aux règlements ou au contrat et de se procurer ou de procurer à autrui un avantage illicite au préjudice de l'opérateur ou de l'utilisateur final, commis par le biais de l'utilisation d'un service de communications électroniques ».*

74. Il est à cet égard renvoyé à l'avis critique de l'APD concernant les exceptions mentionnées ci-dessus et introduites par la loi du 20 juillet 2022.[28] L'avis rappelle notamment que simple potentialité d'une fraude ne pouvait « *justifier une conservation préventive systématique des données de trafic de l'ensemble des utilisateurs d'un moyen de communication électroniques nécessaires à la lutte contre la fraude et l'utilisation malveillante du réseau* ». [29]

b) Le traitement des données opéré par BICS au regard des principes rappelés ci-dessus

75. Il ressort des informations reçues par les plaignants que BICS non seulement ne supprime pas les données des utilisateurs, mais les transmets à TeleSign pour d'autres finalités que la transmission de la communication, en violation flagrante des articles 122 et suivants de la loi du 13 juin 2005.

76. Dans ses réponses aux demandes d'accès des plaignants, (Pièces 6) BICS invoque son intérêt légitime et la détection et la prévention des fraudes comme base de licéité pour le transfert des données vers TeleSign.

77. Or, le transfert des données vers TeleSign et leur utilisation pour l'attribution de scores aux numéros de téléphone et d'autres finalités obscures de « prévention de la fraude » ne répondent pas aux exceptions prévues aux §§ 2 et suivants de l'article 122 de la loi du 13 juin 2005, lesquelles sont d'interprétation stricte. En effet, il convient notamment de considérer les éléments suivants :

- le transfert systématique et massif[30] de tous les numéros de téléphone à TeleSign afin que cette dernière attribue un score à tout numéro n'est pas proportionné : il revient à ficher l'ensemble des utilisateurs dont les communications transitent par BICS, alors même qu'un telle rétention systématiques des données à des fins de police et de justice n'est admise qu'à des conditions très strictes,[31]
- le service de scoring de TeleSign n'a pas vocation à détecter les fraudes et utilisations malveillantes sur leurs réseaux et services et éviter que les utilisateurs finaux ne subissent un préjudice ou ne soient importuné, mais plutôt à traiter l'ensemble des données de trafic pour en générer un revenu considérable et vendre une solution à des clients qui ne sont pas des opérateurs de communications électroniques sous le couvert de « prévention des fraudes »[32], et
- les données ne sont pas traitées ou générées dans le cadre de la fourniture de ce réseau ou de ce service mais pas un tiers pour des utilisations étrangères au fonctionnement des réseaux et services de communications électroniques.

---

[28] Avis n°108/2021 de l'APD du 18 juin 2021.

[29] Selon l' avis de l'APD (n°108/2021, p. 31), "*toute personne peut, potentiellement, commettre un « fraude» ou une «utilisation malveillante du réseau » ou, en être victime, mais cette potentialité – qui existe également pour les crimes graves dont la lutte constituait l'objectif de la règlementation sur laquelle portait l'arrêt de la CJUE – ne peut, au regard de la jurisprudence de la CJUE, être jugée suffisante pour justifier une conservation préventive systématique des données de trafic de l'ensemble des utilisateurs d'un moyen de communication électroniques nécessaires à la lutte contre la fraude et l'utilisation malveillante du réseau* ».

[30] Et encadré par des SCCs et une obligation contractuelle pour BICS de fournir ces données à TeleSign.

[31] CJEU, arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, Arrêts du 6 octobre 2020, Privacy International, C-623/17, et La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, Cour Const., arrêt du 22 avril 2021, 54/2021.

[32] Notons que le Module 1 « responsable du traitement à responsable du traitement » utilisé pour le transfert de données de BICS vers TeleSign mentionne « l'amélioration du produit score de TeleSign ». Voir page 13 des SCCs entre BICS et TeleSign, Pièce 7.

78. Notons en outre que BICS que le choix des SCCs « responsable du traitement vers responsable du traitement », en sus de SCCs « responsable du traitement vers sous-traitant » permet à TeleSign de définir elle-même les finalités et moyens de traitement de ces données, sans aucune base légale, information aux utilisateurs, ou dérogation aux conditions strictes entourant l'utilisation des données communications électroniques précitées.

79. Par conséquent, BICS a violé à tout le moins :

- l'article 5.1.e) du RGPD et l'article 122 de la loi du 13 juin 2005 en conservant les données pour une durée excédant la durée de conservation nécessaire à la fourniture des services d'interconnexion ;
- les articles 5.1.b) et c) et 6 du RGPD en utilisant les données des utilisateurs pour des finalités incompatibles avec les utilisations permises en vertu de l'article 122 de la loi du 13 juin 2005.

3.2.3 Transfert de données vers TeleSign non conforme au RGPD

80. BICS a procédé au transfert de données vers TeleSign, fournisseur de services de communication électronique au sens du §1881a du titre 50 du U.S. Code et, à ce titre, est soumis à la surveillance des services de renseignement américains en vertu du §1881a du titre 50 du U.S. Code ("FISA 702").

81. Or, la CJUE dans son arrêt *Schrems II*[33], a explicitement conclu que les transferts ultérieurs à des sociétés relevant du §1881a du titre 50 du U.S. Code non seulement violent les articles pertinents du chapitre 5 du RGPD mais aussi les articles 7 et 8 de la Charte des Droits Fondamentaux ainsi que l'essence de l'article 47 de la même Charte.[34] Tout nouveau transfert viole donc le droit fondamental au respect de la vie privée, à la protection des données et au droit à un recours effectif et à un procès équitable.

82. En vertu de l'arrêt *Schrems II* précité, les SCCs ne peuvent garantir le transfert de données sans garantie supplémentaire les protégeant contre l'accès par les autorités américaines de surveillance en vertu de leur droit national (voir points 134 et 135 de l'arrêt).

83. Toutefois, comme il a déjà été soulevé ci-dessus, selon les informations fournies par BICS elle-même, les mesures supplémentaires pour garantir la protection des données se résument aux mesures suivantes :

- minimisation des données ;
- pseudonymisation ;
- encryptage ;
- transfert via un protocole SFTP ;
- stricte politique d'accès aux données ; et
- accès aux fichiers et droits d'audit.

[33] Décision de la CJUE, 20 juillet 2020, C-311/18.

[34] Voir §95 de la décision *Schrems II*.

84. Il est impossible de conclure que ces « mesures supplémentaires » (par ailleurs fort vaguement décrites, et qui ressemblent plus à des mesures de sécurité de base pour un traitement de ce genre) garantissent l'absence d'accès par les autorités américaines compétentes aux données envoyées par BICS à TeleSign.

85. BICS a donc violé les articles 44 et suivant du Chapitre V du RGPD, en transférant des données sans garanties appropriées.

86. Selon l'arrêt *Schrems II*, l'autorité de contrôle compétente doit suspendre ou mettre fin au transfert de données à caractère personnel vers le pays tiers concerné en vertu de l'article 58.2, f) et j) du RGPD (voir les paragraphes 134 et 135 de l'arrêt).

87. En outre, comme développé ci-dessus (section 3.2.2), BICS a procédé à un transfert massif, récurrent, et répété de données vers TeleSign, en vertu de SCCs (Module1) donnant à TeleSign la qualité de responsable du traitement pour une finalité totalement incompatible avec la loi du 13 juin 2005. Dès lors, l'intérêt légitime de lié à la détection et la prévention des fraudes invoqué par BICS ne peut justifier un tel transfert de données vers TeleSign. BICS viole donc également les articles 6 et 14 du RGPD, en procédant à un traitement (le transfert en question) sans aucune base légale et sans information des utilisateurs.

3.3 Le traitement de données opéré par TeleSign

3.3.1 TeleSign a manqué à ses obligations d'information auprès des plaignants

88. Tout d'abord, il convient de constater que ce n'est que grâce aux révélations du journal *Le Soir* (voir ci-dessus, section 2.3) que les plaignants ont été informés qu'ils étaient fichés et profilés par une société américaine dont ils n'avaient jamais entendu parler. Et pour cause : TeleSign ne les avait jamais informés du traitement dont ils faisaient l'objet.

89. Suite à leurs demandes d'accès, ils se sont en outre rendu compte –à leur plus grande surprise- que cette société leur attribuait en effet un score, lequel était partagé avec les clients de TeleSign, toujours sans qu'ils en soient informés (voir réponses aux plaignants, Pièces 8).

90. TeleSign a procédé au traitement de données millions d'utilisateurs de téléphonie sans même leur fournir ce serait-ce que le début d'une information quant à ce traitement. Or, l'article 14 du RGPD est on ne peut plus clair quant à l'obligation d'information des personnes concernées. Il en est de même de l'article 8.2 des SCCs signées avec BICS qui impose à l'importateur des données, à savoir TeleSign d'informer les personnes concernées, afin de leur permettre d'exercer effectivement leurs droits en vertu de l'article 10 des SCCs. Sans information, et sans information par voie de presse, les plaignants seraient encore dans l'ignorance des traitements en cause dans cette plainte.

91. Plus encore, lorsque plusieurs plaignants sont revenus vers TeleSign en 2023 pour obtenir l'ensemble des informations légalement requises en vertu de l'article 15 du RGPD, TeleSign a répondu que les données de ces plaignants avaient été supprimées, et que TeleSign n'étaient dès

lors plus en état de répondre à la question de savoir combien de temps les données étaient conservées (voir par exemple réponse du 25 mars 2023 de TeleSign à [redacted], Pièce 8.3a).

92. En outre, lors de la demande de précision des plaignants sur la question de savoir pourquoi les données de la plaignante avaient été effacées et n'étaient plus considérées comme nécessaires par TeleSign, cette dernière a considéré que cette réponse allait au-delà de ses obligations en vertu de l'article 15 du RGPD.

93. Or, l'article 15.1.d du RGPD mentionne expressément que le responsable du traitement doit informer les personnes concernées sur *« lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ».* Force est de constater que TeleSign n'a pas répondu à cette demande malgré le texte clair de l'article 15.1.d du RGPD.

94. Il ressort de ce qui précède que TeleSign a donc manqué à son devoir d'information en ne fournissant aucune information avant la première demande d'accès, mais également lors des demandes subséquentes. TeleSign a donc à tout le moins violé les articles 5.1.a, 12, 14 et 15 du RGPD, et l'article 8.2 des SCCs signées avec BICS.

3.3.2 TeleSign traite les données des plaignants sans base légale valable au sens du RGPD et de la loi du 13 juin 2005 et en violation des SCCs

95. TeleSign considère traiter les données sur base de l'intérêt légitime au sens de l'article 6.1.f du RGPD, pour des raisons de *« prévention de la fraude, de protection contre le spamming, le phishing, l'abus de promotion, les faux comptes, les prises illicites de comptes et toute autre attaque entraînant des coûts »* (voir par exemple réponse à [redacted], voir Pièce 8.3).[35]

96. Cependant, en vertu des SCCs signées avec BICS, TeleSign reçoit les données de BICS pour deux finalités :

- « L'amélioration du produit Score de TeleSign » quand TeleSign reçoit les données en tant que responsable du traitement recevant les données de BICS (Pièce 7, Module 1, tableau page 13),
- « L'assistance de BICS à la prévention des fraudes » quand TeleSign reçoit les données en tant que sous-traitant recevant les données de BICS (Pièce 7, Module 2, tableau page 31).

97. Concernant l'utilisation des données à des fins d'amélioration du produit Score de Telesign, force est de constater que l'amélioration d'un produit attribuant un score de confiance n'est pas compatible avec le traitement initial des données par BICS, comme déjà développé ci-dessus (voir section 3.2.2). A l'évidence, si un traitement n'est pas compatible avec les finalités strictes prescrites par la loi du 13 juin 2005, leur simple transfert à une société tierce ne peut permettre d'en faire un usage libre non soumis aux mêmes restrictions, à défaut de vider les principes de la directive « vie privée et communications électroniques » de sa substance.[36]

---

[35] *« Our phone number reputation and risk assessment tool is offered to our customers for fraud prevention purposes; protecting against spam, phishing, promotion abuse, fake accounts, account takeovers and other costly attacks. »*

[36] Il suffirait en effet pour un opérateur soumis aux conditions strictes de la loi du 13 juin 2005 de transférer les données à un opérateur qui ne l'est pas pour faire un usage libre des données

98. En outre, alors même que l'articulation entre ces différentes finalités n'est pas claire pour les plaignants ayant reçu les informations de TeleSign, il convient de constater que TeleSign viole l'article 8.1 des SCCs (Module 1) lorsqu'elle traite les données reçues de BICS puisqu'elle les utilise à d'autres fins[37] que celles décrites dans les SCCs (« amélioration du produit score de TeleSign »).

99. Enfin, comme déjà développé (section 3.2.2), le choix des SCCs « responsable du traitement vers responsable du traitement », en sus de SCCs « responsable du traitement vers sous-traitant » est susceptible de permettre à TeleSign de définir elle-même les finalités et moyens de traitement de ces données, sans aucune base légale, information aux utilisateurs, ou dérogation aux conditions strictes entourant l'utilisation des données communications électroniques précitées.

100. En ce qui concerne « l'assistance de BICS à la prévention des fraudes », il a été déjà souligné que, au regard des informations dont les plaignants disposent, les finalités de prévention de la fraude opérée par BICS –et à tout le moins par TeleSign- ne rentrent pas dans les exceptions des §§4 et suivants de l'article 122 de la loi du 13 juin 2005. Il reste cependant difficile de faire la part des traitements pour lesquels TeleSign serait responsable du traitement ou sous-traitant, et ce malgré une mise à jour de TeleSign dans une version mise à jour en mars 2023 de sa « privacy notice », où TeleSign tente de clarifier dans quels cas elle agit en tant que sous-traitant ou responsable du traitement.

101. Il ressort de ce qui précède que TeleSign viole les articles 5.1 et 6 du RGPD, ainsi que l'article 8.1 des SCCs signées avec BICS, conjointement avec les articles 122 et suivants de la loi du 13 juin 2005.

3.3.3 TeleSign procède illégalement à un profilage et à une prise de décisions automatisées

102. TeleSign procède à une évaluation de profils d'utilisateurs de numéro de téléphone au moyen d'algorithmes pour détecter les utilisateurs avant même la création d'un compte auprès de ses clients.[38]

103. TeleSign procède donc au profilage et à la prise de décisions automatisées au sens de l'article 22 du RGPD. En effet, le produit score de TeleSign est indiscutablement un outil de profilage (lequel est en outre basé sur un traitement illégal, voir ci-dessus section 3.3.2), défini par l'article 4 du RGPD comme « *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le*

[37] « *Prévention de la fraude, protection contre le spamming, le phishing, l'abus de promotion, les faux comptes, les prises illicites de comptes et toute autre attaque entraînant des coûts ».*

[38] *« Leveraging our proprietary insight into the volume of traffic around the world and the data captured by our products, we've developed the ability to predict potential fraud based on a variety of phone attributes, machine learning algorithms, data and behavioral patterns.*

Today our expanded products and solutions allow you to both preserve your ecosystem and your user base by detecting a suspicious user before account creation and identifying and blocking account takeover attacks before they occur. », repris du site de TeleSign : https://www.telesign.com/security.

rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique. »

104. TeleSign met également un dispositif de décision automatisée au sens de ce même article 22 du RGPD. Dès lors que TeleSign établit un « score » des utilisateurs concernés et les partage avec ses « clients » qui adoptent alors une décision sur la base de ce score.

105. L'Avocat Général Pikamäe a déjà récemment considéré au sujet d'un traitement similaire que *« l'établissement automatisé d'une valeur de probabilité concernant la capacité de la personne concernée à honorer un prêt à l'avenir constitue déjà une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques concernant cette personne ou l'affectant de manière significative de façon similaire lorsque cette valeur, établie au moyen de données à caractère personnel relatives à ladite personne, est communiquée par le responsable du traitement à un tiers responsable du traitement et que, conformément à une pratique constante, celui-ci fonde sa décision relative à l'établissement, à l'exécution ou à la cessation d'une relation contractuelle avec cette même personne de manière déterminante sur ladite valeur ».*[39]

106. Ce profilage est encore plus alarmant quand on constate qu'aucun des plaignants n'avait été informé que leurs données avaient été transférées à TeleSign pour se voir profiler à leur insu. Aucune information sur le profilage n'a été donné aux personnes concernés, et les finalités précises de ce scoring sont encore floues pour les plaignants (qui sont ces clients à qui TeleSign fournit les scores, quand, pourquoi et sur quelle base ?).

107. Il ressort de ce qui précède que TeleSign a procédé (et procède encore) à un traitement illégal en vertu de l'article 22 du RGPD. Il convient d'ordonner à TeleSign de cesser un tel traitement sans préjudice de toute autre mesure correctrice appropriée à l'encontre de TeleSign.

3.3.4 Violation des règles sur les transferts hors EU

108. Pour les raisons déjà exposées ci-dessus à la Section 3.2.3, le transfert des données des utilisateurs de téléphonie vers TeleSign viole les dispositions du chapitre V du RGPD dès lors que TeleSign est une société tombant sous le coup du FISA américain.

109. Les mesures supplémentaires adoptées par TeleSign incluent celles qui suivent[40] :

- minimisation des données ;
- pseudonymisation (hashing) ;
- encryptage avec AWS ;
- transfert via un protocole SFTP ;
- stricte politique de sécurité et de vie privée ;et
- utilisation des nouvelles clauses-types de la Commission .

110. Comme déjà développé ci-dessus à la Section 3.2.3, ces mesures ne peuvent pas être considérées comme suffisantes au regard de la jurisprudence *Schrems II* de la Cour de Justice. On

[39] Conclusions de l'Avocat Général du 16 mars 2023 dans l'affaire C-634/21, *OQ c. Land Hessen*.

[40] Voir par exemple, réponses à [redacted], [redacted], ou [redacted], Pièces 8.

notera également que TeleSign mentionne les clauses-types comme des « mesures additionnelles », alors que la signature de ces clauses-types est le minimum légalement requis pour entourer le transfert de données. On ne voit donc pas en quoi elles seraient « supplémentaires ».

111. En vertu de ce qui précède, TeleSign a également violé l'article 14 des SCCs signées avec BICS pour, notamment, ne pas avoir notifié BICS de l'existence d'une législation l'empêchant de s'acquitter de ses obligations en tant qu'importateur des données.

3.3.5 Transferts ultérieurs illégaux

a) Transferts vers Microsoft

112. Comme développé ci-dessus (voir §§49 et suivants), TeleSign a transféré les données des plaignants [redacted] et [redacted] à Microsoft sur la base de SCCs communiquées aux plaignants (Pièce 11). Il est impossible de savoir notamment quand ces SCCs ont été signées, les transferts qu'elles couvrent, et les mesures de sécurité entreprises, dès lors que toutes ces informations sont tout simplement inexistantes dans le document.

113. Il est dès lors certain que ces clauses contractuelles n'apportent pas les garanties appropriées pour un transfert ultérieur des données, et en tout état de cause n'apportent pas le même niveau de protection que les clauses signées entre BICS et TeleSign. Ce transfert viole donc l'article 8.7 des SCCs en question, et plus particulièrement son article 8.7.iii).

b) Transferts vers AWS

114. Comme développé ci-dessus (§§47 et suivants), TeleSign a confirmé transféré les données avec AWS. TeleSign a partagé les SCCs datées du 12 décembre 2016 entourant ce transfert (Pièce 9). Ces SCCs mentionnent AWS comme sous-traitant.

- Ces SCCs sont celles adoptées par la Commission européenne dans sa décision 2010/87 du 5 février 2010, laquelle a été abrogée en date du 26 septembre 2021. En outre, il n'est pas précisé si l'exportateur des données, TéléSign ici, agit en tant que responsable du traitement, de sous-traitant, ou à ces deux titres.
- La Clause 2 portant sur le détail du transfert renvoie à la description de l'Appendix 1 qui mentionne juste que les catégories de données transférées sont les données au sujet des personnes qui sont chargées sur les services AWS par l'exportateur des données, sans autre précision.
- L'Appendix 2 renvoie à des mesures de sécurité qui sont décrites dans un addendum qui n'a pas été transmise aux plaignants.

115. Dans ces circonstances, il est soumis que TeleSign viole l'article 8.1 des SCCs signées avec BICS en procédant à un transfert ultérieur non conforme à ses obligations contractuelles.

c) Transferts vers Amazon LLC

116. TeleSign a également partagé avec [redacted] une copie des SCCs pour les transferts avec la société AMAZON SERVICES LLC (Pièce 10 AMAZON LLC SCCS, voir section 2.3.3). Toutefois, le document communiqué par TeleSign est une pure copie des SCCs de la Commission européenne, sans avoir été aucunement remplies, signées, dates, et sans même avoir indiqué quels modules étaient pertinents ou qui était l'exportateur et l'importateur des données. À ce jour, la plaignante n'a pas plus d'informations quant à ce transfert.

117. Dans ces circonstances, il est soumis que TeleSign viole également l'article 8.1 des SCCs signées avec BICS en procédant à un transfert ultérieur non conforme à ses obligations contractuelles.

3.3.6 Exactitude et limitation de la conservation des données

118. Conformément à l'article 8.3 des SCCs signées par TeleSign avec BICS, TeleSign a l'obligation de veiller à ce que les données soient adéquates, pertinentes et limitées à ce qui est nécessaire au regard de la ou des finalités du traitement. En outre, l'article 8.4 des mêmes SCCs disposent que l'importateur ne peut conserver les données plus longtemps que nécessaire et met en place les mesures techniques et organisationnelles pour garantir le respect de cette obligation. Dans la lignée du principe de responsabilité de l'article 5.2 du RGPD, l'article 8.9 des SCCs signées avec BICS disposent que chaque partie doit être en mesure de démontrer ses obligations qui lui incombent, notamment en documentant les activités de traitement menés sous sa responsabilité.

119. Néanmoins, il apparaît que suite à une demande supplémentaire de renseignements de la part de plusieurs des plaignants, TeleSign leur a communiqué que leurs données n'étaient plus traitées et que par conséquent, TeleSign ne pouvait plus leur indiquer quand le traitement de leurs données a commencé ni quand il a cessé (voir Pièces 8.1.a, 8.2.a, 8.3.a, 8.4.a, 8.7.a et 8.10a).

120. En outre, à la question de savoir pourquoi les données des plaignants, qui semblaient si nécessaires pour les finalités poursuivies par TeleSign (à savoir le scoring des numéros de téléphone pour leurs clients) ne l'est subitement plus au moment de la relance des plaignants auprès de TeleSign, cette dernière considère que cette information sort du champ de l'article 15 du RGPD.[41]

121. Elle précise en outre que le fait que les données ne soient plus traitées par TeleSign « n'empêche pas TeleSign de recevoir dans le futur le numéro de téléphone des plaignants de la part de leur partenaire pour leur fournir le service de scoring ». Comment et pourquoi TeleSign recevrait encore le numéro de téléphone de la part de tiers pour fournir un score sur la base d'un numéro que TeleSign prétend ne plus traiter ? TeleSign ne l'explique pas.

[41] *« While we appreciate your inquiry in this respect, it goes beyond the scope of Article 15 of the GDPR.*
We do nevertheless wish to point out that although your personal data ceased to be used for fraud prevention in the context of Score, we cannot prevent our current and future customers, with whom you share your phone number, from sharing your phone number with us (again) in connection with the services that we provide to them. »

122. En vertu du principe de responsabilité, de nécessité (sous-tendant l'article 6.1.f du RGPD) et de limitation des données, il est clair que TeleSign devrait pourvoir répondre aux questions concernant :

- la durée de conservation des données reçues. Si la réponse à cette question ne peut pas porter sur une donnée précise, la politique de conservation devrait à tout le moins permettre à TeleSign de répondre à la question conformément à l'article 14.2a. du RGPD,
- la justification de la nécessité (et *a contrario* la disparition de cette dernière) de traiter les données pour la finalité avancée (ici, la prévention des fraudes sur la base de l'intérêt légitime au sens de l'article 6.1.f du RGPD),
- la justification des éléments ci-dessus même après le traitement sur la base d'une documentation à jour décrivant les processus de traitement mis en œuvre et les conditions les entourant.

123. Sur la base de ce qui précède, il est soumis que TeleSign a violé à tout le moins les articles 5.1.e, 5.2, et 24 du RGPD, ainsi que les articles 8.3, 8.4 et 8.9 des SCCs signées avec BICS.

4. CONCLUSION

4.1 Réserves concernant la présente plainte

124. Le contenu de la présente plainte est sans préjudice de nouveaux éléments factuels ou de violations éventuelles qui seraient révélées en cours de procédure en fonction des constations et informations apportées par et à l'APD et toute autre partie en cours de procédure.

125. Eu égard au peu de transparence concernant les différents traitements concernés, il est en effet difficile pour les plaignants de comprendre ces derniers et de faire valoir adéquatement et efficacement leurs droits.

126. Il apparaît que TeleSign a mis à jour sa politique de confidentialité en mars 2023.[42] Le but annoncé par TeleSign sur sa page web est notamment de rendre cette politique plus claire, d'expliciter quand TeleSign ou ses clients agissent en tant que responsable du traitement ou de sous-traitant, et d'apporter plus de détails sur les raisons pour lesquelles TeleSign traite les données, comment elle les utilise et à quelles fins.

127. Il n'est pas exclu que TeleSign, se rendant compte des demandes des plaignants, ait non seulement changé sa « privacy notice », mais également ses pratiques, par exemple, en adoptant une politique de conservation des données ou en modifiant les traitements de données concernés. Il est dans tous les cas avancé que les changements opérés par TeleSign survenus après les demandes d'accès n'ont pas empêché que les différentes violations mentionnés dans la présente plainte ont effectivement eu lieu, et qu'elles sont susceptibles d'avoir concerné plusieurs millions d'utilisateurs, et non pas uniquement les plaignants.

128. Dans ce contexte, *noyb* se réserve également le droit de joindre de nouvelles pièces, d'ajouter des nouveaux éléments, de soulever d'autres points de droit, et de représenter d'autres plaignants dans le cadre de la présente procédure.

4.2 Demande d'enquête

129. Il est demandé à l'autorité de contrôle de procéder à une enquête sur les traitements visés par la présente plainte, et notamment

- d'obtenir confirmation que les données des plaignants ont été, ou sont encore traitées par TeleSign et pour quelles raisons ;
- d'obtenir plus d'informations sur les différents transferts opérés par BICS vers TeleSign et inversement, notamment quant à leur base légale et leurs finalités précises ;
- d'obtenir des informations complètes et intelligibles sur les opérations de traitement opérées par TeleSign à l'endroit des données des plaignants ; et
- de demander à toute autre partie non encore identifiée dans la présente plainte les renseignements nécessaires pour les besoins de l'enquête et de la résolution de la plainte.

[42] https://www.telesign.com/our-updated-privacy-notice-protecting-you-and-your-identity.

4.3 Mesures correctrices

130. Outre la reconnaissance des violations des droits des plaignants et des dispositions légales identifiées dans la présente plainte (et sous réserve d'autres violations qui seraient identifiées par les plaignants ou l'APD en cours de procédure, notamment par son service d'inspection), il convient que l'APD prononce au moins les mesures correctrices suivantes :

- la cessation des transferts de BICS vers TeleSign ;
- l'arrêt de tout traitement de données par TeleSign ;
- la suppression des données illégalement transférées et traitées ;
- l'obligation à tous les acteurs concernés d'informer les plaignants et toute personne concernée des traitements passés et du sort réservé à leurs données ;
- le prononcé d'une amende adéquate, compte tenu notamment de la gravité des violations constatées, mais également du nombre potentiellement très élevé de personnes concernées et du profit tiré par les activités de traitement illégales par les sociétés concernées.

4.4 Contact et communication

131. Pour tout contact, l'autorité peut contacter *noyb* par email à [redacted] sous la référence C-063.

132. La plainte étant déposée en français, la langue de la procédure sera également le français.

Vienne, le 23 Juin 2023

[redacted]