

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

5 octobre 2021

PROPOSITION DE RÉSOLUTION**relative à la lutte contre la cyberfraude
utilisant des mules bancaires****AMENDEMENTS**

*Voir:*Doc 55 **2043/ (2020/2021):**

001: Proposition de résolution de MM. Freilich et Donné.

002: Avis de l'Autorité de protection des données.

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

5 oktober 2021

VOORSTEL VAN RESOLUTIE**betreffende het bestrijden van
cyberfraude via geldezels****AMENDEMENTEN**

*Zie:*Doc 55 **2043/ (2020/2021):**

001: Voorstel van resolutie van de heren Freilich en Donné.

002: Advies van de Gegevensbeschermingsautoriteit.

05347

N° 1 DE MM. **FREILICH ET DONNÉ**

Considérant B

Remplacer les mots “comptes bancaires” par les mots “comptes de paiement”.

NR. 1 VAN DE HEREN **FREILICH EN DONNÉ**

Considerans B

Het woord “bankrekeningen” vervangen door het woord “betaalrekeningen”.

Michael FREILICH (N-VA)
Joy DONNÉ (N-VA)

N° 2 DE MM. FREILICH ET DONNÉ

Considérant C

Remplacer le mot “d’une banque” par les mots “de prestataires de services de paiement”.

JUSTIFICATION

Le mot “banque” renvoie traditionnellement à un établissement de crédit. La problématique des mules bancaires ne touche pas uniquement les établissements de crédit, mais l’ensemble des prestataires de services de paiement, y compris les établissements de crédit et les établissements de monnaie électronique. La résolution recouvre par conséquent l’ensemble des prestataires de services de paiement.

Nr. 2 VAN DE HEREN FREILICH EN DONNÉ

Considerans C

Het woord “bank” vervangen door het woord “betaaldienstaanbieder”.

VERANTWOORDING

Onder “bank” wordt traditioneel verwezen naar een kredietinstelling. De problematiek van de geldezels raakt niet alleen de kredietinstellingen maar alle betaaldienstaanbieders, inclusief betalingsinstellingen en instellingen voor elektronisch geld. De resolutie omvat bijgevolg alle betaaldienstaanbieders.

Michael FREILICH (N-VA)
Joy DONNÉ (N-VA)

N° 3 DE MM. FREILICH ET DONNÉ

Considérant F/1 (*nouveau*)

Insérer un considérant F/1 rédigé comme suit:

“F/1. vu l’avis de l’Autorité de protection des données, selon lequel il convient de veiller, lors de la lutte contre le phénomène des mules bancaires, à la nécessité et à la proportionnalité du traitement des données à caractère personnel;”

JUSTIFICATION

L’Autorité de protection des données souligne qu’il convient de s’assurer, lors de l’élaboration normative de la résolution, de la nécessité et de la proportionnalité du traitement des données à caractère personnel.

Les mesures prises en vue de lutter contre le phénomène d’escroquerie par le biais du hameçonnage et du hameçonnage par SMS, où les mules bancaires sont utilisées, doivent viser à limiter dans le temps l’ampleur d’une technique d’escroquerie et à réduire le nombre de victimes. Le traitement des données à caractère personnel d’une mule bancaire ou de tiers impliqués dans une escroquerie doit se justifier en vue d’atteindre cet objectif. Il convient à cet égard de respecter le principe de proportionnalité du traitement de données à caractère personnel sensibles.

Nr. 3 VAN DE HEREN FREILICH EN DONNÉ

Considerans F/1 (*nieuw*)

Een considerans F/1 invoegen, luidende:

“F/1. gelet op het advies van de Gegevensbeschermingsautoriteit, volgens welk dient te worden gewaakt bij het bestrijden van het fenomeen van geldezels over de noodzakelijkheid en proportionaliteit van de verwerking van de persoonsgegevens;”

VERANTWOORDING

De Gegevensbeschermingsautoriteit wijst er opdat bij de normatieve uitwerking van deze resolutie dient te worden gewaakt over de noodzakelijkheid en de proportionaliteit van de gegevensverwerking.

De maatregelen die worden genomen om het fenomeen van oplichting te bestrijden door middel van phishing en smishing waarbij gebruik wordt gemaakt van geldezels moeten gericht zijn op de omvang van een oplichtingstechniek of -truc te beperken in tijd en om het aantal slachtoffers te verminderen. De verwerking van persoonsgegevens van een geldezel of derden die betrokken worden bij een oplichting, dient te worden gerechtvaardigd met het oog op deze doeleinde. Daarbij dient het principe van de proportionaliteit van de verwerking van gevoelige persoonsgegevens te worden geëerbiedigd.

Michael FREILICH (N-VA)
Joy DONNÉ (N-VA)

N° 4 DE MM. FREILICH ET DONNÉ

Demande 3

Les mots “soupçon de blanchiment d’argent” **sont remplacés par le mot** “cyberfraude”.

JUSTIFICATION

La proposition de résolution met l’accent sur la cyberfraude commise à l’aide de mules bancaires. Les mules bancaires peuvent également blanchir de l’argent. L’avis de la CTIF renvoie à l’article 56, § 2, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l’utilisation des espèces. Cet article permet déjà aux établissements financiers, appartenant ou non à un même groupe, d’échanger des informations concernant un même client et une même transaction. Un cadre juridique devrait également disposer que les prestataires de services de paiement peuvent aussi échanger des données relatives à des comptes et à des transactions suspects en cas de cyberfraude.

Nr. 4 VAN DE HEREN FREILICH EN DONNÉ

Verzoek 3

De woorden “een vermoeden van het witwassen van geld” **vervangen door het woord** “cyberfraude”.

VERANTWOORDING

Het voorstel van resolutie legt het accent op cyberfraude via geldezels. Geldezels kunnen ook geld witwassen. Het advies van de CFI verwijst naar artikel 56, § 2, van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten. Dit artikel biedt financiële instellingen, al dan niet behorende tot eenzelfde groep, reeds de mogelijkheid om informatie uit te wisselen over eenzelfde cliënt en eenzelfde verrichting. Een wettelijk kader zou eveneens moeten bepalen dat betalingsdienstaanbieders ook gegevens over verdachte rekeningen en transacties kunnen uitwisselen in geval van cyberfraude.

Michael FREILICH (N-VA)
Joy DONNÉ (N-VA)

N° 5 DE MM. FREILICH ET DONNÉ

Demande 3/1 (*nouvelle*)**Insérer une demande 3/1 rédigée comme suit:**

“3/1. créer un centre de lutte contre l’escroquerie (scam center) au sein du Centre pour la Cybersécurité Belgique (CCB);”

JUSTIFICATION

Le hameçonnage (*phishing*) et le hameçonnage par SMS (*smishing*) sont des formes d’escroquerie très pratiquées. La victime potentielle reçoit un courriel (*phishing*) ou un message instantané (*smishing*) dans lequel l’escroc se présente sous une autre identité, celle de votre banque par exemple, mais également celle d’un ami ou d’un membre de la famille.

La CTIF estime qu’il serait intéressant de centraliser les données relatives à l’escroquerie commise par le biais de la cyberfraude. Cette centralisation doit permettre d’identifier plus rapidement et de manière plus structurée les pratiques d’escroquerie. Un centre de lutte contre l’escroquerie (*scam center*) doit permettre d’intensifier et d’accélérer la prévention et d’éviter les doublons dans le travail de recherche.

À cet égard, nous estimons qu’il est utile d’intégrer le centre de lutte contre l’escroquerie (*scam center*) au sein du Centre pour la Cybersécurité Belgique

Nr. 5 VAN DE HEREN FREILICH EN DONNÉ

Verzoek 3/1 (*nieuw*)**Een verzoek 3/1 invoegen, luidende:**

“3/1. een “scam center” op te zetten bij het Centrum voor Cybersecurity België (CCB);”

VERANTWOORDING

Een veel gebruikte vorm van oplichting is phishing en smishing. Het potentiële slachtoffer wordt benaderd via e-mail (phishing) of sms of instant messaging (smishing) waarbij de oplichter zich voordoeft als iemand anders, zoals je bank, maar evengoed een vriend of familielid. Gelijkaardige berichten worden herhaaldelijk naar talloze potentiële slachtoffers gestuurd.

Volgens de CFI zou het interessant zijn om gegevens inzake oplichting door cyberfraude te centraliseren. Dit moet het mogelijk maken om sneller en op een meer gestructureerde manier praktijken van oplichting te identificeren. Een “*scam center*” moet het mogelijk maken om meer en sneller preventief op te treden en om dubbel opsporingswerk te vermijden.

Daarbij denken wij dat het nuttig is het “*scam center*” onder te brengen bij het Centrum voor Cybersecurity België.

Michael FREILICH (N-VA)
Joy DONNÉ (N-VA)

N° 6 DE MM. FREILICH ET DONNÉ

Demande 3/2 (*nouvelle*)**Insérer une demande 3/1 rédigée comme suit:**

“3/2. mieux informer les jeunes des risques sur le plan pénal liés à l’octroi de l’accès à leur compte bancaire à des tiers;”

JUSTIFICATION

Les escrocs agissent très sournoisement en vue d'utiliser le compte bancaire des jeunes à des fins illégales pour escroquer d'autres personnes. Lors de l'ouverture d'un compte bancaire, les jeunes devraient être mieux informés des risques sur le plan pénal qui peuvent découler du transit de fonds sur leur compte bancaire dans le but de masquer le compte émetteur ou destinataire de l'organisation criminelle sous-jacente.

Nr. 6 VAN DE HEREN FREILICH EN DONNÉ

Verzoek 3/2 (*nieuw*)**Een verzoek 3/2 invoegen, luidende:**

“3/2. jongeren beter te informeren over de strafrechtelijke gevaren die zijn verbonden aan het verlenen van toegang aan derden tot hun betaalrekening;”

VERANTWOORDING

Oplichters gaan erg gewiekt te werk om de betaalrekening van jongeren te misbruiken bij oplichting van andere personen. Wanneer jongeren een betaalrekening openen zouden zij beter moeten worden geïnformeerd over de strafrechtelijke gevaren die het gevolg kunnen zijn wanneer zij gelden over hun betaalrekening laten stromen om de oorsprong of bestemming van de achterliggende criminele organisatie te verbergen.

Michael FREILICH (N-VA)
Joy DONNÉ (N-VA)