DOC 55 **2627/001**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

12 avril 2022

PROPOSITION DE RÉSOLUTION

relative à la lutte contre la fraude sur internet

(déposée par M. Bert Moyaers)

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

12 april 2022

VOORSTEL VAN RESOLUTIE

betreffende het bestrijden van internetfraude

(ingediend door de heer Bert Moyaers)

N-VA	:	*Nieuw-Vlaamse Alliantie*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
PS	:	*Parti Socialiste*
VB	:	*Vlaams Belang*
MR	:	*Mouvement Réformateur*
CD&V	:	*Christen-Democratisch en Vlaams*
PVDA-PTB	:	*Partij van de Arbeid van België – Parti du Travail de Belgique*
Open Vld	:	*Open Vlaamse liberalen en democraten*
Vooruit	:	*Vooruit*
Les Engagés	:	*Les Engagés*
DéFI	:	*Démocrate Fédéraliste Indépendant*
INDEP-ONAFH	:	*Indépendant – Onafhankelijk*

Abréviations dans la numérotation des publications:		*Afkorting bij de nummering van de publicaties:*	
DOC 55 0000/000	*Document de la 55e législature, suivi du numéro de base et numéro de suivi*	*DOC 55 0000/000*	*Parlementair document van de 55e zittingsperiode + basisnummer en volgnummer*
QRVA	*Questions et Réponses écrites*	*QRVA*	*Schriftelijke Vragen en Antwoorden*
CRIV	*Version provisoire du Compte Rendu Intégral*	*CRIV*	*Voorlopige versie van het Integraal Verslag*
CRABV	*Compte Rendu Analytique*	*CRABV*	*Beknopt Verslag*
CRIV	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*	*CRIV*	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toespraken (met de bijlagen)*
PLEN	*Séance plénière*	*PLEN*	*Plenum*
COM	*Réunion de commission*	*COM*	*Commissievergadering*
MOT	*Motions déposées en conclusion d'interpellations (papier beige)*	*MOT*	*Moties tot besluit van interpellaties (beigekleurig papier)*

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

L'année 2021 a été marquée par un nombre record de tentatives de soutirer de l'argent à nos concitoyens au moyen de courriels ou de SMS trompeurs ou d'autres formes de fraude en ligne. Le Centre pour la cybersécurité Belgique (CCB) reçoit pas moins de 13 000 signalements par jour, soit 4,5 millions par an. Le montant des pertes financières déclarées au point de contact du Service public fédéral Économie, PME, Classes moyennes et Énergie (ci-après SPF Économie) par des Belges victimes de faux courriels et SMS durant la période du 1er janvier 2019 au 28 janvier 2022 s'élevait ainsi à 41 090 499,58 euros.[1] Les faits de fraude informatique enregistrés par le ministère public ont augmenté de 116 % au cours des dix dernières années, contre une augmentation de 81 % pour le recel et le blanchiment d'argent.[2]

Les criminels qui commettent ces méfaits sont en outre de plus en plus rusés. Ils exploitent de plus en plus souvent et de plus en plus rapidement l'actualité (primes corona, vaccin de rappel ou saison des cadeaux). Leurs méthodes de base restent plus ou moins identiques, mais ils y ajoutent une touche d'actualité, ce qui rend leurs tentatives de hameçonnage plus crédibles. La probabilité que les victimes cliquent sur le lien et communiquent leurs coordonnées bancaires est donc plus élevée. Les faux messages sont par ailleurs rédigés dans un néerlandais ou un français de mieux en mieux maîtrisé, ce qui permet de supposer que les hameçonneurs sont aujourd'hui plus nombreux à opérer depuis la Belgique.[3]

Les criminels adaptent continuellement leur *modus operandi*. Ainsi, pendant la pandémie, ils ont eu davantage recours à des techniques telles que le hameçonnage, etc. pour obtenir de meilleurs résultats. La criminalité est en constante évolution. Aucune nouvelle menace n'est identifiée, mais les criminels adaptent leur façon de procéder pour la rendre plus efficace.

La lutte contre la fraude sur internet doit être à la fois répressive et préventive. Il convient de sensibiliser en permanence les victimes potentielles en leur disant que ce qui est trop beau pour être vrai, n'est généralement

1 "*Phishing*? *Ne vous faites pas avoir!*", *https://news.economie.fgov.be/209650-phishing-ne-vous-faites-pas-avoir.*

2 "*Le ministère public présente ses statistiques 2020*", *https://www.om-mp.be/fr/page/ministere-public-presente-ses-statistiques-2020.*

3 Vanderstraeten, J., "*Met 4,5 miljoen nooit zoveel phishing-meldingen als in 2021*: *dit zijn de nieuwste oplichtingstrucs waarvoor u beter oppast*", in *Het Laatste Nieuws* du 21 décembre 2021. *hln.be/consument/met-4-5-miljoen-nooit-zoveel-phishing-meldingen-als-in-2021-dit-zijn-de-nieuwste-oplichtingstrucs-waarvoor-u-beter-oppast~ad9db9d0/.*

TOELICHTING

DAMES EN HEREN,

In 2021 waren er nog nooit zoveel pogingen om geld te ontfutselen van onze landgenoten door middel van misleidende mails, sms'jes of andere vormen van onlinefraude. Het Centrum voor Cybersecurity (CCB) krijgt maar liefst 13 000 meldingen per dag of 4,5 miljoen meldingen per jaar. De gemelde financiële schade voor de Belgische slachtoffers bij het Meldpunt van de Federale Overheidsdienst Economie, KMO, Middenstand en Energie (hierna: "FOD Economie") ten gevolge van valse e-mails en sms'en in de periode van 1 januari 2019 tot en met 28 januari 2022 bedroeg bijvoorbeeld 41 090 499,58 euro.[1] De geregistreerde feiten van informaticabedrog bij het openbaar ministerie zijn de afgelopen tien jaar met 116 % gestegen, heling en witwassen met 81 %.[2]

De criminelen die hier achter schuilgaan, gaan bovendien steeds gewiekster te werk. Zij misbruiken steeds vaker en sneller de actualiteit zoals de coronapremies, de boosterprik of de pakjestijd. Hun basismethodes blijven min of meer dezelfde maar door er een actueel laagje over te gieten, komen de phishingpogingen waarachtiger over. De kans dat mensen erop doorklikken en hun bankgegevens doorspelen wordt daardoor ook groter. De valse berichten zijn bovendien in steeds beter Nederlands of Frans opgesteld waardoor het vermoeden bestaat dat meer phishingcriminelen vanuit België zelf opereren.[3]

De criminelen passen voortdurend hun *modi operandi* aan. Zo werd gedurende de pandemie meer gebruikgemaakt van technieken als phishing en dergelijke om succesvoller te zijn. De ciminaliteit is voortdurend in evolutie. Er worden geen nieuwe bedreigingen vastgesteld maar in plaats daarvan passen criminelen hun werkwijze aan en maken ze die meer effectief.

De aanpak van internetfraude moet zowel repressief als preventief zijn. De potentiële slachtoffers moeten continu worden bewust gemaakt dat indien iets te mooi is om waar te zijn, dit meestal ook zo is. Bij een preventieve

1 "*Phishing? Laat je niet vangen!*", *news.economie.fgov.be/209649-phishing-laat-je-niet-vangen.*

2 "*Het openbaar ministerie stelt de statistieken van 2020 voor*", *om-mp.be/nl/page/het-openbaar-ministerie-stelt-statistieken-van-2020-voor.*

3 Vanderstraeten, J., "*Met 4,5 miljoen nooit zoveel phishing-meldingen als in 2021: dit zijn de nieuwste oplichtingstrucs waarvoor u beter oppast*", in *Het Laatste Nieuws* van 21 december 2021. *hln.be/consument/met-4-5-miljoen-nooit-zoveel-phishing-meldingen-als-in-2021-dit-zijn-de-nieuwste-oplichtingstrucs-waarvoor-u-beter-oppast~ad9db9d0/.*

pas vrai. En matière de lutte préventive, le suivi et la perception sont essentiels. La prévention coûte moins cher et prend moins de temps que la réparation des dommages causés par la cybercriminalité, la collecte d'éléments de preuves et l'identification des auteurs des faits.

La prévention et la remédiation sont très importantes, mais un volet répressif est également nécessaire pour dissuader les auteurs éventuels. Les fraudeurs ne se limitent pas à un seul type de fraude ou simplement aux consommateurs ou aux entreprises. Il s'agit souvent d'une criminalité organisée qui ne peut être jugulée que grâce à une stratégie commune, transfrontalière et coordonnée. À cet égard, il convient d'investir au maximum dans le blocage à la source de sites web, de courriels, etc.

Le gouvernement fédéral a déjà entrepris des actions importantes dans la lutte contre la fraude sur internet et contre la cybercriminalité. Outre les campagnes mises en place chaque année pour sensibiliser les consommateurs aux différents dangers et le lancement de l'application safeonweb, le Conseil national de sécurité (CNS) a également approuvé, le 20 mai 2021, les détails de la stratégie 2.0 en matière de cybersécurité. Cette stratégie constitue, pour notre pays, le cadre de l'approche transversale des cybermenaces et des cyberopportunités.

Différents types de fraudes sur internet

La fraude sur internet ou les arnaques en ligne sont les pendants en ligne de l'escroquerie classique. Les fraudeurs recourent à des outils numériques pour soutirer de l'argent ou des biens à des personnes qui ne se doutent de rien en leur tenant de beaux discours et en leur faisant des propositions alléchantes. Lorsque le fraudeur utilise le web à cet effet, les faits sont également qualifiés d'escroquerie.

Par ailleurs, nous assistons à l'émergence de nombreuses nouvelles techniques d'extorsion. Les cryptomonnaies (comme le bitcoin) jouent un rôle de premier plan dans le développement de ces phénomènes. En effet, les criminels peuvent facilement organiser le transfert de cet argent virtuel en conservant l'anonymat complet.[4]

La liste n'est assurément pas exhaustive:

— *phishing* (*smishing*, *vishing*): le *phishing* ou hameçonnage est une forme de cybercriminalité dans laquelle la victime potentielle est approchée par courrier électronique, sms, messagerie instantanée, réseaux sociaux

[4] Rapport de l'audition du 1er septembre 2021 sur "Les cyberattaques menées contre les systèmes IT de l'État et des services publics", *Doc.parl.* Chambre, 2020-2021, DOC 55 2169/001.

aanpak is monitoring en beeldvorming essentieel. De preventie vraagt minder geld en tijd dan het herstellen van de door cybercriminaliteit veroorzaakte schade, het verzamelen van het bewijsmateriaal of het identificeren van de daders.

De preventie en de remediëring zijn heel belangrijk maar ook een repressief sluitstuk is nodig om de eventuele daders te ontraden. De fraudeurs beperken zich niet tot één fraudevorm of tot louter de consumenten of de ondernemingen. Het betreft vaak georganiseerde criminaliteit die enkel kan worden beteugeld door een gezamenlijke, grensoverschrijdende, gecoördineerde aanpak. Hierbij moet er maximaal worden ingezet op het bij de bron blokkeren van websites, mailberichten, *et cetera*…

De federale regering heeft al belangrijke stappen gezet in het bestrijden van internetfraude en cybercrime. Naast de diverse campagnes die elk jaar worden opgezet om consumenten bewust te maken van de verschillende gevaren en de lancering van een safeonweb app, heeft de Nationale Veiligheidsraad (NVR) op 20 mei 2021 ook de details van de cybersecurity strategie 2.0 goedgekeurd. Deze strategie vormt voor ons land het kader voor de transversale aanpak van cyberdreigingen en -kansen.

Verschillende vormen van internetfraude

De internetfraude of internetoplichting is de onlinevariant van de klassieke oplichting waarbij wordt gebruikgemaakt van digitaal gereedschap: het afhandig maken van geld of goederen van nietsvermoedende personen met mooie woorden en voorstellen. Ook wanneer iemand daarvoor gebruikmaakt van het internet is er sprake van oplichting.

Daarnaast worden we ook geconfronteerd met heel wat nieuwe vormen van afpersing. De cryptomunten (zoals de bitcoin) spelen hierbij een belangrijke rol. Het is immers virtueel cash geld dat de illegale wereld in volledige anonimiteit en op een gemakkelijkere manier kan transfereren.[4]

Dit is zeker geen exhaustieve lijst:

— phishing *(*smishing*, vishing):* phishing is een vorm van cybercriminaliteit waarbij het potentiële slachtoffer wordt benaderd via een e-mail, een sms, een instant messaging, de sociale media of de telefoon. De oplichter

[4] Verslag van de hoorzitting dd. 1 september 2021 over "De cyberaanvallen op het IT-systeem van de staat en de overheidsdiensten", *Parl.St.* Kamer, 2020-2021, DOC. 55 2169/001.

ou téléphone. L'escroc se fait passer pour quelqu'un d'autre. Il peut s'agir de votre banque, de votre fournisseur d'énergie ou d'une entreprise technologique. Le *phishing* et ses conséquences sont à l'origine de 80 % des cyberincidents.[5] En 2020, environ 67 000 transactions frauduleuses par hameçonnage ont eu lieu en Belgique pour un montant de près de 34 millions d'euros.[6] L'objectif est de "pêcher" ("*phishing*" en anglais) des données sensibles telles que des informations personnelles, des mots de passe, des données de la carte de banque ou de crédit. Une fois ces données récoltées, l'escroc a le champ libre. Il peut alors par exemple accéder à des comptes importants de la victime et lui voler son argent ou son identité;[7]

— *ransomware* ou rançongiciels: les systèmes sont cryptés par un logiciel malveillant et une rançon doit être payée pour que les systèmes et les données soient à nouveau accessibles. Trente pour cent des victimes paient la rançon. Il s'agit généralement de petites PME. Si elles ne paient pas, il y a souvent un préjudice économique considérable, qui a de toute façon un coût;[8]

— fraude aux achats: des biens sont commandés sans que l'acheteur ait l'intention de les payer. En 2021, la Direction générale de l'inspection économique du SPF Économie a reçu 872 signalements de tentatives d'escroquerie de vendeurs sur des plateformes de seconde main pour un montant total de 434 884,32 euros;[9]

— fraude à l'amitié ou fraude émotionnelle: de l'argent est transféré pour aider un partenaire ou un ami en ligne dans un pays lointain à se sortir de ses difficultés. En réalité, cette amitié ou cette relation n'existe pas. En 2020 et 2021, le SPF Économie a reçu respectivement 1 317 et 1 781 signalements de fraude à l'amitié. C'est presque le double du nombre de signalements par rapport à avant la crise du coronavirus. Les escrocs ont réussi à soutirer un montant record de 18 474 928,54 euros en 2020 et 2021;[10]

doet zich daarbij voor als iemand anders. Dat kan je bank, je energieleverancier of een technologiebedrijf zijn. Phishing en de gevolgen daarvan liggen ten grondslag aan 80 % van de cyberincidenten.[5] In 2020 blijkt dat er zich in België ongeveer 67 000 frauduleuze transacties door phishing hebben voorgedaan voor een bedrag van ongeveer 34 miljoen euro.[6] Het doel is om te "hengelen" ("phishing" in het Engels) naar gevoelige gegevens zoals persoonlijke informatie, wachtwoorden, bank- of kredietkaartgegevens. Eens men die gegevens heeft buitgemaakt krijgt de oplichter vrij spel. Hij kan daardoor toegang krijgen tot bijvoorbeeld belangrijke accounts van het slachtoffer en zijn geld of identiteit stelen;[7]

— ransomware*:* systemen worden versleuteld middels malware en er moet losgeld betaald worden om de systemen en gegevens weer toegankelijk te maken. Dertig procent van de slachtoffers betalen het losgeld. Meestal gaat het om kleine kmo's. Indien ze niet betalen, is er vaak sprake van grote economische schade die hoe dan ook een kostprijs heeft;[8]

— aankoopfraude*:* er worden goederen besteld zonder de intentie om deze ooit te betalen. De Algemene Directie Economische Inspectie van de FOD Economie heeft in 2021 872 meldingen ontvangen over pogingen om verkopers op tweedehandsplatforms op te lichten voor een totaal bedrag van 434 884,32 euro;[9]

— vriendschapsfraude of emotionele fraude*:* er wordt geld overgemaakt om een onlinepartner of -vriend in een ver land uit de nood te helpen. In werkelijkheid bestaat deze vriendschap of relatie niet. In 2020 en 2021 ontving de FOD Economie respectievelijk 1 317 meldingen en 1 781 meldingen van vriendschapsfraude. Dat is bijna een verdubbeling van het aantal meldingen vóór de coronacrisis. De daders slaagden erin om in 2020 en 2021 het recordbedrag van maar liefst 18 474 928,54 euro buit te maken;[10]

---

5 Rapport de l'audition du 10 novembre 2020 sur "La coopération avec les entreprises technologiques dans la lutte contre la fraude financière et économique sur internet", Doc. Parl. Chambre, 2020-2021, DOC 55 1633/001.

6 "*Phishing en 2020*: *les chiffres*", *https://www.febelfin.be/fr/communique-de-presse/phishing-en-2020-les-chiffres.*

7 "*Phishing*: *ne mordez pas à l'hameçon*" *www.test-achats.be/hightech/internet/dossier/phishing.*

8 Rapport de l'audition du 10 novembre 2020 sur "La coopération avec les entreprises technologiques dans la lutte contre la fraude financière et économique sur internet", Doc. Parl. Chambre, 2020-2021, DOC 55 1633/001.

9 Dupon, Y., "*FOD Economie waarschuwt voor nepkopers op tweedehandssites*: *met deze tips loop je niet in de va*l.", in *Het Laatste Nieuws* du 18 janvier 2022. *hln.be/binnenland/fod-economie-waarschuwt-voor-nepkopers-op-tweedehandssites-met-deze-tips-loop-je-niet-in-de-val~a3ab5ca3/.*

10 "*Online vriendschap*: *oprecht of toch niet*?", *news.economie.fgov.be/203589-online-vriendschap-oprecht-of-toch-niet.*

5 Verslag van de hoorzitting dd. 10 november 2020 over "De samenwerking met de technologiebedrijven in de strijd tegen financieel-economische internetfraude", *Parl. St.* Kamer, 2020-2021, DOC. 55 1633/001.

6 "*Phishing in 2020: de cijfers*", *febelfin.be/nl/press-room/phishing-2020-de-cijfers.*

7 "*Phishing: zo laat je oplichters bot vangen*" *test-aankoop.be/hightech/internet/dossier/phishing.*

8 Verslag van de hoorzitting dd. 10 november 2020 over "De samenwerking met de technologiebedrijven in de strijd tegen financieel-economische internetfraude", *Parl. St.* Kamer, 2020-2021, DOC. 55 1633/001.

9 Dupon, Y., "*FOD Economie waarschuwt voor nepkopers op tweedehandssites: met deze tips loop je niet in de va*l.", in *Het Laatste Nieuws* van 18 januari 2022. *hln.be/binnenland/fod-economie-waarschuwt-voor-nepkopers-op-tweedehandssites-met-deze-tips-loop-je-niet-in-de-val~a3ab5ca3/.*

10 "*Online vriendschap: oprecht of toch niet?*", *news.economie.fgov.be/203589-online-vriendschap-oprecht-of-toch-niet.*

— fraude à l'identité: une personne acquiert les données personnelles d'une autre personne (vol d'identité) afin de se faire passer pour cette personne. Cette fausse identité peut être utilisée pour escroquer des victimes. Par ailleurs, le fraudeur peut également accéder à des systèmes informatiques, à des formes de prestation de services électroniques et à des comptes liés à des cartes bancaires et de crédit. Dans certains cas, les conséquences de la fraude à l'identité sont considérables. Si, par exemple, des criminels parviennent à contracter des prêts ou à louer un immeuble en votre nom, l'huissier ou la police peuvent se présenter soudainement à votre porte. Il peut ensuite s'écouler des années avant que votre nom ne soit blanchi.

Les criminels qui dérobent de l'argent par le biais de la fraude sur internet ne placent pas directement cet argent sur leur propre compte. Ils utilisent une mule financière pour faire transiter l'argent. Il s'agit d'un des systèmes que les criminels mettent en place pour aider d'autres criminels à blanchir de l'argent. Ces mules financières sont souvent des jeunes vulnérables sur le plan socio-économique. Ces jeunes ignorent souvent dans quoi ils s'engagent. Ce système permet aux criminels de ne pas s'exposer eux-mêmes, mais donne l'impression que ce sont ces mules financières qui ont dérobé l'argent.[11] Si les jeunes peuvent continuer à gagner de l'argent rapidement sans trop risquer de se faire prendre, ils passeront à des faits criminels plus graves et plus importants, ce qui aura pour effet d'alourdir la charge des services d'inspection et de la Justice (tremplin vers la criminalité).

Problèmes concernant la lutte contre la fraude sur internet

— l'approche morcelée:

La Belgique dispose d'une structure de l'État complexe, ce qui complique la mise en œuvre d'une politique de cybersécurité coordonnée.

• Le CCB: le Centre pour la Cybersécurité Belgique (CCB) est l'autorité nationale en charge de la cybersécurité en Belgique. Il supervise, coordonne et veille à la mise en œuvre de la stratégie belge en matière de cybersécurité. Grâce à un échange d'informations optimal, les entreprises, les autorités, les opérateurs de services essentiels et les citoyens peuvent compter sur une protection adéquate. Le CCB sensibilise la population aux principales cybermenaces et l'informe des moyens de se protéger contre ces menaces. Le CCB a créé *safeonweb.be* et collecte les menaces actuelles tout en prodiguant des conseils pour surfer en toute sécurité. La

[11] "*Geldezels of "money mules*", *politie.be/5355/vragen/criminaliteit-op-internet/geldezels-of-money-mules.*

— identiteitsfraude: men verwerft persoonlijke gegevens van iemand anders (identiteitsdiefstal) om zich dan geloofwaardig voor te doen als deze persoon. Met deze valse identiteit is men in staat slachtoffers op te lichten. Daarnaast kan men ook toegang verwerven tot computersystemen, vormen van elektronische dienstverlening en betaal- en creditcardrekeningen. In sommige gevallen zijn de gevolgen van identiteitsfraude verstrekkend. Als criminelen bijvoorbeeld op jouw naam leningen weten af te sluiten of een pand kunnen huren, kan de deurwaarder of politie ineens voor de deur staan. Het kan dan jaren duren vooraleer je naam is gezuiverd.

De criminelen die geld stelen via internetfraude plaatsen dit niet onmiddellijk op hun eigen rekening. Ze gebruiken een geldezel om het geld door te sluizen. Dit is een van de systemen die criminelen opzetten om andere criminelen te helpen bij het witwassen van geld. Deze geldezels zijn vaak sociaal-economisch kwetsbare jongeren. Zij weten vaak niet waar ze in verzeild raken. Zo lopen de criminelen niet zelf in de kijker maar lijkt het alsof deze geldezels dat geld hebben gestolen.[11] Indien de jongeren snel geld kunnen blijven verdienen zonder een grote pakkans zal dit leiden tot een doorstroming naar grotere en zwaardere criminele feiten met een grotere belasting voor de inspectiediensten en Justitie tot gevolg (opstapcriminaliteit).

Problemen bij het bestrijden van internetfraude

— de versnipperde aanpak*:*

België heeft een complexe overheidsstructuur wat een gecoördineerd cyberveiligheidsbeleid voor overheidsdiensten niet eenvoudig maakt.

• CCB: het Centrum voor Cybersecurity België (CCB) is de nationale autoriteit voor cyberveiligheid Het CCB superviseert, coördineert en waakt over de toepassing van de Belgische cyberveiligheidsstrategie. Door optimale informatie-uitwisseling kunnen bedrijven, de overheid, aanbieders van essentiële diensten en de bevolking zich gepast beschermen. Het CCB maakt de bevolking bewust van de voornaamste cyberdreigingen en hoe zich ertegen te beschermen. CCB heeft *safeonweb.be* opgericht en verzamelt actuele dreigingen en tips om veilig te surfen. Men vraagt om verdachte berichten te sturen naar *verdacht@safeonweb.be* of *suspect@safeonweb.*

[11] "*Geldezels of "money mules*", *politie.be/5355/vragen/criminaliteit-op-internet/geldezels-of-money-mules.*

population est invitée à envoyer les messages suspects à *suspect@safeonweb.be* ou à *verdacht@safeonweb.be*. Lancée récemment, la nouvelle application *safeonweb* permet également aux utilisateurs d'être avertis en cas de nouveaux messages de hameçonnage.

• La CERT: la *Computer Emergency Response Team* fédérale, en abrégé *CERT.be*, est le service opérationnel du Centre pour la Cybersécurité Belgique (CCB). *CERT.be* est chargé de détecter, d'observer et d'analyser les problèmes de sécurité en ligne et d'informer les différents groupes cibles à ce sujet. La CERT ne dispose pas de compétences policières et ne peut donc pas procéder à des devoirs d'enquête (comme identifier les suspects ou faire mettre un site web hors ligne). Elle ne peut pas transmettre les notifications qu'elle reçoit au parquet compétent.

• La police: les services de la police intégrée sont chargés de la lutte contre la criminalité informatique. En tant que police de première ligne, la police locale fait office de premier point de contact pour les citoyens, les entreprises et les services publics. Dans ce cadre, elle fait intervenir les services spécialisés (RCCU/FCCU) lorsque c'est nécessaire. Au sein de la police judiciaire fédérale (PJF), les *Regional Computer Crime Units* (RCCU) et la *Federal Computer Crime Unit* (FCCU) sont chargées de la lutte judiciaire contre la criminalité TIC.

• Le ministère public: l'information judiciaire en général, mais aussi celle qui concerne la cybercriminalité en particulier, est menée dans chaque arrondissement judiciaire sous la direction du procureur du Roi compétent. Celui-ci confie aux services de la police intégrée et, le cas échéant, à d'autres services de recherche les devoirs nécessaires pour rassembler les traces et faire apparaître la vérité. Au bout du compte, c'est également le procureur du Roi qui porte ou non les cyberinfractions devant le tribunal. À cet égard, le procureur du Roi dispose généralement d'un ou de plusieurs magistrats de référence en matière de cybercriminalité, qui s'occupent en priorité de l'enquête sur les cyberinfractions.

• Le Service public fédéral Économie: le SPF Économie a pour mission de créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et des services en Belgique. Compte tenu de la numérisation croissante de notre société et de nos entreprises, le SPF Économie est impliqué dans différents domaines de la cybersécurité. Il a créé le site *pointdecontact.be*. Le SPF Économie avertit quotidiennement la population des phénomènes de fraude. Il réalise des analyses juridiques des signalements soumis au point de contact et informe les acteurs concernés (notamment les banques) des modes opératoires du ou des fraudeurs afin qu'ils puissent bloquer l'accès si nécessaire.

be. Onlangs werd ook de nieuwe app *Safeonweb* gelanceerd waarbij gebruikers een waarschuwing krijgen bij nieuwe phishingberichten.

• CERT: het federale *Computer Emergency Response Team*, kortweg *CERT.be* is de operationele dienst van het Centrum voor Cybersecurity België (CCB). *CERT.be* heeft als opdracht het online opsporen, observeren en analyseren van veiligheidsproblemen en de verschillende doelgroepen hierover informeren. Het CERT heeft geen politionele bevoegdheden en kan dus geen onderzoeksdaden stellen (zoals verdachten identificeren of een website offline laten halen.). Ze kunnen de meldingen die ze verkrijgen niet doorgeven aan het bevoegde parket.

• De politie: de geïntegreerde politiediensten staan in voor de bestrijding van de informaticacriminaliteit. Als eerstelijnspolitie vormt de Lokale Politie het eerste aanspreekpunt voor de burgers, bedrijven en overheidsdiensten. Vanuit deze rol betrekt zij de gespecialiseerde diensten (RCCU/FCCU) wanneer dit vereist is. Binnen de Federale Gerechtelijke Politie (FGP) staan de Regionale *Computer Crime Units* (RCCU's) en de Federale *Computer Crime Unit* (FCCU) in voor de gerechtelijke aanpak van ICT-criminaliteit.

• Het openbaar ministerie: het opsporingsonderzoek in het algemeen, maar ook voor cybercriminaliteit in het bijzonder, wordt in elk gerechtelijk arrondissement gevoerd onder leiding van de bevoegde procureur des Konings. Deze geeft de geïntegreerde politiediensten en desgevallend andere opsporingsdiensten de nodige opdrachten teneinde de sporen te verzamelen en de waarheid aan het licht te brengen. Op het einde van de rit is het eveneens de procureur des Konings die de cybermisdrijven al dan niet voor de rechtbank brengt. De procureur des Konings heeft hierbij doorgaans een of meerdere referentiemagistraten cybercrime die zich bij voorrang inlaten met het onderzoek naar cybermisdrijven.

• De federale Overheidsdienst Economie: heeft als opdracht de voorwaarden te scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. Gezien de toenemende digitalisering van onze maatschappij en onze bedrijven is de FOD Economie betrokken in verschillende domeinen van cyberveiligheid. Zij hebben het *Meldpunt.be* opgericht. De FOD Economie waarschuwt de bevolking dagelijks over fraudefenomenen. Zij voert juridische analyses uit van de meldingen ingediend via het Meldpunt en stelt de betrokken actoren (bijvoorbeeld de banken) in kennis over de modi operandi van de fraudeur(s) waardoor deze zo nodig de toegang blokkeren. Wanneer

Lorsque des données exploitables (comme des comptes bancaires) apparaissent dans les dossiers, il identifie les responsables, procède à une enquête sur le suspect et prend les mesures nécessaires pour mettre fin à la pratique (comme la rédaction de procès-verbaux et/ou la fermeture de sites web au moyen d'une procédure administrative).[12]

• Par ailleurs, on mentionnera encore l'Institut belge des services postaux et des télécommunications (IBPT), le Centre de Crise national (NCCN), la Sûreté de l'État (VSSE), l'Organe de coordination pour l'analyse de la menace (OCAM), la Cellule de traitement des informations financières (CTIF), l'Autorité des services et marchés financiers (FSMA).

Il est logique que les différents services apportent chacun leur contribution à partir de leur propre domaine d'action et expertise. Mais si une victime doit contacter trois services publics avant d'être aidée, il y a quelque chose qui ne va pas dans cette approche. Cette fragmentation de l'approche a pour conséquence que les fraudeurs, en particulier ceux qui opèrent depuis l'étranger, ne sont presque jamais pris.

La lutte contre la cybercriminalité nécessite une approche transfrontalière coordonnée. Les services de police locaux peuvent procéder aux interrogatoires des suspects, mais il est nécessaire de disposer, au sein de la police, d'une unité centrale de lutte contre la cybercriminalité investie de missions plus étendues que celles de la FCCU et de la RCCU. Nous avons besoin d'une approche intégrée de la cybercriminalité où tant les services de police que les services publics (comme la Sûreté de l'État, l'OCAM, la police, le SPF Finances, la CTIF, le SPF Économie, la FSMA, le CCB, etc.), mais aussi les acteurs concernés (comme les banques, les opérateurs télécoms, etc.), peuvent échanger des informations. Actuellement, l'approche est trop fragmentée. Le résultat est que différents services publics travaillent sur les mêmes dossiers et qu'on ne fait pas le lien entre les dossiers, ce qui a pour conséquence que l'on ne peut avoir une vision globale du réseau (de la superstructure) et que les principaux acteurs ne peuvent être poursuivis.

Une approche intégrée du hameçonnage se heurte à la faiblesse des moyens ainsi qu'à la divergence des prescriptions légales en matière de flux d'informations et de gestion des données. Le partage d'informations entre les différents acteurs de la lutte contre le hameçonnage permettrait d'entamer des enquêtes plus efficacement et plus rapidement en travaillant les uns avec les autres

[12] "Stratégie Cybersécurité Belgique 2.0 2021-2025", *https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_FR_DP2.pdf.*

bruikbare gegevens (zoals bankrekeningen) in de dossiers opduiken, identificeert zij de verantwoordelijken, stelt zij een onderzoek in naar de verdachte en neemt zij de nodige maatregelen om de praktijk te stoppen (zoals processen-verbaal opstellen en/of websites laten afsluiten via een administratieve procedure).[12]

• Daarnaast is er nog het Belgische Instituut voor Postdiensten en Telecommunicatie (BIPT), het Nationaal Crisiscentrum (NCCN), de Veiligheid van de Staat (VSSE), het Coördinatieorgaan voor de dreigingsanalyse (OCAD), de Cel voor Financiële Informatieverwerking (CFI), de Autoriteit voor Financiële Diensten en Markten (FSMA)…

Het is logisch dat de verschillende diensten elk vanuit hun eigen werkveld en expertise een bijdrage leveren. Maar als een slachtoffer drie overheidsdiensten moet contacteren vooraleer hij geholpen wordt, is er iets mis aan de aanpak. Die versnipperde aanpak zorgt ervoor dat de fraudeurs, zeker degenen die vanuit het buitenland opereren, bijna niet worden aangepakt.

De aanpak van cybercrime vergt een gecoördineerde grensoverschrijdende aanpak. De lokale politiediensten kunnen de verhoren van de verdachten uitvoeren maar er is nood aan een centrale cybercrime unit binnen de politie die verder gaat dan de taken van FCCU en RCCU. We hebben nood aan een geïntegreerde aanpak van cybercriminaliteit waarbij zowel de politionele diensten als de overheidsdiensten (zoals de VSSE, het OCAD, de politie, de FOD Financiën, de CFI, de FOD Economie, de FSMA, het CCB, *et cetera*…), maar ook de betrokken actoren (zoals banken, telecomoperatoren, …) aan gegevensuitwisseling kunnen doen. Nu is de aanpak te versnipperd. Het gevolg is dat verschillende overheidsdiensten op dezelfde dossiers werken en de linken tussen de dossiers niet gemaakt worden waardoor het netwerk (de bovenbouw) ook niet in kaart wordt gebracht en de spilfiguren niet vervolgd kunnen worden.

Een geïntegreerde aanpak van phishing wordt bemoeilijkt door de beperkte middelen alsmede door de divergente wettelijke voorschriften inzake informatiedoorstroming en databeheer. Het kunnen delen van informatie tussen de verschillende actoren in de strijd tegen phishing zou toelaten om efficiënter en sneller onderzoeken op te starten door met elkaar in plaats van

[12] "Cybersecurity Strategie België 2.0 2021-2025", *https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_NL_DP6.pdf.*

plutôt que chacun de son côté. Les ressources publiques pourraient ainsi être utilisées plus efficacement.

Les piliers suivants sont importants pour une approche efficace de la fraude:

1. le traitement et la diffusion des plaintes: toutes les informations/tous les signaux doivent être envoyés à un service de coordination afin de pouvoir déterminer les mesures à prendre dans un délai très court;

2. le traitement et la diffusion de l'information pour accroître l'efficacité et réduire la charge de travail en évitant d'accomplir deux fois la même tâche;

3. les plaintes de deuxième ligne, l'analyse, la perception du phénomène, le suivi et l'étude de marché: cela permet de formuler des propositions de mesures supplémentaires, d'élaborer de nouvelles méthodes de recherche, de proposer des projets de loi, d'adapter la législation en vigueur, etc.;

4. la coordination de gros dossiers multithématiques et/ou transrégionaux/internationaux;

5. le suivi et la prise en compte des nouvelles tendances par le biais d'une coopération et d'un feed-back avec tous les services concernés;

6. la capacité de répondre de manière adéquate et efficace à la fraude, en évitant de se renvoyer la balle au niveau des signalements et des victimes.

Un fraudeur utilise différentes formes de fraude et également différents canaux (téléphone portable, numéro de compte bancaire, e-mail, …) pour commettre une fraude. Si les dossiers sont attribués à des organisations publiques sur la base d'un thème, d'un numéro de compte bancaire ou d'une adresse électronique, il peut arriver qu'un fraudeur fasse l'objet de différents dossiers au sein de différentes directions et qu'il ne soit jamais poursuivi en raison du nombre insuffisant d'éléments et de victimes.

Un service central devrait permettre une vision globale du problème en cartographiant les liens avec la Belgique, les réseaux et les principaux acteurs.

Il est donc nécessaire de mettre en place un service faîtier de coordination anti-fraude. En effet, la coopération est essentielle pour assurer notre cybersécurité de manière efficace et coordonnée. Cela peut permettre de réduire considérablement la charge de travail des parquets, car ils ne recevront plus plusieurs procès-verbaux

naast elkaar te werken. Zo kunnen overheidsmiddelen doeltreffender worden ingezet.

Voor een efficiënte aanpak van fraude zijn volgende pijlers belangrijk:

1. de klachtenverwerking en klachtenverdeling: alle informatie/signalen dienen naar een coördinerende dienst verzonden te worden, zodoende dat er op zeer korte tijd bepaald kan worden welke maatregelen moeten genomen worden;

2. de informatieverwerking en -verdeling om aldus meer efficiëntie te bekomen en de werkdruk te verminderen door dubbel werk te vermijden;

3. de tweedelijnsklachten, analyse, beeldvorming, monitoring en marktstudie: hierdoor kunnen voorstellen voor bijkomende maatregelen worden geformuleerd, nieuwe onderzoeksmethoden worden uitgewerkt, wetsontwerpen worden voorgesteld, de vigerende wetgeving worden aangepast, *et cetera*…;

4. het coördineren van grote dossiers die thematisch en/of regionaal/internationaal overschrijdend zijn;

5. het opvolgen en ageren van nieuwe markttendensen via samenwerking en terugkoppeling met alle bevoegde diensten;

6. het adequaat en efficiënt kunnen reageren op fraude waardoor een pingpong met meldingen en slachtoffers vermeden wordt.

Een fraudeur gebruikt verschillende fraudevormen en ook verschillende kanalen (gsm, bankrekeningnummer, e-mail, ...) om de fraude te plegen. Indien dossiers toegewezen worden aan overheidsorganisaties op basis van een thematiek, een bankrekeningnummer of een e-mail kan het gebeuren dat betreffende dezelfde fraudeur, diverse dossiers aan diverse directies worden toegewezen en hij telkens niet wordt vervolgd wegens te weinig elementen en te weinig slachtoffers.

Er dient een centrale dienst te komen die gericht is op de beeldvorming waarbij de linken met België, de netwerken en de spilfiguren in kaart worden gebracht.

Er is dus nood aan een overkoepelende coördinatiedienst inzake fraudebestrijding. De samenwerking is tenslotte essentieel om onze cyberveiligheid op een effectieve en gecoördineerde wijze te verzekeren. Hierdoor kan de werklast van de parketten aanzienlijk verlagen omdat niet vijf maal een proces-verbaal lastens dezelfde

à charge du même fraudeur de la part de services publics différents.

— personnel spécialisé:

La *Federal Computer Crime Unit* (FCCU) et les *Regional Computer Crime Units* (RCCU) sont des unités de la Police Judiciaire Fédérale (PJF). La FCCU se situe au sein de la direction centrale DJSOC et les RCCU au sein des directions judiciaires déconcentrées dans les arrondissements (PJF). Chaque PJF dispose d'une RCCU.

La Police Judiciaire Fédérale lutte contre la cybercriminalité à deux niveaux. À l'échelle des directions judiciaires déconcentrées, les unités régionales spécialisées soutiennent à la fois la Police Fédérale et la Police Locale dans l'analyse du matériel informatique saisi dans le cadre de dossiers judiciaires. Elles enquêtent également sur la cybercriminalité au sein de leur arrondissement judiciaire.

Au niveau fédéral, la FCCU mène des enquêtes et fournit un appui aux divisions d'enquête des services centraux. Les *geeks* de la FCCU ont notamment pour tâches de constituer et d'entretenir un réseau de partenaires et de contacts, de cartographier les cybermenaces, de produire des rapports de contextualisation et d'analyse, d'effectuer l'analyse forensique (qui consiste à effectuer une analyse du système d'information après une attaque informatique) des différents appareils et supports ICT (*Information and Communication Technology*), de mener des enquêtes judiciaires complexes visant des organisations cybercriminelles et d'identifier les *hackers* responsables des attaques sur les infrastructures critiques.[13]

Il ressort de ma question écrite n° 0372 qu'en 2021, seulement 26 postes de travail (et 5 CAlog) étaient occupés sur les 44 postes du cadre prévu pour la FCCU. Cette unité est dès lors confrontée à un manque aigu de personnel, de savoir-faire et de moyens. Selon la police fédérale, les RCCU sont également en sous-effectifs. Le métier d'informaticien au sein des services publics est cependant un métier en pénurie en général.[14] La rigidité des structures et des statuts entrave tout simplement la mise en place d'une politique de recrutement flexible. Il ne s'agit donc pas seulement de rémunération, mais aussi d'organisation. Le tableau organique de la FCCU,

[13] "*Federal Computer Crime Unit*", *https://www.police.be/villagepolicier/fr/police-federale/federal-computer-crime-unit.*

[14] Question écrite n° 0372 du 1er mars 2021 de M. Bert Moyaers intitulée "FCCU et RCCU", publiée dans le Bulletin des Questions et Réponses B046 du 7 avril 2021, *https://www.lachambre.be/QRVA/pdf/55/55K0046.pdf.*

fraudeur wordt overgemaakt door telkens een andere overheidsdienst.

— gespecialiseerd personeel:

De *Federal Computer Crime Unit* (FCCU) en de *Regional Computer Crime Units* (RCCU) zijn eenheden van de Federale Gerechtelijke Politie (FGP). De FCCU situeert zich binnen de centrale directie DJSOC en de RCCU's binnen de gedeconcentreerde gerechtelijke directies in de arrondissementen (FGP's). Elke FGP beschikt over een RCCU.

De FGP bestrijdt cybercriminaliteit op twee niveaus. Op het niveau van de gedeconcentreerde gerechtelijke directies ondersteunen de gespecialiseerde regionale eenheden zowel de Federale Politie als de Lokale Politie bij de analyse van in beslag genomen computermateriaal. Ze voeren ook onderzoeken uit naar cybercriminaliteit binnen hun gerechtelijk arrondissement.

Op federaal niveau voert de FCCU onderzoeken uit en levert steun aan de onderzoeksafdelingen van de centrale diensten. De taken van de FCCU bestaan in het bijzonder uit het opbouwen en onderhouden van een netwerk van partners en contacten, het in kaart brengen van de cyberdreigingen, het opstellen van de contextualiserings- en analyseverslagen, het maken van forensische analyses (dit zijn analyses van het informatiesysteem na een computeraanval) van de verschillende toestellen en ICT-supports *(ICT: Information and Communication Technology*), het voeren van complexe gerechtelijke onderzoeken naar cybercriminele organisaties en het identificieren van hackers te die verantwoordelijk zijn voor aanvallen op kritieke infrastructuren.[13]

Uit mijn schriftelijke vraag nr. 0372 bleek dat bij het FCCU in 2021 het voorziene kader van 44 personeelsleden slechts met 26 personeelsleden (en 5 CALog) was ingevuld. De FCCU kampt dus met een acuut tekort aan personeel, knowhow en middelen. Ook bij de RCCU zou men volgens de federale politie kampen met een tekort aan personeel. De functie van ICT'er binnen de overheidsdiensten blijkt wel vaker een knelpuntberoep.[14] De strakke structuren en statuten staan nu eenmaal een flexibel rekruteringsbeleid in de weg. Het betreft niet enkel de verloning maar ook de organisatie. De organieke tabel van de FCCU bestaat bijvoorbeeld enkel

[13] "*Federal Computer Crime Unit*", *politie.be/politiedorp/nl/federale-politie/federal-computer-crime-unit.*

[14] Schriftelijke vraag nr. 0372 van 1 maart 2021 van de heer Bert Moyaers over "FCCU en RCCU", gepubliceerd in het Bulletin van Vragen en Antwoorden B046 van 7 april 2021. *dekamer.be/kvvcr/showpage.cfm?section=qrva&language=nl&cfm=qrvaXml.cfm?legislat=55&dossierID=55-B046-1192-0372-2020202108403.xml.*

par exemple, ne comprend que des postes d'inspecteur principal spécialisé. Par conséquent, leur sélection – et parfois leur rejet – se fait en fonction des capacités requises pour un fonctionnaire de police dirigeant.

Certaines zones de police locale sont submergées par les plaintes concernant la cybercriminalité, qui fait désormais partie de la formation de base de tous les inspecteurs de police. Le phénomène est donc pris au sérieux, même s'il est encore possible de s'améliorer.

Il ressort en outre d'une réponse de M. Van Quickenborne, ministre de la Justice, qu'en raison du COVID-19, la formation nécessaire et imposée par la loi aux services de police n'a pas encore été organisée, si bien que les services spécialisés du Commissariat Général *Special Unit* (CGSU) sont aujourd'hui les seuls services à pouvoir réaliser une interaction virtuelle de cette nature. Cette formation destinée aux services de police ordinaires doit être organisée dans les plus brefs délais. Elle est en effet importante car elle leur permettra de procéder aux constatations nécessaires dans le monde virtuel.[15]

— acteurs techniques:

Des plateformes commerciales sont souvent utilisées pour contacter des victimes, les duper ou leur dérober des informations. Des plateformes telles que Facebook, Instagram, etc. sont utilisées par des criminels pour cibler le particulier au travers de contenus sponsorisés (utilisation de profils de personnes connues) dans le but d'amener l'utilisateur à cliquer sur ces liens.[16]

Il existe un régime légal d'exonération de responsabilité sous certaines conditions, moyennant obligation d'information, pour trois catégories de prestataires de services techniques agissant en qualité d'intermédiaires (articles XII.17, XII.18, XII.19 du Code de droit économique (ci-après: "CDE")):

— prestataires qui fournissent une activité de simple transport/transmission ("opérateurs")

— prestataires qui fournissent une activité de stockage sous forme de copie temporaire de données;

uit gespecialiseerde hoofdinspecteurs. Zij worden dus ook gescreend en soms afgewezen op basis van de capaciteiten van een leidinggevende politieambtenaar.

Sommige lokale politiezones worden overspoeld met klachten over cybercriminaliteit. De informaticacriminaliteit zit in de basismodule van alle politie-inspecteurs. Er is dus zeker aandacht voor de problematiek, al is er nog ruimte voor verbetering.

Daarnaast blijkt uit een antwoord van minister Van Quickenborne dat ingevolge COVID-19 moet worden vastgesteld dat de noodzakelijke wettelijk vereiste opleiding voor de politiediensten nog niet werd georganiseerd zodat de gespecialiseerde diensten van het Commissariaat Generaal *Special Units* (CGSU) thans de enige zijn die dergelijke virtuele interactie mogen uitvoeren. Die opleiding voor de reguliere politiediensten moet er zo snel mogelijk komen. Die opleiding is immers belangrijk om hen toe te laten de nodige vaststellingen te doen in de virtuele wereld.[15]

— technische actoren:

Vaak worden commerciële platforms gebruikt om slachtoffers te contacteren, te misleiden of informatie te ontfutselen. Criminelen misbruiken platforms zoals Facebook, instagram, *et cetera*… om de burger te benaderen met bijvoorbeeld gesponsorde content (gebruiken profielen van bekende personen). Zo wordt de gebruiker ertoe aangezet om deze links aan te klikken.[16]

Krachtens een wettelijke regeling kunnen drie categorieën van als tussenpersoon optredende technische dienstverleners onder bepaalde voorwaarden (en middels informatieplicht) van aansprakelijkheid worden ontheven (artikelen XII.17, XII. 18, XII. 19 van het Wetboek van Economisch Recht (hierna: "WER"), met name de dienstverleners:

— van wie de activiteiten louter het doorgeven van informatie betreft (zogenaamde operatoren)

— van wie de activiteiten de opslag in de vorm van tijdelijke kopiëring van gegevens betreft;

---

15 Réponse de M.Vincent Van Quickenborne, ministre de la Justice, aux questions jointes de M. Bert Moyaers intitulées "Les possibilités d'infiltration pour la police en cas de cybercrime" et "Le reportage de Pano sur la cybercriminalité" posées au sein de la commission de la Justice le 31 mars 2021, *Doc. parl., Chambre, 2020-2021,*CRIV 55 COM 436, page 49, en haut. *lachambre.be/doc/CCRI/pdf/55/ic436.pdf.*

16 Rapport de l'audition du 10 novembre 2020 consacrée à "La coopération avec les entreprises technologiques dans la lutte contre la fraude financière et économique sur internet", *Doc. parl., Chambre, 2020-2021,* DOC 55 1633/001.

15 Antwoord van minister van Justitie Vincent Van Quickenborne op de samengevoegde vragen van de heer Bert Moyaers over "De infiltratiemogelijkheden van de politie in geval van cybercrime" en "De Pano-reportage over cybercriminaliteit" in de commissie Justitie van 31 maart 2021, *Parl. St.* Kamer, 2020-2021, DOC. CRIV. 55 COM 436, pag.49 bovenaan. *dekamer.be/doc/CCRI/pdf/55/ic436.pdf.*

16 Verslag van de hoorzitting dd. 10 november 2020 over "De samenwerking met de technologiebedrijven in de strijd tegen financieel-economische internetfraude", *Parl. St.* Kamer, 2020-2021, DOC. 55 1633/001.

— prestataires qui fournissent une activité d'hébergement.

Les trois catégories de prestataires de services techniques agissant en qualité d'intermédiaires ont l'obligation légale d'informer rapidement les autorités administratives ou judiciaires compétentes à l'égard des intermédiaires techniques. On constate cependant que cette obligation légale d'informer les autorités administratives ou judiciaires n'est guère respectée.

Le refus de collaboration n'est pas punissable d'une peine d'emprisonnement, alors que cette peine est prévue pour les banques (article 46*quater* du Code d'instruction criminelle). L'amende maximale de 80 000 euros infligée en cas de refus de collaboration est insignifiante pour de telles multinationales.

En vue d'une lutte efficace contre la fraude sur internet à titre général, il conviendra que l'autorité compétente et les intermédiaires techniques collaborent comme suit:

— les prestataires de services concernés devront immédiatement porter à la connaissance des autorités compétentes toutes les activités présumées illicites;

— les prestataires de services devront identifier les utilisateurs de leurs services afin de répondre aux demandes des autorités compétentes qui enquêtent sur les auteurs d'infractions dissimulant leur véritable identité;

— les prestataires de services devront conserver les données afin de répondre aux demandes des autorités compétentes visant à établir la preuve des infractions commises par les utilisateurs de leurs services;

— les prestataires de services devront réagir rapidement aux demandes des autorités compétentes d'appliquer une procédure *notice and action* visant la cessation des infractions commises par les utilisateurs de leurs services.[17]

Le CCB coopère aussi, par exemple, avec les fournisseurs d'accès internet. Cette coopération fonctionne de manière satisfaisante mais dépend de la bonne volonté des acteurs (fournisseurs d'accès internet, Google, Microsoft, etc.). À l'heure actuelle, ces partenariats ne sont aucunement structurels ni formels. Dès que la mise en œuvre de certaines mesures devient trop coûteuse pour les fournisseurs d'accès internet, on ne peut garantir que la coopération continuera d'être efficace. Par exemple, lorsque le CCB constate qu'il y

[17] *Idem*.

— van wie de activiteiten hostdiensten betreft.

Deze drie categorieën van dienstverleners zijn wettelijk verplicht de bestuurlijke of de gerechtelijke autoriteiten die bevoegd zijn voor de als tussenpersoon optredende technische dienstverleners, onverwijld in kennis te stellen. Helaas kan men vaststellen dat die wettelijke informatieplicht jegens de bestuurlijke en de gerechtelijke autoriteiten amper in acht wordt genomen.

De niet-medewerking is niet strafbaar met een gevangenisstraf terwijl dit bij de banken (artikel 46*quater* van het Wetboek van Strafvordering) wel het geval is. De maximale geldboete bij niet-medewerking bedraagt 80 000 euro en is een peulschil voor dergelijke multinationals.

Met het oog op de doeltreffende bestrijding van de internetfraude in het algemeen is het onontbeerlijk dat de bevoegde autoriteit en de betrokken actor als volgt samenwerken:

— de betrokken dienstverleners moeten de bevoegde autoriteiten onverwijld in kennis stellen van alle vermeende onwettige activiteiten;

— de dienstverleners moeten de gebruikers van hun diensten identificeren teneinde te voldoen aan de verzoeken van de bevoegde autoriteiten die een onderzoek instellen naar de plegers van misdrijven die hun ware identiteit verbergen;

— de dienstverleners moeten de gegevens bewaren teneinde te voldoen aan de verzoeken van de bevoegde autoriteiten om het bewijs te leveren van de door de gebruikers van hun diensten gepleegde misdrijven;

— de dienstverleners moeten snel gevolg geven aan de verzoeken van de bevoegde autoriteiten om een *notice-and-action*procedure toe te passen om een einde te maken aan de door de gebruikers van hun diensten gepleegde misdrijven.[17]

Daarnaast werkt bijvoorbeeld het CCB samen met de internetproviders. Die samenwerking verloopt naar behoren maar berust op de welwillendheid van de actoren (*internet service providers* (ISP's), Google, Microsoft, *et cetera*…). Die samenwerkingsverbanden zijn thans geenszins structureel noch formeel. Van zodra de tenuitvoerlegging van bepaalde maatregelen voor de internetproviders te duur wordt, kan niet worden gewaarborgd dat die samenwerking efficiënt zal blijven verlopen. Wanneer het CCB bijvoorbeeld vaststelt dat er een probleem is

[17] *idem*.

a un problème affectant spécifiquement les adresses IP (*Internet Protocol*) d'un grand opérateur, on attend de ce dernier qu'il mette en garde ses clients, ce qui demande un sérieux effort. Parfois, ces acteurs coopèrent, et parfois pas. Ces entreprises jouent parfois elles-mêmes le rôle de juge et décident seules à quelles demandes elles donnent suite ou pas. Certaines osent même parfois facturer les coûts engagés dans le cadre de leur collaboration aux enquêtes.[18]

Le SPF Économie met quotidiennement le public en garde contre les phénomènes de fraude et veille au respect de la législation économique. Il effectue des analyses juridiques sur la base des signalements soumis au point de contact et informe les acteurs concernés (par exemple les plateformes de réseaux sociaux et les banques) sur le *modus operandi* des fraudeurs afin de leur permettre de bloquer l'accès à ces derniers si nécessaire. Lorsque des données exploitables (telles que des publicités, des numéros de téléphone, des comptes bancaires) apparaissent dans les dossiers, le SPF identifie les responsables. Il demande ces informations aux acteurs concernés (par exemple Facebook, Google, les banques, etc.) par l'intermédiaire desquels l'infraction est commise. Cette demande est fondée sur l'article XV.3, 5/1°, du CDE. Sur la base de cet article, les agents de contrôle du SPF Économie peuvent en effet (par dérogation aux articles 46*bis* et 46*quater* du Code d'instruction criminelle) se faire produire par toute personne, gratuitement et sur première réquisition, tous les renseignements permettant l'identification des personnes faisant l'objet d'une enquête et des personnes impliquées dans des flux financiers et de données nécessaires dans le cadre de l'enquête.

Lorsque le SPF Économie a identifié un suspect, il mène une enquête à son égard et prend les mesures nécessaires pour faire cesser la pratique concernée (par exemple en rédigeant des procès-verbaux et/ou en faisant fermer des sites web par le biais d'une procédure administrative).

— difficulté d'engager des poursuites:

La cybercriminalité fait de très nombreuses victimes. Sur le plan de la politique en matière de poursuites pénales, des choix doivent toutefois être faits et des priorités doivent être définies. Un nouveau plan national de sécurité pour la police va voir le jour. La question de la cybercriminalité y sera également abordée. Si les enquêtes réalisées dans ce domaine sont confiées à la police locale, cela risque d'être source d'inégalités. En effet, certaines zones de police disposent des moyens

[18] *Idem*.

dat specifiek de IP-adressen (IP is Internet Protocol) in het bereik van een grote operator treft, dan wordt van die laatste verwacht dat hij zijn klanten waarschuwt wat een serieuze inspanning vergt. Soms werken die actoren mee, soms ook niet. Deze bedrijven spelen soms zelf voor rechter en beslissen op eigen houtje aan welke vraag al dan niet gevolg wordt gegeven. De commerciële bedrijven durven ook weleens kosten aan te rekenen die ze hebben gemaakt in het kader van hun medewerking aan de onderzoeken.[18]

De FOD Economie waarschuwt de bevolking dagelijks over fraudefenomenen en houdt toezicht op de correcte naleving van de economische wetgeving. Zij voert juridische analyses uit van de meldingen ingediend via het Meldpunt en zij stelt de betrokken actoren (bijvoorbeeld socialemediaplatforms en banken) in kennis over de modi operandi van de fraudeur(s) waardoor deze zo nodig de toegang blokkeren. Wanneer bruikbare gegevens (zoals advertenties, telefoonnummers, bankrekeningen) in de dossiers opduiken, identificeert zij de verantwoordelijken. Zij vordert deze inlichtingen in bij de betrokken actoren (bijvoorbeeld Facebook, Google, banken.) via dewelke het misdrijf wordt gepleegd. Dit verzoek is gebaseerd op artikel XV.3, 5/1°, van het WER. Op basis van dit artikel kunnen de controleagenten van de FOD Economie (in afwijking van de artikelen 46*bis* en 46*quater* van het Wetboek van Strafvordering) zich op eerste vordering door elke persoon gratis alle inlichtingen laten verstrekken die de identificatie mogelijk maken van personen die het voorwerp uitmaken van een onderzoek en personen die betrokken zijn bij financiële stromen en gegevensstromen die noodzakelijk zijn in het kader van het onderzoek.

Wanneer zij een verdachte heeft geïdentificeerd, stelt zij een onderzoek in naar de verdachte en neemt zij de nodige maatregelen om de praktijk te stoppen (zoals processen-verbaal opstellen en/of websites laten afsluiten via een administratieve procedure).

— moeilijk vervolgbaar:

De cybercriminaliteit zorgt voor heel veel slachtoffers. In het strafvervolgingsbeleid moeten evenwel keuzes worden gemaakt en prioriteiten worden gesteld. Er komt een nieuw nationaal veiligheidsplan voor de politie. De problematiek over cybercriminaliteit komt hier ook aan bod. Indien het onderzoek daarvoor aan het lokale politieniveau wordt overgelaten, dreigt men een ongelijkheid te creëren. Sommige politiezones hebben de middelen voor dat soort onderzoek maar andere niet. Men kan

[18] *Idem*.

nécessaires pour ces enquêtes, mais d'autres pas. On peut donc se demander à quel niveau les enquêtes devraient idéalement être menées. Il existe également différents niveaux de criminalité informatique. De plus, cette forme de criminalité a souvent une dimension internationale qui appelle une approche également internationale.[19]

Une *Cyber Unit* a déjà été créée au parquet fédéral. Cette unité compte trois magistrats formés dans le domaine de la cybercriminalité et, d'ici 2022, son cadre devrait être renforcé par deux magistrats supplémentaires. Cependant, le parquet fédéral ne peut évidemment pas tout gérer. C'est pourquoi il se concentre sur les attaques perpétrées contre les infrastructures critiques. Au cours de l'audition organisée à la Chambre des représentants sur les cyberattaques menées contre les système IT de l'État et des services publics, M. Frédéric Van Leeuw, procureur fédéral, a indiqué que la magistrature du siège manifestait encore trop peu d'intérêt pour la cybercriminalité. Il est évident que cela pose des problèmes dès que ces magistrats sont confrontés à des dossiers complexes.[20]

Il ressort de ma question écrite n° 1035 qu'au total, 37982 dossiers concernant la cybercriminalité ont été transmis aux parquets en 2021, ce qui représente une augmentation de 37 % par rapport à 2019. Environ 4 % d'entre eux ont donné lieu à une assignation devant le tribunal correctionnel (après une information ou une instruction), tandis que 69 % des dossiers sont restés sans suite. Par ailleurs, 68 % des classements sans suite sont fondés sur un motif technique, ce qui empêche toutes poursuites pénales ultérieures. Les principaux motifs invoqués sont le fait que l'auteur ou les auteurs sont inconnus (57 %) et l'insuffisance de preuves (9 %). Parmi les dossiers classés sans suite, 32 % environ ont un motif d'opportunité. Il s'agit essentiellement de motifs politiques (24 %) et plus précisément de capacités d'enquête insuffisantes (18 %).[21]

Les efforts de sensibilisation (par exemple les campagnes actuellement en cours) sont certes nécessaires mais ils ne sont jamais suffisants en tant que tels. L'application de la législation est souvent trop tardive en cas de fraude en ligne (les fraudeurs créent par exemple chaque jour de nouveaux faux *webshops* qui restent en ligne pendant quelques jours tout au plus et tous les versements sont immédiatement retirés en

[19] *Idem*.
[20] *Idem*.
[21] Moyaers Bert (14 février 2022). Question n° 1035: "Le nombre de déclarations d'escroquerie sur internet, de hacking et de fraude informatique." *https://www.dekamer.be/kvvcr/showpage.cfm?section=qrva&language=fr&cfm=qrvaXml.cfm?legislat=55&dossierID=55-Bxxx-1188-1035-2021202214049.xml*.

zich dus afvragen op welk niveau welke onderzoeken het best worden gevoerd. Er zijn ook verschillende niveaus van informaticacriminaliteit. Bovendien is er vaak een internationaal aspect aan die soort van criminaliteit wat ook een internationale aanpak vergt.[19]

Binnen het federaal parket werd reeds een Cyber Unit opgericht. Die unit telt drie magistraten met een opleiding in cyberzaken en tegen 2022 zou het personeelsbestand met twee extra magistraten worden uitgebreid. Het ligt evenwel voor de hand dat het federaal parket niet alles kan beheren en daarom spitst het zich toe op de aanvallen op de kritieke infrastructuur. Federaal procureur Frédéric Van Leeuw meldde tijdens de hoorzitting over de cyberaanvallen op het IT-systeem van de Staat en de overheidsdiensten in de Kamer van volksvertegenwoordigers dat de zittende magistratuur nog te weinig interesse toont voor cybercriminaliteit. Het ligt voor de hand dat dit problemen geeft zodra zij met complexe dossiers te maken krijgt.[20]

Uit mijn schriftelijke vraag 1035 blijkt dat er in 2021 in totaal 37.982 zaken met betrekking tot. informaticacriminaliteit binnengekomen zijn op de parketten. Dit is een stijging van 37 % ten opzichte van 2019. Daarvan werd ongeveer 4 % gedagvaard voor de correctionele rechtbank (na een opsporingsonderzoek of na een gerechtelijk onderzoek), terwijl 69 % van de zaken zonder gevolg bleef. Bij 68 % van de zondergevolgstellingen ligt een technisch motief aan de oorzaak, waarbij verdere strafrechtelijke vervolging niet mogelijk is. Het gaat daarbij voornamelijk om de motieven dader(s) onbekend (57 %) en onvoldoende bewijzen (9 %). Van de zonder gevolg gestelde zaken kent ongeveer 32 % een opportuniteitsmotief. Het gaat daarbij hoofdzakelijk om beleidsmotieven (24 %), en meer bepaald te weinig recherche-capaciteiten (18 %).[21]

Inzetten op sensibiliseren is zeker nodig (lopende campagnes zijn hier het voorbeeld van) maar is op zich nooit afdoende. Het toepassen van de wetgeving is voor internetfraude vaak te laat (bijvoorbeeld fraudeurs richten iedere dag nieuwe valse webshops op die hooguit enkele dagen online zijn en alle stortingen worden onmiddellijk contant afgehaald). Een onderzoek duurt (in het beste geval) reeds enkele dagen vooraleer kan

[19] *Idem*.
[20] *Idem*.
[21] Moyaers Bert (14 februari 2022). Vraag nr.1035: "Aangiftes informaticabedrog, hacking en internetfraude" *https://www.dekamer.be/kvvcr/showpage.cfm?section=qrva&language=nl&cfm=qrvaXml.cfm?legislat=55&dossierID=55-Bxxx-1188-1035-2021202214049.xml*.

espèces). Une enquête prend (au mieux) plusieurs jours avant que les responsables puissent être identifiés. Et lorsqu'un responsable est installé à l'étranger, c'est encore plus difficile.

L'identification des suspects et sa notification manuelle aux acteurs visés par une pratique frauduleuse (par exemple aux banques) permettent de contenir presque entièrement un phénomène de fraude, mais c'est un processus long et surtout lent. Prévoir une notification automatique permettrait de gagner un temps précieux. Par exemple, lorsque le point de contact central reçoit trois signalements de fraude en ligne liés à un certain numéro de compte bancaire, la banque devrait en être avertie automatiquement. Ce serait plus efficace et plus productif pour toutes les parties prenantes. Étant donné que les consommateurs seront de plus en plus actifs en ligne à l'avenir et qu'ils feront de plus en plus d'achats sur le web, la fraude augmentera dans les mêmes proportions. Les chiffres traduisent déjà cette évolution. À l'avenir, il sera presque impossible de traiter manuellement ces grandes quantités de données et d'informer à temps les acteurs concernés, par exemple les opérateurs de télécommunications, les fournisseurs d'accès à internet, les sociétés de cartes de crédit et les banques pour qu'ils puissent réagir adéquatement. L'envoi automatique d'un avertissement aux différents acteurs concernés pourrait permettre de remédier à ce problème.

Les auteurs utilisent les nouvelles technologies pour atteindre un grand nombre de victimes potentielles en très peu de temps et en faisant le moins d'efforts possible. Ils peuvent opérer sans entrave au-delà des frontières des États, ce qui complique l'enquête pénale. En tout état de cause, les décisions d'enquête européennes ou les commissions rogatoires internationales ralentissent l'enquête.[22]

Une stratégie transfrontalière commune et coordonnée s'impose. En outre, il doit être légalement possible d'échanger des informations entre les différents services de police au niveau national comme avec l'étranger.

worden nagegaan wie verantwoordelijk is. Wanneer de verantwoordelijke in het buitenland gevestigd is, wordt het helemaal moeilijk.

Het identificeren van verdachten en het manueel op de hoogte stellen van de betrokken actoren (bijvoorbeeld de banken) van een frauduleuze praktijk, kan ervoor zorgen dat een fraudefenomeen bijna volledig wordt ingedijkt. Dit is een tijdrovend en voornamelijk langzaam proces. Als men dit proces zou kunnen implementeren via een automatisch kennisgeving zou men cruciale tijd kunnen winnen. Als het centraal meldpunt bijvoorbeeld drie meldingen krijgt over onlinefraude gerelateerd aan een bepaald bankrekeningnummer, dan zou de bank hiervan automatisch op de hoogte moeten gebracht worden. Dit zou voor alle actoren efficiënter en succesvoller zijn. Steeds meer zal men online actief zijn en online aankopen doen zodat de fraude navenant zal stijgen. Dat blijkt reeds uit de cijfers. Het zal in de toekomst bijna niet meer mogelijk zijn om deze grote hoeveelheden data manueel te verwerken en de betrokken actoren zoals de telecomoperatoren, de internet providers, de kredietkaartmaatschappijen, de banken op tijd op de hoogte te stellen zodat zij nog gepast kunnen reageren. Een automatische "*warning*" naar de verschillende betrokken actoren zou hierop een antwoord kunnen bieden.

De daders gebruiken de nieuwe technologieën om op zeer korte tijd een massa aan potentiële slachtoffers te bereiken met zo weinig mogelijk moeite. De daders kunnen ongehinderd over de staatsgrenzen heen opereren waardoor dit het strafonderzoek bemoeilijkt. Het opstellen van Europese onderzoeksbevelen of internationale rechtshulpverzoeken zorgt hoe dan ook voor vertraging in het onderzoek.[22]

Een gezamenlijke grensoverschrijdende gecoördineerde aanpak is nodig. Daarnaast dient het wettelijk mogelijk te zijn om informatie uit te wisselen tussen de verschillende politionele diensten zowel in het binnenland als het buitenland.

[22] Rapport de l'audition du 10 novembre 2020 sur "La coopération avec les entreprises technologiques dans la lutte contre la fraude financière et économique sur internet", *doc. parl.* Chambre, 2020-2021, DOC 55 1633/001.

[22] Verslag van de hoorzitting dd. 10 november 2020 over "De samenwerking met de technologiebedrijven in de strijd tegen financieel-economische internetfraude", *Parl. St.* Kamer, 2020-2021, DOC 55 1633/001.

— un cadre légal flou:

En principe, l'existence d'une base légale claire garantit une intervention plus efficace. Cette base légale claire fait défaut dans le cas de la fraude sur internet. Ainsi, le hameçonnage recouvre par exemple différentes qualifications pénales.[23] Il est parfois poursuivi sur la base de l'article 496 du Code pénal (escroquerie) ou sur la base de l'article 504*quater* de ce Code (fraude informatique).

On parle d'escroquerie (article 496 du Code pénal) lorsque trois éléments constitutifs sont réunis:

— le fait de se faire remettre ou délivrer des fonds/meubles;

— le recours par le fraudeur à des moyens frauduleux qui ont conduit à la remise. Ces moyens frauduleux sont à leur tour énumérés de manière exhaustive dans la loi (usage de faux noms ou de fausses qualités ou recours à des manœuvres frauduleuses (un mensonge ne suffit pas, il faut des actes supplémentaires qui rendent ce mensonge crédible));

— l'intention de s'approprier une chose appartenant à autrui.

L'escroquerie n'est donc pas facile à démontrer (il reste très difficile en pratique de réunir les éléments permettant de prouver l'escroquerie). Il faut également tenir compte des priorités fixées par les parquets dans leur politique de poursuites. Les tentatives d'escroquerie ne sont par exemple presque jamais poursuivies. On constate donc dans la pratique un taux de classement sans suite élevé pour la fraude sur internet (y compris pour les dossiers de hameçonnage) (voir *supra*).

Pour remédier à cette situation, on pourrait envisager d'adapter la législation de façon à créer davantage de possibilités de répression. L'intégration du hameçonnage dans le Code pénal s'inscrit dans la volonté, exprimée dans l'accord de gouvernement, de rendre le Code pénal plus précis.[24]

L'établissement d'un cadre légal spécifique permettrait d'apporter davantage de clarté et offrirait plus de possibilités de répression. On pourrait s'inspirer à cet égard des articles VI. 106 et VI. 107 du CDE, qui visent

[23] Par exemple, le fait d'accéder illégalement au système informatique de la victime peut être constitutif de piratage et la rédaction et l'envoi d'un faux courriel peuvent être constitutives de faux en informatique.

[24] "Accord de gouvernement", *Doc.parl.*, Chambre, 2019-2020, DOC 55 0020/001, p. 80. *belgium.be/nl/over_belgie/overheid/federale_overheid/federale_regering/beleid/regeerakkoord.*

— onduidelijk wettelijk kader:

In principe zorgt een duidelijke wettelijke basis voor een beter optreden. Deze duidelijke wettelijke basis ontbreekt bij internetfraude. Phishing omhelst bijvoorbeeld meerdere misdrijven.[23] Bij phishing wordt soms geverbaliseerd op basis van oplichting als bedoeld in artikel 496 van het Strafwetboek of op basis van informaticabedrog als bedoeld in artikel 504*quater* van het Strafwetboek.

Om te kunnen spreken van oplichting (artikel 496 van het Strafwetboek) moet voldaan te zijn aan drie constitutieve elementen:

— het doen afgeven of leveren van gelden/roerende goederen;

— het gebruikmaken door de fraudeur van de "bedrieglijke middelen" die "geleid hebben tot de afgifte". Deze bedrieglijke middelen worden op hun beurt limitatief opgesomd in de wet (zijnde het gebruik maken van een valse naam, van een valse hoedanigheid of van een listige kunstgreep (leugen is niet voldoende, maar bijkomende handelingen die de leugen geloofwaardig maken));

— het oogmerk om zich een zaak toe te eigenen dat aan een ander toebehoort.

Het aantonen van oplichting is dus niet vanzelfsprekend (in de praktijk blijft het heel moeilijk om de bewijslast te verzamelen om oplichting aan te tonen). Bijkomend stellen de parketten ook prioriteiten inzake het vervolgingsbeleid. Een poging tot oplichting wordt bijvoorbeeld niet of nauwelijks vervolgd. In de praktijk is er dus een hoge seponeringsgraad voor internetfraude (waaronder "phishingdossiers"). (cf. *supra*)

Een oplossing kan bestaan uit een aanpassing van de wetgeving waardoor er meer mogelijkheden worden gecreëerd inzake de handhaving. Het opnemen van phishing in het Strafwetboek kadert in de doelstelling van het regeerakkoord om het Strafwetboek accurater te maken[24].

Een specifiek wettelijk kader zorgt voor duidelijkheid en biedt meer mogelijkheden inzake de handhaving. Als inspiratie kan worden gekeken naar de artikelen VI. 106 en VI. 107 WER die specifiek malafide reclameronselaars

[23] Bijvoorbeeld het onrechtmatig toegang nemen tot het informaticasysteem van het slachtoffer kan een hacking uitmaken en het opmaken en verzenden van een valse e-mail kan een valsheid in informatica inhouden.

[24] "Het Regeerakkoord", *Parl. St.* Kamer, 2019-2020, DOC. 55 0020/001, pag. 108. *belgium.be/nl/over_belgie/overheid/federale_overheid/federale_regering/beleid/regeerakkoord.*

spécifiquement les démarcheurs publicitaires de mauvaise foi. Différents fraudeurs ont pu être condamnés sur la base de ces articles et le problème des démarcheurs publicitaires a été endigué.

Les victimes

— sensibilisation/prévention:

Près d'un travailleur sur quatre ouvre des courriels malveillants. Un quart d'entre eux communiquent même des données personnelles à cette occasion. C'est ce qui ressort d'un rapport annuel de Phished, une entreprise située à Louvain qui dispense des formations sur le hameçonnage. Il est donc très important de poursuivre la sensibilisation.

Les signalements faits au point de contact ont actuellement une double fonction. Il s'agit tout d'abord d'une demande d'assistance (individuelle), mais ces signalements permettent également de recueillir des éléments en vue d'évaluer l'ampleur de certains phénomènes et de détecter les véritables problèmes qui se posent. Une troisième fonction pourrait être envisagée (fonction de vérification): on mettrait ces informations à la disposition du citoyen par le biais d'une fonction de recherche, de façon à promouvoir la prévention. On pourrait créer dans le cadre du point de contact un lien "Vérifier le vendeur" qui ferait office de fonction de vérification. Avant d'acheter ou de vendre, les citoyens auraient ainsi la possibilité de vérifier si d'autres personnes ont eu des expériences négatives avec le vendeur ou l'acheteur. Le citoyen/consommateur pourrait effectuer des recherches à partir de numéros de compte IBAN, d'adresses électroniques, de numéros de téléphone ou d'un URL (*uniform resource locator* ou adresse internet) d'un magasin en ligne/d'un site internet, par exemple. Cet outil existe déjà dans plusieurs États membres (on peut notamment citer le *Landelijk meldpunt internetoplichting* néerlandais).

Ainsi qu'il a été indiqué ci-dessus, l'approche fragmentée est néfaste. La création d'un point de contact central ou d'une plateforme de base permettrait aux citoyens d'obtenir plus rapidement des informations et une assistance.

— protection/assistance:

Il est malheureusement rare que les victimes récupèrent leur argent. En effet, les cybercriminels prennent très vite possession des fonds. Une fois l'enquête terminée, il ne reste plus grand-chose à récupérer.

Quand une victime fait une déclaration à la police, un procès-verbal est établi. Le magistrat de garde est

viseren. Op basis van deze artikelen werden verschillende fraudeurs veroordeeld en werd de problematiek van reclameronselaars ingedijkt.

Slachtoffers

— sensibiliseren/preventie:

Bijna een op vier werknemers klikt op malafide mails. Nog eens een kwart van hen vult zelfs persoonlijke gegevens in. Dat blijkt uit een jaarrapport van Phished, een Leuvens bedrijf dat aan phishingtraining doet. De nood om mensen te blijven sensibiliseren, is dus groot.

De meldingen die binnenkomen bij het Meldpunt hebben momenteel een dubbele functie. Enerzijds zijn ze een vraag tot (individuele) hulpverlening en anderzijds vormen ze signalen waardoor de omvang van bepaalde fenomenen kan worden ingeschat en de echte problemen in de markt kunnen worden gedetecteerd. Een derde functie zou kunnen zijn om die informatie beschikbaar te stellen aan de burger via een opzoekingsfunctie en zo preventie mogelijk te maken (zogenaamde checkfunctie). "Check de verkoper" zou een link kunnen zijn die wordt aangebracht bij het meldpunt en als checkfunctie zou kunnen fungeren. De burger zou aldus, voor hij iets koopt of verkoopt, kunnen controleren of er met de (ver)koper negatieve ervaringen zijn geweest. De burger/consument kan dan zoeken op IBAN-rekeningnummers, e-mailadressen, telefoonnummers of een URL (*uniform resource locator* of internetadres) van bijvoorbeeld een webwinkel/website. Deze tool bestaat reeds in verschillende lidstaten (bijvoorbeeld het Landelijk meldpunt internetoplichting in Nederland).

Zoals hierboven al besproken is een versnipperde aanpak nefast. Een centraal aanspreekpunt of basisplatform zorgt ervoor dat de burger niet al te lang moet zoeken naar informatie en bijstand.

— bescherming/hulp:

De slachtoffers krijgen helaas zelden hun geld terug. De gelden vertrekken immers zeer snel bij de internetcriminelen. Op het moment dat een dergelijk onderzoek wordt afgesloten, valt er niet veel meer te rapen.

Wanneer een slachtoffer aangifte doet bij de politie wordt er een proces-verbaal opgemaakt. De dienstdoende

chargé de transmettre une réquisition à la police afin de bloquer les avoirs des comptes et d'identifier le propriétaire. La réquisition est transmise à l'établissement bancaire qui active le blocage dans les plus brefs délais. Avec un peu de chance, une partie du préjudice peut être récupérée. Généralement, l'argent a déjà disparu du compte. La plupart des cas se produisent juste avant le week-end car il est plus difficile de contacter les banques à ce moment-là.

En cas de fraude (hameçonnage par exemple), la législation (articles VII.38 et suivants du CDE) prévoit en fait deux cas dans lesquels la banque doit prendre en charge le préjudice financier:

— si le client était dans l'impossibilité de constater l'utilisation illégitime de son instrument de paiement avant qu'un paiement ne soit effectué. Cela signifie, par exemple dans le cas d'un hameçonnage, que la banque est tenue de compenser intégralement les pertes financières du client, à condition que ce dernier ait respecté les conditions d'utilisation de la banque et qu'il ait signalé la perte, le vol, l'utilisation illégitime ou l'utilisation non autorisée de son instrument de paiement à temps à la banque;

— si le client aurait pu constater l'utilisation illégitime de l'instrument de paiement avant qu'un paiement ne soit effectué. Dans un tel cas, la banque doit prendre le préjudice en charge après déduction d'une franchise de 50 euros, à moins que le client n'ait pas respecté certaines obligations en raison d'une négligence grave. Il est par exemple question de négligence grave si le client a noté ses codes secrets sous une forme aisément identifiable et les a conservés à proximité sa carte bancaire, ou s'il n'a pas informé sa banque à temps d'une suspicion de perte, de vol ou d'utilisation illégitime de sa carte bancaire.

En l'occurrence, la notion de négligence grave est relativement subjective. L'exposé des motifs ne donne pas davantage de possibilités d'interprétation et dès lors que l'article VII. 43 CDE n'est en vigueur que depuis le 9 août 2018, la jurisprudence sur laquelle baser une interprétation est limitée. Les prestataires de services de paiement interprètent dès lors la notion de "négligence grave" comme ils l'entendent, avec pour conséquence que les victimes de hameçonnage, par exemple, ne sont pas indemnisées par ces prestataires.

Ombudsfin constate également que les résultats de la médiation dans les cas de fraude sont moins positifs que les années précédentes. Seul un tiers des plaintes pour hameçonnage considérées fondées par Ombudsfin ont pu être résolues. En effet, la question de savoir si

magistraat wordt verzocht om een vordering aan de politie te bezorgen om de tegoeden op de rekening te blokkeren en de eigenaar te identificeren. De vordering wordt bezorgd aan de bankinstelling, die, naargelang de instelling, de blokkering asap (*as soon as possible*) uitvoert. Met wat geluk kan af en toe nog een deel van het nadeel gerecupereerd worden. Meestal zijn de gelden reeds verdwenen van de rekening. De meeste gevallen spelen zich af net voor het weekend omdat de banken dan maar beperkt contacteerbaar zijn.

In geval van fraude (bijvoorbeeld phishing) bepaalt de wetgeving (artikel VII.38 en volgende van het WER) in feite twee gevallen waarin de bank het financieel verlies dient te dragen:

— indien de klant het onrechtmatig gebruik van zijn betaalinstrument niet kon vaststellen voordat een betaling plaatsvond. Dit betekent dat in geval van bijvoorbeeld phishing de bank verplicht is om de financiële verliezen van de cliënt volledig te vergoeden op voorwaarde dat de cliënt de gebruiksvoorwaarden van de bank heeft nageleefd en het verlies, de diefstal, het onrechtmatig gebruik of het niet-toegestane gebruik van het betaalinstrument op tijd heeft gemeld aan de bank.

— indien de klant het onrechtmatig gebruik van het betaalinstrument wel kon vaststellen voordat een betaling plaatsvond. Op basis hiervan dient de bank het verlies te dragen, na aftrek van een franchise van 50 euro, tenzij de betaler door grove nalatigheid bepaalde verplichtingen niet is nagekomen. Van grove nalatigheid is bijvoorbeeld sprake wanneer de klant zijn geheime codes in een gemakkelijk herkenbare vorm genoteerd heeft en bij zijn bankkaart heeft bewaard, alsook het niet tijdig in kennis stellen van zijn bank indien de klant verlies, diefstal of het onrechtmatig gebruik van zijn bankkaart vermoedt.

Het begrip grove nalatigheid is in deze redelijk subjectief. De memorie van toelichting geeft ook niet veel mogelijkheden tot betere interpretatie en gezien het artikel VII. 43 WER pas sinds 9 augustus 2018 in voege is, is er ook weinig rechtspraak om de interpretatie op te baseren. De betalingsdienstaanbieder interpreteren "grove nalatigheid" dan ook naar believen met als gevolg dat slachtoffers van bijvoorbeeld phishing niet worden terugbetaald door de betalingsdienstaanbieders.

Ook Ombudsfin stelt vast dat de bemiddelingsresultaten in fraudedossiers minder positief zijn dan de voorgaande jaren. Slechts een derde van de phishingdossiers die Ombudsfin gegrond achtte, kon worden opgelost. Dit komt omdat de vraag of banken al dan

les banques sont légalement tenues ou non d'intervenir dans les dommages résultant d'opérations de paiement non autorisées dépend du fait que la fraude aurait pu ou non être détectée à l'avance par la victime et de l'évaluation de la négligence grave de la part de la victime (voir le rapport annuel 2019). Les deux évaluations exigent que toutes les circonstances factuelles soient prises en compte. Les banques apprécient actuellement les faits d'une manière différente que Ombudsfin.[25]

Le juge d'instruction Philippe Van Linthout perçoit une contradiction entre les grandes exigences en matière de sécurité dont se targuent les banques et la facilité d'utilisation de leurs applications. Ces applications permettent aux clients de s'identifier et de transférer des montants importants dans le monde entier avec leur smartphone. Les comptes privés et les comptes d'entreprise sont accessibles au travers de la même technologie, de telle sorte que tous les comptes peuvent être pillés si le mot de passe est connu.

"Un SMS contenant un code d'accès pour confirmer la transaction peut déjà permettre au client de détecter des opérations suspectes et d'avertir sa banque", selon M. Van Linthout. "Les transactions Visa sur internet devraient s'accompagner systématiquement d'un contrôle par la banque. De nombreux utilisateurs s'agacent de devoir sortir leur boîtier pour une transaction sur internet, alors qu'il s'agit d'une protection efficace. Certaines banques ont recours à un algorithme qui signale les paiements anormaux, alors que d'autres ne font quasiment rien. La fraude dans le monde numérique est d'une simplicité effrayante."[26] (traduction)

Il y a par ailleurs la problématique des mules bancaires qui, comme les étudiants, sont très souvent victimes de fraude à l'amitié. Des données sont utilisées pour ouvrir un crédit auprès de banques en ligne. Il est très facile d'ouvrir un compte avec seulement un selfie, par exemple, en guise de contrôle. La législation antiblanchiment est bonne mais elle n'est pas respectée à cet égard. Il faut davantage de contrôles de la part de l'Autorité des services et marchés financiers (FSMA).

niet wettelijk tot tussenkomst in de schade ten gevolge van niet toegestane betalingstransacties gehouden zijn, afhankelijk is van de vraag of de fraude al dan niet op voorhand gedetecteerd kon worden door het slachtoffer en van de beoordeling van een grove nalatigheid in zijn hoofde. Voor beide beoordelingen dient rekening te worden gehouden met alle feitelijke omstandigheden. We stellen vast dat de banken de feiten op dit moment op een andere wijze beoordelen dan Ombudsfin.[25]

Onderzoeksrechter Philippe Van Linthout ziet een tegenstelling tussen de hoge veiligheidseisen die de banken claimen en hun gebruiksvriendelijke apps. Via die app op hun smartphone kunnen hun klanten zich identificeren en wereldwijd grote bedragen overschrijven. Privé- en bedrijfsrekeningen zijn via dezelfde technologie toegankelijk zodat alle rekeningen kunnen worden geplunderd als het paswoord bekend is.

"Eén sms met een toegangscode om de transactie te bevestigen kan de klant al snel waarschuwen van verdachte bewegingen zodat hij de bank kan verwittigen", zegt de heer Van Linthout. "Ook zouden Visatransacties op het internet steevast gepaard moeten gaan met een controle via de bank. Veel gebruikers zijn geprikkeld als ze voor een internettransactie hun bakje moeten bovenhalen, terwijl hen dat perfect beschermt. Sommige banken grijpen in met een algoritme dat ongewone betalingen signaleert. Andere doen nauwelijks iets. Het is ronduit schrikbarend hoe eenvoudig fraude is in de cyberwereld."[26]

Daarnaast heeft men de geldezels die net als studenten ook zeer vaak slachtoffers van vriendschapsfraude zijn. Gegevens worden gebruikt om een krediet te openen bij internetbanken. Het is heel gemakkelijk om een rekeningnummer te openen met enkel een selfie, enzo meer… als controle. De antiwitwaswetgeving zit goed maar wordt hierin niet nageleefd. Er is dus nood aan meer controles door de Autoriteit voor Financiële Diensten en Markten (FSMA).

Bert MOYAERS (Vooruit)

---

25 Ombudsfin, *Rapport annuel 2020 https://www.ombudsfin.be/sites/default/files/RA-Ombudsfin%202020_0.pdf.*

26 Brockmans, H., Juge d'instruction Philippe Van Linthout, "*Het is schrikbarend hoe eenvoudig fraude is in de cyberwereld*", *Trends,* 27 janvier 2022. *https://trends.knack.be/economie/beleid/onderzoeksrechter-philippe-van-linthout-het-is-schrikbarend-hoe-eenvoudig-fraude-is-in-de-cyberwereld/article-longread-1827183.html.*

25 "Jaarverslag 2020 Ombudsfin" *ombudsfin.be/sites/default/files/JV-Ombudsfin%202020_0.pdf.*

26 Brockmans, H., Onderzoeksrechter Philippe Van Linthout: "*Het is schrikbarend hoe eenvoudig fraude is in de cyberwereld*" in *Trends* van 27 januari 2022. *trends.knack.be/economie/beleid/onderzoeksrechter-philippe-van-linthout-het-is-schrikbarend-hoe-eenvoudig-fraude-is-in-de-cyberwereld/article-longread-1827183.html.*

PROPOSITION DE RÉSOLUTION

La Chambre des représentants,

A. constatant que plusieurs points de contact et/ou sites web s'adressent aux consommateurs et/ou victimes de fraude sur internet;

B. constatant que la lutte contre la fraude sur internet est éparpillée, plusieurs services publics travaillant dès lors sur les mêmes dossiers sans établir de liens entre eux;

C. soulignant la pénurie de personnel spécialisé dans le domaine de cybercriminalité au sein de la police intégrée;

D. concluant qu'il est difficile d'attirer du personnel à cause des structures rigides et des statuts;

E. constatant que les zones de police locale sont souvent confrontées à des plaintes en matière de cybercriminalité et qu'il convient d'accorder plus d'attention à ce problème;

F. déplorant que la formation requise en matière d'interaction virtuelle n'ait pas encore été organisée;

G. constatant que l'obligation d'information légale à l'égard des autorités administratives et judiciaires est à peine respectée par certains prestataires de services;

H. déplorant que l'absence de coopération de ces prestataires de services ne soit pas sanctionnée en conséquence;

I. concluant qu'il convient de mieux encadrer, au niveau européen, la coopération entre les prestataires de services technologiques;

J. constatant que plus de la moitié des déclarations sont classées sans suite, ce qui empêche les poursuites pénales ultérieures;

K. observant que l'identification des suspects et l'information des acteurs concernés prennent beaucoup de temps et s'appuient surtout sur une procédure lente;

L. constatant l'absence de base légale claire réglant la fraude sur internet;

M. constatant que le gouvernement investit beaucoup dans la sensibilisation des citoyens, mais qu'il n'existe pas aujourd'hui de point de contact central;

VOORSTEL VAN RESOLUTIE

De Kamer van volksvertegenwoordigers,

A. stelt vast dat er verschillende meldpunten en websites bestaan voor de consument en/of het slachtoffer van internetfraude;

B. constateert dat er een versnipperde aanpak bestaat inzake internetfraude waardoor verschillende overheidsdiensten op dezelfde dossiers werken en de linken tussen de dossiers niet gemaakt worden;

C. wijst op het tekort aan gespecialiseerd personeel inzake cybercriminaliteit bij de geïntegreerde politie;

D. concludeert dat het moeilijk is om personeel aan te trekken door de strakke structuren en statuten;

E. stelt vast dat lokale politiezones vaak worden geconfronteerd met klachten over cybercriminaliteit en er meer aandacht nodig is voor deze problematiek;

F. laakt dat de vereiste opleiding inzake virtuele interactie nog niet werd georganiseerd;

G. stelt vast dat de wettelijke informatieplicht jegens de bestuurlijke en de gerechtelijke autoriteiten door sommige dienstverleners amper in acht wordt genomen;

H. laakt dat de niet-medewerking van deze dienstverleners niet navenant bestraft wordt;

I. concludeert dat de medewerking van de technologische dienstverleners beter moet worden afgedwongen op Europees niveau;

J. stelt vast dat meer dan de helft van de aangiftes zonder gevolg blijft waardoor verdere strafrechtelijke vervolging niet mogelijk is;

K. merkt dat het identificeren van verdachten en het manueel op de hoogte stellen van de betrokken actoren zeer tijdrovend en voornamelijk een langzaam proces is;

L. concludeert dat bij internetfraude een duidelijke wettelijke basis ontbreekt;

M. stelt vast dat de regering veel inzet op het sensibiliseren van de burger maar een centraal aanspreekpunt momenteel ontbreekt;

N. constatant que les prestataires de services de paiement interprètent à leur guise la notion de négligence grave visée à l'article VII.43 du Code de droit économique;

O. soulignant l'attitude parfois passive des prestataires de services de paiement à l'égard de la détection préventive des transactions inhabituelles;

P. déplorant la facilité avec laquelle les criminels peuvent ouvrir un crédit en ligne en utilisant les données de leurs victimes;

Demande au gouvernement fédéral:

1. de créer un point de contact central ou une plateforme de base où le consommateur ou la victime pourra à la fois porter plainte ou demander des informations;

2. de créer un service fédéral spécialisé de lutte contre la fraude qui assure une coordination centrale et réunit des délégués de tous les services agissant en qualité d'officiers de liaison entre les services publics et le service de lutte contre la fraude. Les piliers suivants y sont intégrés:

a. le traitement et la diffusion des plaintes: toutes les informations/tous les signaux doivent être envoyés à un service de coordination afin de pouvoir déterminer les mesures à prendre dans un délai très court;

b. le traitement et la diffusion des informations dans un souci d'efficacité et de réduction de la charge de travail en évitant d'accomplir deux fois la même tâche;

c. l'analyse des plaintes de deuxième ligne, la perception du phénomène, le suivi et l'étude de marché: cela permet de formuler des propositions de mesures supplémentaires, d'élaborer de nouvelles méthodes de recherche, de proposer des projets de loi, d'adapter la législation en vigueur, etc.;

d. la coordination des gros dossiers multithématiques et/ou transrégionaux/internationaux;

e.le suivi et la prise en compte des nouvelles tendances par le biais d'une coopération et d'un feed-back avec tous les services compétents;

f. le souci d'éviter la multiplication des signalements et des victimes en répondant de manière adéquate et efficace à la fraude;

N. stelt vast dat de betalingsdienstaanbieders het begrip grove nalatigheid in artikel VII. 43 van het Wetboek van Economisch Recht naar believen interpreteren;

O. wijst op de soms passieve ingesteldheid van betaaldienstverleners bij het preventief opsporen van ongewone transacties;

P. laakt het gemak waarmee criminelen op basis van gegevens van slachtoffers een onlinekrediet kunnen openen;

Verzoekt de federale regering:

1. één centraal aanspreekpunt of basisplatform op te richten waar de consument/slachtoffer terecht kan voor zowel klachten als informatie;

2. een gespecialiseerde federale fraudebestrijdingsdienst op te richten die zorgt voor een overkoepelende coördinatie en waarin afgevaardigden van alle diensten vertegenwoordigd zijn die werken als liaisonofficier tussen de diverse overheidsdiensten en de federale fraudebestrijdingsdienst. Daarin worden de volgende pijlers verwerkt:

a. klachtenverwerking en klachtenverdeling: alle informatie/signalen dienen naar een coördinerende dienst verzonden te worden, zodoende er op zeer korte tijd bepaald kan worden welke maatregelen dienen genomen te worden;

b. informatieverwerking en informatieverdeling om efficiëntie te bekomen en de werkdruk te verminderen door dubbel werk te vermijden;

c. tweedelijnsklachtenanalyse, beeldvorming, monitoring en marktstudie waardoor voorstellen voor bijkomende maatregelen geformuleerd kunnen worden, nieuwe onderzoeksmethoden kunnen worden ontwikkeld en uitgewerkt, wetsontwerpen kunnen worden voorgesteld en de vigerende wetgeving kan worden aangepast, *et cetera*…;

d. coördineren van grote dossiers die thematisch en/of regionaal/internationaal overschrijdend zijn;

e. het opvolgen en ageren van nieuwe markttendensen via samenwerking en terugkoppeling met alle bevoegde diensten;

f. het vermijden van een "pingpong" van meldingen en slachtoffers door adequaat en efficiënt op fraude te reageren;

3. de mettre en place une banque de données nationale qui récoltera et exploitera les informations disponibles;

4. d'investir dans l'automatisation des données entre les différents acteurs;

5. d'attirer, au sein de la *Federal Computer Crime Unit* (FCCU), des *Regional Computer Crime Units (RCCU)* et de la police intégrée, suffisamment d'enquêteurs spécialisés capables d'enquêter sur les infractions liées au web;

6. de dispenser à tous les services de police une formation actualisée en permanence sur la cybercriminalité;

7. de mettre à disposition un manuel numérique que la police pourra utiliser si elle est confrontée à des affaires/victimes de ce type;

8. d'examiner comment la police peut attirer du personnel doté d'une expertise suffisante;

9. d'investir dans des équipes d'enquête communes réunissant des enquêteurs techniques et tactiques;

10. d'encourager la mise en place d'un plus grand nombre de *Local Crime Computer Units* (LCCU) dans différentes zones travaillant de manière transfrontalière dans les domaines de l'accueil, de l'enquête, de l'assistance aux victimes, etc.;

11. d'organiser la formation légale requise pour les services de police ordinaires en matière d'interaction virtuelle;

12. d'examiner comment le cadre légal pourrait être modifié pour imposer également l'identification aux prestataires de services étrangers;

13. de responsabiliser davantage les intermédiaires techniques de l'internet afin qu'ils soient proactifs dans la détection des fraudes et qu'ils luttent contre celles-ci;

14. d'œuvrer à la mise en place structurelle et formelle de partenariats avec les acteurs technologiques;

15. d'examiner quelles sanctions plus lourdes peuvent éventuellement être infligées en cas de non-collaboration des prestataires de services technologiques, comme le refus d'accès aux utilisateurs belges ou une amende proportionnelle au chiffre d'affaires de l'entreprise technologique;

3. een nationale databank voor onlinefraude op te richten die de beschikbare informatie verzamelt en exploiteert;

4. te investeren in het automatiseren van de data tussen de verschillende actoren;

5. voldoende gespecialiseerde onderzoekers aan te trekken bij de *Federal Computer Crime Unit* (FCCU), de *Regional Computer Crime Units* (RCCU) en de geïntegreerde politie die internetgerelateerde misdrijven kunnen onderzoeken;

6. blijvende geüpdate vorming over cybercriminaliteit te geven voor alle politiediensten;

7. een digitale handleiding ter beschikking te stellen die de politie kan volgen als ze met dergelijke zaken/slachtoffers wordt geconfronteerd;

8. te onderzoeken hoe de politie personeel kan aantrekken dat over voldoende expertise beschikt;

9. in te zetten op gemeenschappelijke onderzoeksteams met zowel technische als tactische rechercheurs;

10. meer *Local Crime Computer Units* (LCCU) in verschillende zones aan te moedigen die grensoverschrijdend werken inzake onthaal, recherche, slachtofferbejegening, …;

11. de noodzakelijke wettelijk vereiste opleiding voor de reguliere politiediensten inzake virtuele interactie te organiseren;

12. te onderzoeken hoe het wettelijk kader kan worden aangepast om het mogelijk te maken om ook bij buitenlandse dienstverleners een identificatie af te dwingen;

13. technische tussenpersonen op het internet verder te responsabiliseren om fraude proactief op te merken en hiertegen actie te ondernemen;

14. in te zetten op het structureel en formeel vastleggen van samenwerkingsverbanden met technologische actoren;

15. te onderzoeken welke mogelijke zwaardere straffen kunnen worden opgelegd bij niet-medewerking van de technologische dienstverleners zoals het ontzeggen van toegang tot de Belgische gebruikers of een geldboete in verhouding tot de omzet van het technologiebedrijf;

16. de plaider, au niveau européen, en faveur d'une coordination accrue permettant aux autorités policières et judiciaires nationales d'exiger, sur tout le territoire de l'Union européenne, la coopération de plateformes pour fournir certaines données concrètes;

17. d'accorder au parquet, dans le cadre d'une enquête, un accès gratuit aux données concernées, car pour l'instant les renseignements à fournir sont souvent facturés à la Justice;

18. de développer un système de notification automatique aux différents acteurs concernés de telle sorte que ceux-ci puissent réagir plus vite et plus efficacement aux signalements;

19. de modifier la législation en vigueur dans le but d'adapter les méthodes d'investigation à la criminalité du 21e siècle, comme l'infiltration des réseaux sociaux et le *mystery shopping*;

20. d'adapter le cadre légal de manière à créer une base légale claire permettant de mieux lutter contre des pratiques telles que le hameçonnage dans les différents codes dont le Code de droit économique et le Code pénal;

21. de procéder, tous les cinq ans, à une analyse du cadre légal afin de vérifier sa pertinence en fonction des nouvelles techniques utilisées par les cybercriminels;

22. d'ajouter au point de contact central une fonction de vérification permettant au citoyen, avant d'acheter ou de vendre quelque chose, de contrôler très facilement par le biais d'une fonction de recherche – grâce au numéro de compte IBAN, à une adresse électronique ou une URL –, s'il y a eu des expériences négatives en lien avec l'acheteur/le vendeur;

23. d'examiner si les conditions prévues à l'article VII.43 du Code de droit économique sont bien respectées, de déceler d'éventuelles lacunes et d'examiner la nécessité de modifier la législation et d'assouplir les conditions afin de mieux aider les victimes (par exemple en cas de négligence grave);

24. d'examiner, de concert avec les acteurs concernés, la possibilité de ralentir les virements en temps réel en faveur de fournisseurs de crypto-monnaies et de transmetteurs de fonds;

16. op Europees vlak te pleiten voor meer coördinatie waardoor nationale politionele en gerechtelijke autoriteiten op het hele grondgebied van de Europese Unie de medewerking zouden kunnen opeisen van platformen om bepaalde concrete gegevens te verschaffen;

17. het parket een kosteloze toegang te verschaffen tot de betrokken data in het raam van een onderzoek omdat deze gegevens nu vaak aan Justitie worden aangerekend;

18. een systeem te ontwikkelen waarbij een automatische kennisgeving naar de verschillende betrokken actoren wordt uitgestuurd zodat deze actoren sneller en efficiënter de meldingen kunnen aanpakken;

19. de vigerende wetgeving te wijzigen met als doel de onderzoeksmethoden aan te passen aan de criminaliteit van de 21e eeuw zoals de infiltratie op sociale media en de mystery shopping;

20. het wettelijk kader aan te passen zodat er een duidelijke wettelijke basis kan gecreëerd worden om praktijken zoals phishing beter aan te pakken in de verschillende wetboeken zoals het Wetboek van Economisch Recht en het Strafwetboek;

21. elke vijf jaar een analyse uit te voeren van het wettelijke kader om af te toetsen of het nog afdoende is in functie van de nieuwe technieken waarmee cybercriminelen opereren;

22. op het centraal aanspreekpunt een checkfunctie toe te voegen waarbij de burger zeer eenvoudig via een opzoekingsfunctie – met het IBAN-rekeningnummer, een e-mailadres, een telefoonnummer of een URL – kan controleren, alvorens hij iets koopt of verkoopt, of er met de (ver)koper negatieve ervaringen zijn geweest;

23. te bekijken of de voorwaarden bepaald in artikel VII.43 van het Wetboek van Economisch Recht goed wordt nageleefd, de gebreken in kaart te brengen en na te gaan of een aanpassing van de wetgeving nodig is en de voorwaarden soepeler moeten worden vastgelegd om de slachtoffers beter te helpen (bijvoorbeeld bij grove nalatigheid);

24. met de betrokken actoren te onderzoeken of het mogelijk is om realtime-overschrijvingen naar cryptocurrency-aanbieders en *money transmitters* te vertragen;

25. de charger l'Autorité des services et marchés financiers (FSMA), sur la base de la législation anti-blanchiment, de procéder à des contrôles spécifiques des banques en ligne lors de l'ouverture d'un numéro de compte.

21 mars 2022

25. de Autoriteit voor Financiële Diensten en Markten (FSMA) opdracht te geven om, op basis van de anti-witwaswetgeving, specifiek controle uit te voeren bij internetbanken bij het openen van een rekeningnummer.

21 maart 2022

Bert MOYAERS (Vooruit)

Imprimerie centrale – Centrale drukkerij