DOC 55 **1633/001**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

10 novembre 2020

LA COOPÉRATION AVEC LES ENTREPRISES TECHNOLOGIQUES DANS LA LUTTE CONTRE LA FRAUDE FINANCIÈRE ET ÉCONOMIQUE SUR INTERNET

Audition

RAPPORT

FAIT AU NOM DE LA COMMISSION
DE L'ÉCONOMIE,
DE LA PROTECTION DES CONSOMMATEURS
ET DE L'AGENDA NUMÉRIQUE
PAR
M. **Michael FREILICH**

SOMMAIRE Pages

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

10 november 2020

DE SAMENWERKING MET DE TECHNOLOGIEBEDRIJVEN IN DE STRIJD TEGEN FINANCIEEL-ECONOMISCHE INTERNETFRAUDE

Hoorzitting

VERSLAG

NAMENS DE COMMISSIE
VOOR ECONOMIE,
CONSUMENTENBESCHERMING
EN DIGITALE AGENDA
UITGEBRACHT DOOR
DE HEER **Michael FREILICH**

INHOUD Blz.

03432

Composition de la commission à la date de dépôt du rapport/
Samenstelling van de commissie op de datum van indiening van het verslag
Président/Voorzitter: Stefaan Van Hecke

A. — Titulaires / Vaste leden:		**B. — Suppléants / Plaatsvervangers:**
N-VA	Michael Freilich, Katrien Houtmeyers, Anneleen Van Bossuyt	Peter De Roover, Joy Donné, Frieda Gijbels, Wouter Raskin
Ecolo-Groen	N, Stefaan Van Hecke, Dieter Vanbesien, Albert Vicaire	Julie Chanson, Laurence Hennuy, N, Gilles Vanden Burre
PS	Christophe Lacroix, Patrick Prévot, Philippe Tison	Malik Ben Achour, Ahmed Laaouej, Eliane Tillieux
VB	Erik Gilissen, Reccino Van Lommel	Katleen Bury, Wouter Vermeersch, Hans Verreyt
MR	Denis Ducarme, Florence Reuter	Nathalie Gilson, Kattrin Jadin, Benoît Piedboeuf
CD&V	Leen Dierick	N, Jef Van den Bergh
PVDA-PTB	Roberto D'Amico	Maria Vindevoghel, Thierry Warmoes
Open Vld	Kathleen Verhelst	Robby De Caluwé, Christian Leysen
sp.a	Melissa Depraetere	Anja Vanrobaeys, Kris Verduyckt

C. — Membres sans voix délibérative / Niet-stemgerechtigde leden:

cdH	Maxime Prévot
DéFI	Sophie Rohonyi

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*
sp.a	:	*socialistische partij anders*
cdH	:	*centre démocrate Humaniste*
DéFI	:	*Démocrate Fédéraliste Indépendant*
INDEP-ONAFH	:	*Indépendant - Onafhankelijk*

Abréviations dans la numérotation des publications:		*Afkorting bij de numering 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 defi nitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)*
PLEN	*Séance plénaire*	*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)*

MESDAMES, MESSIEURS,

Au cours de sa réunion du 16 septembre 2020, votre commission a décidé de consacrer une audition à la coopération avec les entreprises technologiques dans la lutte contre la fraude financière et économique sur Internet.

Au cours de cette audition, qui a eu lieu le 14 octobre 2020, les personnes suivantes ont été entendues:

— M. Olivier Bogaert, commissaire, *Federal Computer Crime Unit*, Police fédérale;

— Mme Cécile Coppin, experte e-commerce, Direction générale de l'Inspection économique, SPF Économie;

— Mme Phédra Clouner, *deputy director*, *Centre for Cyber Security Belgium*;

— M. Robrecht De Keersmaecker, substitut du procureur général d'Anvers, coordinateur principal du réseau d'expertise Cybercrime;

— M. Geert Baudewijns, CEO, Secutec.

I. — **EXPOSÉS INTRODUCTIFS**

A. **Exposé introductif de M. Olivier Bogaert (FCCU)**

Monsieur Olivier Bogaert entend exposer la fraude internet comme perçue au niveau de la police fédérale. Concrètement, la fraude internet n'est pas la même chose que la fraude informatique, pour laquelle il existe déjà un article dans le code pénal (article 504*quater*), même si cette dernière peut faire partie du mode opératoire.

Une fraude internet est une escroquerie classique qui utilise le numérique comme outil.

Infractions pénales qui se trouvent déjà dans le code pénal:

— escroquerie: article 496;

— fraude informatique: article 504*quater*;

— faux en informatique: article 210*bis*;

— hacking: article 550*bis*;

— sabotage informatique: article 550*ter*;

DAMES EN HEREN,

Uw commissie heeft tijdens haar vergadering van 16 september 2020 beslist een hoorzitting te houden over de samenwerking met de technologiebedrijven in de strijd tegen financieel-economische internetfraude.

Tijdens deze hoorzitting, die heeft plaatsgevonden op 14 oktober 2020, werden gehoord:

— de heer Olivier Bogaert, commissaris, *Federal Computer Crime Unit*, Federale Politie;

— mevrouw Cécile Coppin, experte e-commerce, Algemene Directie Economische Inspectie, FOD Economie;

— mevrouw Phédra Clouner, *deputy director*, *Centre for Cyber Security Belgium*;

— de heer Robrecht De Keersmaecker, substituut-procureur-generaal te Antwerpen, hoofdcoördinator Expertisenetwerk Cybercrime;

— de heer Geert Baudewijns, ceo, Secutec.

I. — **INLEIDENDE UITEENZETTINGEN**

A. **Inleidende uiteenzetting van de heer Olivier Bogaert (FCCU)**

De heer Olivier Bogaert licht internetfraude toe vanuit de invalshoek van de federale politie. Concreet is internetfraude niet hetzelfde als informaticafraude (die al is vervat in artikel 504*quater* van het Strafwetboek), al kan informaticafraude wel deel uitmaken van de *modus operandi*.

Internetfraude is een klassieke vorm van oplichting waarbij gebruik wordt gemaakt van digitaal gereedschap.

De volgende strafmisdrijven zijn al in het Strafwetboek opgenomen:

— oplichting: zie artikel 496;

— informaticabedrog: zie artikel 504*quater*;

— valsheid in informatica: zie artikel 210*bis*;

— hacking: zie artikel 550*bis*;

— computersabotage: zie artikel 550*ter*;

— usurpation d'identité: article 231;

— faux en écriture: article 193.

Tendances (faits le plus fréquemment rapportés)

— fraudes commerciales en ligne (achats ou ventes): par exemple, pendant la crise du COVID-19 il y avait beaucoup d'annonces pour des masques ou des désinfectants, mais souvent le consommateur ne recevait rien);

— fraudes au président (utiliser le nom du chef d'entreprise afin de cibler certaines autres personnes);

— fraudes au logiciel malveillant (ou *cryptolocker*: logiciel qui va bloquer toutes les données au sein d'une entreprise);

— fraudes à l'acompte;

— fraudes au placement;

— fraudes aux émotions (par exemple, pendant la crise du COVID-19 beaucoup de personnes se sont rendues sur des faux sites de rencontres virtuelles et les personnes qui sont tombées dans le piège sont devenues après des victimes de chantage);

— vol d'identité.

Comment? (Mode opératoire)

— la victime a diffusé beaucoup d'informations personnelles et professionnelles;

— LinkedIn, principal outil visant le monde professionnel: quand on effectue quelques recherches simples dans les rapports annuels des entreprises on trouve facilement les coordonnées des personnes qui occupent des fonctions de comptabilité ou de gestion au sein d'une entreprise; on va alors envoyer un document que la personne ouvre et qui sera la source de l'infection;

— Facebook, Instagram, … sont utilisés pour cibler le particulier via, notamment, les contenus sponsorisés, par exemple des profils de personnes (la RTBF en est victime pour l'instant) pour des placements bitcoin: il s'agit de visages publics connus qui sont utilisés pour amener l'utilisateur à cliquer sur des liens;

— le contact se fait surtout par e-mail mais de plus en plus aussi via des SMS et des messageries: par exemple une alerte SMS pendant la crise du COVID-19 qui prétend que le Conseil national de Sécurité a soi-disant décidé

— identiteitsfraude: zie artikel 231;

— valsheid in geschriften: zie artikel 193.

Trends (vaakst gerapporteerde feiten)

— onlinehandelsfraude (aankoop of verkoop): tijdens de COVID-19-crisis waren er bijvoorbeeld veel aanbiedingen voor maskers of ontsmettingsproducten, die na bestelling vaak echter niet aan de consument werden geleverd;

— ceo-fraude (waarbij de naam van de bedrijfsleider wordt gebruikt om bepaalde personen te benaderen);

— *malware* (of *cryptolocker*: software die alle data binnen een onderneming blokkeert);

— voorschotfraude;

— beleggingsfraude;

— emotionele fraude (tijdens de COVID-19-crisis zijn bijvoorbeeld veel mensen op valse datingsites beland; wie in die val is getrapt, werd vervolgens het slachtoffer van chantage);

— identiteitsdiefstal.

Hoe? (modus operandi)

— het slachtoffer heeft veel persoonlijke en beroepsmatige informatie verstrekt;

— LinkedIn, de grootste netwerktool in de bedrijfswereld: via enkele eenvoudige zoekopdrachten in de jaarverslagen van de ondernemingen komt men makkelijk aan de contactgegevens van de personen die bij de boekhouding of het management van een onderneming werken; vervolgens wordt een document naar hen verstuurd, dat (na opening) het systeem infecteert;

— Facebook, Instagram enzovoort worden gebruikt om de burger te benaderen via met name gesponsorde *content*: zo worden bijvoorbeeld profielen van bekende personen gebruikt voor beleggingen in bitcoin (momenteel is de RTBF het mikpunt). Bekende gezichten worden gebruikt om de gebruiker ertoe aan te zetten de links aan te klikken;

— het contact wordt vooral gelegd via e-mail, maar almaar vaker ook via sms of een chatbericht: zo werden tijdens de COVID-19-crisis sms'en uitgestuurd om te melden dat de Nationale Veiligheidsraad zogezegd had

de rembourser certaines factures. Quand on clique sur le lien on arrive sur une plateforme où il faut donner toute une série de données personnelles qui permettent après de faire tomber la personne, notamment en sollicitant les codes *Digipass*, ce qui permet aux escrocs de faire des virements à leur profit.

Tendances

— entre 2018 et 2019, on a vu une augmentation de 29 % (par ex. 11 000 dossiers pour fraudes à la carte bancaire);

— la victime est ciblée avec précision et tombe dans le piège du *phishing*;

— augmentation de 80 % durant cette période soit, 2 365 dossiers contre 1 312 en 2018;

— 40 000 signalements venant du monde bancaire et liés au *phishing* (le niveau judiciaire ne donne pas l'image parfaite de la situation);

— en 2019, 600 000 réquisitoires visant à l'identification de numéros ou d'entités;

— 200 000 concernaient plus de 10 données à identifier.

Évolution souhaitée

— obligation de conservation des données pour une période plus longue que la période actuelle de 9 mois;

— obligation qui s'applique à toute structure offrant un service numérique sur notre territoire (même si elle n'est pas localisée en Belgique);

— dans le cadre d'une enquête, accès gratuit aux données concernées (pour l'instant les renseignements à fournir sont souvent facturés à la Justice);

— pouvoir de réquisition accordé à un enquêteur ayant la qualité d'officier de police judiciaire: plus de rapidité et moins de lourdes procédures pour le magistrat (à l'heure actuelle, pour les réquisitoires, chaque fois le magistrat doit recevoir le procès-verbal, et établir le réquisitoire qui va ensuite être envoyé par l'enquêteur. En France, par exemple, le magistrat délègue à l'officier de police judiciaire les fonctions en question ainsi que l'enquêteur puisse directement contacter les opérateurs);

— il faudrait centraliser la prévention en faisant en sorte que l'on ait une seule et unique plateforme de

beslist bepaalde facturen terug te betalen. Wie vervolgens op de link klikt, belandt op een platform waar hij een hele reeks persoonsgegevens moet vermelden, maar waarmee hij achteraf in de val wordt gelokt aangezien bijvoorbeeld ook *digipass*-codes worden opgevraagd, waardoor de oplichters stortingen naar hun eigen rekening kunnen doen.

Trends

— in 2019 werd een stijging genoteerd met 29 % ten opzichte van 2018 (zo waren er 11 000 dossiers inzake bankkaartfraude);

— het slachtoffer wordt gericht geviseerd en trapt in de *phishing*-val;

— in 2019 is het aantal dossiers ter zake gestegen met 80 % (2 365 dossiers tegenover 1 312 in 2018);

— de banksector heeft melding gemaakt van 40 000 gevallen van *phishing* (het aantal rechtszaken geeft geen volledig beeld van de situatie);

— in 2019 waren er 600 000 vorderingen met betrekking tot de identificatie van nummers of van eenheden;

in 200 000 gevallen ter zake moesten meer dan 10 gegevens worden nagetrokken.

Wenselijke evolutie

— verplichting tot het langer bijhouden van de gegevens dan de huidige periode van 9 maanden;

— verplichting die geldt voor elke structuur die een digitale dienst op ons grondgebied aanbiedt (ook al is die zelf niet in België gevestigd);

— kosteloze toegang tot de betrokken data in het raam van een onderzoek (vooralsnog worden de te verstrekken gegevens vaak aan Justitie aangerekend);

— toekenning van een vorderingsbevoegdheid aan een speurder in de hoedanigheid van officier van gerechtelijke politie: snellere voortgang en minder logge procedures voor de magistraat (momenteel moet de magistraat, voor de vorderingen, telkens het proces-verbaal ontvangen en de vordering opstellen, die vervolgens door de speurder zal worden verstuurd. In Frankrijk, bijvoorbeeld, delegeert de magistraat die taken aan de officier van gerechtelijke politie en mag de speurder rechtstreeks contact nemen met de operatoren);

— centralisatie van de preventie, zodat er één enkel basisplatform is, met name *Safeonweb.be*. Aldus moet

base, notamment *Safeonweb.be*, pour que le citoyen ne doive pas faire trop de recherches pour informations et assistance: la victime d'une arnaque par exemple trouvera sur le site le lien vers le SPF Économie et le formulaire à remplir.

B. **Exposé introductif de Mme Cécile Coppin (SPF Économie)**

Mission – Vision – Compétences

L'Inspection économique a pour mission de veiller au bon fonctionnement du marché via le respect de la réglementation économique, au service des consommateurs et des entreprises. Elle met en œuvre les moyens légaux dont elle dispose pour faire cesser les pratiques commerciales illégales et les sanctionner. Ses sanctions revêtent un caractère pénal dans les cas les plus graves, à côté de ses interventions préventives à caractère pédagogique.

Ses compétences sont résumées en trois piliers:

— la protection des consommateurs;

— la concurrence entre les entreprises;

— la lutte contre la fraude économique.

L'Inspection économique a pour vision d'être:

— un maillon immanquable dans la stratégie du SPF Économie via une surveillance du marché effective, visible, orientée vers le client et organisée efficacement;

— l'élément central de la surveillance économique du fonctionnement du marché des biens et des services et de la lutte contre la fraude économique, la fraude de masse et les arnaques à la consommation, sur la base de sa connaissance du marché, en concertation avec les groupes cibles et en coopération avec les administrations nationales, régionales et internationales.

L'Inspection économique prend connaissance principalement des perturbations du marché à partir des signalements qu'elle réceptionne et traite via le Point de contact, le guichet unique géré par le SPF Économie, et dont certains accès sont accordés en fonction de leurs compétences respectives à la Police fédérale, l'AFSCA, l'AFMPS, le SIRS et le SPF Finances (*https://pointdecontact.belgique.be*).

de burger niet al te lang zoeken naar informatie en bijstand. Iemand die het slachtoffer wordt van bijvoorbeeld oplichting, zal op die website een link vinden naar de FOD Economie en naar het in te vullen formulier.

B. **Inleidende uiteenzetting van mevrouw Cécile Coppin (FOD Economie)**

Opdracht – Visie – Bevoegdheden

De Economische Inspectie is gelast toe te zien op de goede marktwerking via de inachtneming van de economische reglementering, ten behoeve van de consumenten en van de ondernemingen. Zij hanteert de wettelijke middelen waarover zij beschikt, om een einde te maken aan onwettige handelspraktijken en ze te bestraffen – in de ernstigste gevallen betreft het strafrechtelijke sancties. Daarnaast treedt de Economische Inspectie ook preventief op voor pedagogische doeleinden.

De Economische Inspectie heeft een drieledige bevoegdheid:

— de consumentenbescherming;

— de mededinging tussen de ondernemingen;

— het tegengaan van economische fraude.

De Economische Inspectie beoogt te fungeren:

— als een onmisbare schakel in de strategie van de FOD Economie, door te zorgen voor een effectief, waarneembaar, klantgericht en doeltreffend georganiseerd markttoezicht;

— als het hart van het economisch toezicht op de werking van de goederen- en dienstenmarkt en van de strijd tegen de economische fraude, de massafraude en het consumentenbedrog, op grond van haar kennis van de markt, in samenspraak met de doelgroepen en in samenwerking met de nationale, regionale en internationale instanties.

Van gevallen van verstoorde marktwerking wordt de Economische Inspectie doorgaans in kennis gesteld via meldingen die ze ontvangt en verwerkt via het Meldpunt, het door de FOD Economie beheerde éénloketsysteem. Ook andere instanties, zoals de federale politie, het FAVV, het FAGG, de SIOD en de FOD Financiën kunnen, naargelang van hun respectieve bevoegdheden, toegang krijgen tot het meldpunt (*https://meldpunt.belgie.be*).

Ces signalements peuvent être notamment relatifs à:

— l'offre en vente de produits contrefaits;

— l'exercice d'une activité commerciale de manière illégale (absence d'enregistrement à la BCE);

— des arnaques à la consommation, des suspicions de fraude économique, des pratiques commerciales trompeuses ou agressives;

— l'absence de livraison après commande et paiement par internet.

Comment cela fonctionne concrètement? Quand il n'y a qu'une seule plainte par exemple pour absence de livraison, l'Inspection ne va pas entamer une enquête mais quand 20 consommateurs signalent le même problème dans une période de deux semaines, il y a probablement une fraude derrière.

Collaboration indispensable avec les intermédiaires techniques

La réglementation actuelle est issue de la transposition de la directive sur le commerce électronique[1] dans le livre XII du Code de droit économique (CDE). La situation a évolué en 20 ans: un projet de réforme européenne est en cours (le *Digital Services Act* – la future règlementation horizontale).

Il existe un régime légal d'exonération de responsabilité sous certaines conditions, moyennant obligation d'information, pour trois catégories d'intermédiaires techniques (articles XII.17 CDE, XII.18 CDE, XII.19 CDE):

— ceux qui fournissent une activité de simple transport/ transmission (les "opérateurs" au sens de la loi du 13 juin 2005 relative aux communications électroniques (transposition en cours du Code des communications électroniques européen – IBPT);

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

— ceux qui fournissent une activité d'hébergement.

[1] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur ("directive sur le commerce électronique").

Die meldingen kunnen met name de volgende activiteiten betreffen:

— het te koop aanbieden van namaakproducten;

— het illegaal uitoefenen van een handelsbedrijvigheid (zonder registratie bij de KBO);

— consumentenbedrog, vermoedens van economische fraude, misleidende of agressieve handelspraktijken;

— het uitblijven van de levering na bestelling en betaling via het internet.

Hoe werkt zulks *in concreto*? Indien slechts één klacht wordt ingediend bijvoorbeeld vanwege het uitblijven van een levering, stelt de Inspectie geen onderzoek in, maar wanneer 20 consumenten over een periode van twee weken hetzelfde probleem melden, is wellicht sprake van fraude.

Onmisbare samenwerking met de als tussenpersoon optredende technische dienstverleners

De vigerende reglementering is het resultaat van de omzetting van de richtlijn inzake elektronische handel[1] in boek XII van het Wetboek van economisch recht (WER). Aangezien de situatie de jongste twintig jaar geëvolueerd is, loopt momenteel een Europees hervormingsproject (de *Digital Services Act*, de toekomstige horizontale regelgeving).

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 WER, XII.18 WER, XII.19 WER), met name de dienstverleners:

— van wie de activiteiten louter het doorgeven van informatie betreffen (de zogenaamde "operatoren" volgens de wet van 13 juni 2005 betreffende de elektronische communicatie (lopende omzetting van het Europees wetboek voor elektronische communicatie – BIPT);

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

— van wie de activiteiten host-diensten betreffen.

[1] Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ("richtlijn inzake elektronische handel").

Il y a une obligation légale pour les trois catégories d'informer rapidement les autorités administratives ou judiciaires compétentes dans le chef des intermédiaires techniques:

— base légale: article XII.20 CDE pour les trois catégories d'activités, article XII.19 est spécifique à l'activité d'hébergement;

— constat: cette obligation légale est peu respectée, autant pour prévenir les autorités administratives que pour prévenir les autorités judiciaires.

En vue d'une lutte efficace contre la fraude sur internet de manière générale, économique en particulier, la collaboration entre une autorité compétente et les intermédiaires techniques concernés est indispensable sur quatre niveaux:

1. porter à la connaissance des autorités compétentes les activités présumées illicites;

2. identifier les utilisateurs de leurs services afin de répondre aux demandes des autorités compétentes visant à identifier les auteurs d'infractions dissimulant leur véritable identité;

3. conserver les données afin de répondre aux demandes des autorités compétentes visant à établir la preuve des infractions commises par les utilisateurs de leur service (cf. l'arrêt de la Cour de Justice de l'Union européenne du 6 octobre 2020 dans les affaires jointes C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*; il faudra analyser en détail l'impact de l'arrêt sur les compétences des autorités de contrôle);

4. réagir rapidement aux demandes des autorités compétentes d'appliquer une procédure *notice and action* visant à la cessation des infractions commises par les utilisateurs de leurs services, formellement constatées par ces autorités compétentes et sous la responsabilité de ces autorités compétentes.

Pour l'instant l'Inspection économique a des collaborations qui fonctionnent avec les prestataires mais tout n'est pas harmonisé: on peut par exemple demander à Google de retirer des *Google Ads* illégales (mais cela prendra un certain temps).

En ce qui concerne les places de marché comme *2ememain.be* ou eBay: pour *2ememain.be* l'Inspection

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:

— wettelijke grondslag: zie artikel XII.20 WER voor de drie categorieën van activiteiten, waarbij artikel XII.19 WER alleen de host-diensten betreft;

— vaststelling: die wettelijke informatieplicht jegens de bestuurlijke en de gerechtelijke autoriteiten wordt amper in acht genomen.

Met het oog op de doeltreffende bestrijding van de internetfraude in het algemeen en van de economische fraude in het bijzonder, is het onontbeerlijk dat een bevoegde autoriteit en de als tussenpersoon optredende technische dienstverleners samenwerken als volgt:

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

2. 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;

3. 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 (cf. het arrest van het Hof van Justitie van de Europese Unie van 6 oktober 2020 in de zaken C-511/18, C-512/18 en C-520/18, *La Quadrature du Net e.a.*; de impact van dit arrest op de bevoegdheden van de toezichthoudende autoriteiten zal grondig moeten worden onderzocht);

4. 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 die door die bevoegde autoriteiten formeel werden vastgesteld en die onder de verantwoordelijkheid van die bevoegde autoriteiten ressorteren.

Momenteel werkt de Economische Inspectie weliswaar reeds samen met die dienstverleners, maar niet alles is op elkaar afgestemd: Google kan bijvoorbeeld worden verzocht illegale *Google Ads* te verwijderen, maar dat zal enige tijd in beslag nemen.

Met betrekking tot de marktplaatsen zoals *2dehands.be* of eBay geeft de spreekster aan dat de Economische

économique détient un compte *superuser,* ce qui implique que l'Inspection peut déjà temporairement supprimer une annonce par exemple pour un produit contrefait.

Pour Facebook il a aussi une procédure pour retirer des contenus illégaux.

L'oratrice conclut qu'il n'y a que des procédures volontaires; il n'y a pas une seule procédure uniforme et les délais de réponse ne sont pas identiques. Madame Coppin espère qu'il y aura plus d'harmonisation à l'avenir.

Dans certains cas, l'enquête ne permet pas d'identifier l'auteur de l'infraction (anonymisation du téléphone, du paiement électronique, du surf, de l'enregistrement du nom de domaine, hébergement auprès d'une société établie dans un pays exotique…), ou de prouver l'infraction si les historiques de communication n'ont pas été conservées ou si les publicités trompeuses ou agressives à l'origine de la fraude économique sont personnalisées. L'Inspection économique ne peut enquêter efficacement, ne peut par exemple pas entendre le contrevenant en ses moyens de défense, en raison de son propre comportement, qui constitue déjà en lui-même l'infraction initiale de ne pas s'identifier en tant que prestataire économique (obligation légale d'identification).

Malgré l'obligation légale générale de collaborer sous peine de sanction pénale pour entrave à l'exécution de la mission de l'Inspection économique, certaines dispositions sectorielles, ne relevant pas de la compétence du SPF Économie, sont susceptibles de créer une confusion et une insécurité juridique pour les consommateurs victimes de fraude et les opérateurs télécom.

Concrètement, l'Inspection économique effectue des demandes de collaboration motivées, comprenant la base légale de ses pouvoirs et la disposition légale enfreinte, dans le respect du principe de proportionnalité et des droits fondamentaux, adressée aux:

— entreprises exerçant une activité d'hébergement;

— entreprises exerçant une activité de gestion de noms de domaine (collaboration avec DNS pour rendre des sites avec un suffixe ".be" inaccessibles quand ils sont illégaux);

— plateformes électroniques (places de marché, moteurs de recherche, magasins d'applications, plateformes de voyages et d'hébergement en ligne, plateformes de

Inspectie op *2dehands.be* een *superuser*-account heeft, waardoor ze een advertentie (bijvoorbeeld voor een namaakproduct) reeds tijdelijk kan verwijderen.

Aangaande Facebook is er ook een procedure om illegale content te verwijderen.

De spreekster geeft tot slot aan dat er alleen vrijwillige procedures zijn; er is geen eenvormige procedure en de responstijden verschillen. Mevrouw Coppin hoopt dat er ooit meer afstemming komt.

In sommige gevallen blijkt uit het onderzoek niet wie het misdrijf pleegde (anonimisering van de telefoon, van de elektronische betaling, van het surfgedrag, van de domeinnaamregistratie, hosting bij een maatschappij in een exotisch land, enzovoort), of kan het misdrijf niet worden bewezen wanneer de communicatiegeschiedenis niet werd bijgehouden, dan wel wanneer de aan de oorsprong van de economische fraude liggende misleidende of agressieve reclameboodschappen op het slachtoffer werden toegesneden. De Economische Inspectie kan geen doeltreffend onderzoek voeren, want ze kan bijvoorbeeld de overtreder niet horen over diens verdedigingsmiddelen, aangezien die zich niet als verlener van een economische dienst profileert; dergelijk gedrag vormt overigens op zich al een overtreding (namelijk van de wettelijke identificatieplicht).

Ondanks de wettelijke verplichting om mee te werken (op straffe van een strafrechtelijke sanctie wegens belemmering van de uitvoering van de opdracht van de Economische Inspectie), kunnen sommige sectorale bepalingen die niet onder de bevoegdheid van de FOD Economie vallen, leiden tot verwarring en rechtsonzekerheid bij de door fraude getroffen consumenten en voor de telecomoperatoren.

Concreet verzoekt de Economische Inspectie de volgende bedrijven en instanties om samenwerking, met vermelding van de wettelijke grondslag van haar bevoegdheden en van de overtreden wettelijke bepaling, alsook met inachtneming van het evenredigheidsbeginsel en van de grondrechten:

— ondernemingen met hostingactiviteiten;

— ondernemingen die domeinnamen beheren (samenwerking met DNS om illegale sites met een ".be"-suffix ontoegankelijk te maken);

— elektronische platformen (marktplatformen, zoekmachines, app-winkels, onlinereis- en logiesplatformen, mobiliteitsplatformen, deeleconomieplatformen,

mobilité, plateformes d'économie collaborative, comparateurs, …): on attend une définition plus claire du *Digital Services Act*;

— opérateurs télécom, fournisseurs d'accès à internet;

— établissements financiers: banques, prestataires de paiement en ligne, …

Avant de solliciter la collaboration d'un acteur du secteur privé dans le cadre de l'application de ses conditions contractuelles en cas de constatation d'un non-respect de la réglementation, l'Inspection économique:

— tient compte de la gravité de l'infraction et ne va pas au-delà de ce qui est nécessaire pour atteindre ses objectifs;

— envisage toutes les mesures possibles et vérifie si d'autres mesures pourraient également atteindre les objectifs de manière plus efficace et/ou moins onéreuse et/ou moins attentatoire aux droits fondamentaux et/ou à l'égard d'autres intermédiaires ayant des moyens d'action plus adaptés;

— n'envisage pas une mesure qui aurait pour effet de bloquer également du contenu licite;

— n'envisage pas une mesure qui entraînerait des coûts disproportionnellement élevés pour l'intermédiaire à qui la demande est adressée;

— n'envisage pas une mesure qui aurait pour effet d'imposer une obligation générale de surveillance de l'information que les prestataires intermédiaires transmettent ou stockent, ni une obligation de rechercher activement des faits ou des circonstances qui font présumer l'existence d'activités illicites.

Évolution – enjeux – défis

1. Mettre en place concrètement la révision des compétences d'enquête contenues dans le projet de loi votée le 24 septembre 2020 par la Chambre (projet de loi modifiant le Code de droit économique et d'autres lois en vue de renforcer les compétences de recherche et d'application conformément au règlement (UE) 2017/2394 du Parlement européen et du Conseil du 12 décembre 2017 sur la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs

vergelijkingsdiensten enzovoort); ter zake wordt gewacht op een duidelijker omschrijving van de *Digital Services Act*;

— telecomoperatoren, internetproviders;

— financiële instellingen: banken, dienstverleners voor onlinebetalingen enzovoort.

Wanneer wordt vastgesteld dat een speler uit de privésector de reglementering niet heeft nageleefd bij de implementering van zijn contractuele voorwaarden en hij wordt verzocht zijn medewerking te verlenen, maakt de Economische Inspectie eerst de volgende afwegingen:

— er wordt rekening gehouden met de ernst van de overtreding; de Inspectie gaat niet verder dan wat nodig is om haar doelen te bereiken;

— alle mogelijke maatregelen worden overwogen; tevens wordt nagegaan of de doelstellingen ook zouden kunnen worden bereikt via andere maatregelen die doeltreffender of goedkoper zouden zijn, die de grondrechten minder zouden aantasten, die andere tussenpersonen met beter aangepaste actiemiddelen zouden betreffen, of waarbij sprake zou zijn van een combinatie van die elementen;

— een maatregel komt niet in aanmerking wanneer als gevolg ervan ook rechtmatige content zou worden geblokkeerd;

— een maatregel komt niet in aanmerking wanneer hij onevenredig hoge kosten met zich zou brengen voor de tussenpersoon aan wie het verzoek wordt gericht;

— een maatregel komt niet in aanmerking wanneer hij zou leiden tot een algemene verplichting tot toezicht op de door de dienstverlenende tussenpersonen overgedragen of opgeslagen informatie, dan wel tot de verplichting feiten of omstandigheden actief op te sporen die het bestaan van onwettige activiteiten doen vermoeden.

Evolutie – inzet – uitdagingen

1. De concrete tenuitvoerlegging van de onderzoeksbevoegdheden die werden herzien bij het op 24 september 2020 door de Kamer aangenomen wetsontwerp (Wetsontwerp tot wijziging van het Wetboek van economisch recht en van andere wetten met het oog op het versterken van de opsporings- en handhavingsbevoegdheden in overeenstemming met en in uitvoering van Verordening (EU) 2017/2394 van het Europees Parlement en de Raad van 12 december 2017 betreffende samenwerking tussen de nationale autoriteiten die verantwoordelijk zijn

et abrogeant le règlement (CE) nº 2006/2004 et en exécution de celui-ci (I), DOC 55 1385/001-008):

— suivi des flux financiers et des flux de données télécom: analyse de la cohérence entre les pouvoirs accrus d'enquête dans la mise en œuvre du règlement européen CPC[2], la réglementation de la loi du 13 juin 2005 relative aux communications électroniques en cours de révision et l'arrêt précité de la CJUE du 6 octobre 2020 qui risque de les restreindre;

— possibilité de faire des achats-tests en utilisant une identité fictive ("*mystery shopping*");

— possibilité de prendre des mesures provisoires afin d'éviter un préjudice aux consommateurs: rendre inaccessibles des sites web et procéder à la publication de listes d'entreprises ne respectant pas la législation ("listes grises");

— obtenir ou accepter de la part d'entreprises des engagements tendant à mettre fin à une infraction, et de les publier;

— révision du régime de sanction du droit de la consommation avec une possibilité complémentaire d'infliger des amendes administratives (à côté des procès-verbaux que l'Inspection fait pour le ministère public).

2. Suivre les futurs débats européens concernant le *Digital Services Act (*qui sera probablement finalisé en décembre 2020, sous forme d'un règlement), afin d'apporter une contribution riche en expertise de terrain et en connaissance du marché, à la réforme de l'économie numérique européenne qui devrait être dévoilée en décembre 2020 par la Commission européenne.

3. Analyser, avec l'IBPT et les autres autorités en charge de la lutte contre la fraude, l'impact du secret des communications, du futur Code des communications électroniques européen et de la jurisprudence européenne en matière de *data retention,* sur les faisabilités d'enquête.

[2] Règlement (UE) 2017/2394 du Parlement européen et du Conseil du 12 décembre 2017 sur la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs et abrogeant le règlement (CE) nº 2006/2004.

voor handhaving van de wetgeving inzake consumentenbescherming en tot intrekking van Verordening (EG) nr. 2006/2004 (I) – DOC 55 1385/001-008):

— volgen van de financiële stromen en van de telecomgegevensstromen: ontleding van de samenhang tussen de grotere onderzoeksbevoegdheden inzake de toepassing van de CPC-verordening[2], de reglementering vervat in de momenteel in herziening zijnde wet van 13 juni 2005 betreffende de elektronische communicatie, en het voormelde arrest van het Hof van Justitie van de Europese Unie *de dato* 6 oktober 2020, dat een en ander dreigt te beperken;

— de mogelijkheid om met een fictieve identiteit testaankopen te verrichten ("*mystery shopping*");

— de mogelijkheid om voorlopige maatregelen te nemen, teneinde schade voor consumenten te voorkomen: websites ontoegankelijk maken en overgaan tot de bekendmaking van lijsten met bedrijven die de wetgeving niet in acht nemen ("grijze lijsten");

— verkrijgen of aanvaarden dat in overtreding zijnde ondernemingen zich ertoe verbinden zich voortaan te zullen schikken naar de reglementering, en die verbintenissen bekendmaken;

— de sanctieregeling binnen het consumentenrecht herzien, met een bijkomende mogelijkheid om administratieve geldboetes op te leggen (naast de processenverbaal die de Economische Inspectie ter attentie van het openbaar ministerie opstelt).

2. Volgen van de toekomstige Europese debatten inzake de *Digital Services Act* (die wellicht in december 2020 klaar zal zijn en in een verordening zal worden gegoten), teneinde een grotendeels op ervaring in het veld en op marktkennis gestoelde bijdrage te leveren tot de hervorming van de Europese digitale economie; die zou in december 2020 door de Europese Commissie moeten worden bekendgemaakt.

3. In samenwerking met het BIPT en met de fraudebestrijdingsoverheden nagaan in welke mate het communicatiegeheim, de toekomstige Europese elektronischecommunicatiecode en de Europese rechtspraak inzake *data retention* invloed hebben op de haalbaarheid van de onderzoeken.

[2] Verordening (EU) 2017/2394 van het Europees Parlement en de Raad van 12 december 2017 betreffende samenwerking tussen de nationale autoriteiten die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming en tot intrekking van Verordening (EG) nr. 2006/2004.

C. **Exposé introductif de Mme Phédra Clouner (CCB)**

Le CCB est l'agence nationale pour la cybersécurité qui dépend directement du premier ministre. Le CCB dispose depuis le 1er janvier 2017 d'un service opérationnel, CERT.be, qui intervient en cas de cyberaccident.

Une des missions principales du CCB est de contribuer à la construction d'un internet plus sûr et plus sécurisé pour le citoyen et le consommateur. Il y a deux articles dans l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique (*Moniteur belge* du 21 novembre 2014) qui sont intéressants pour le sujet de cette audition:

— assurer la coordination entre les services et autorités concernées mais aussi entre autorités publiques et le secteur privé et le monde scientifique;

— informer et sensibiliser les utilisateurs des systèmes d'information et de communication, c'est-à-dire les citoyens et les consommateurs.

La menace

L'oratrice expose ensuite la menace telle qu'envisagée par le CCB (l'Inspection économique et la police fédérale pourraient avoir une vision différente): le CCB identifie les problèmes liés à la cybersécurité, c'est-à-dire les problèmes qui touchent à la confidentialité, l'intégrité et la disponibilité des systèmes. Les conséquences de ces systèmes peuvent évidemment être de la fraude ou de l'escroquerie car la motivation principale des cybercriminels reste encore et toujours l'argent.

Notifications au CERT.be

En 2019 il y avait 4 484 notifications au CERT.be. Ce chiffre n'est pas exhaustif (tout le monde ne notifie pas le CCB quand il est victime d'un cybercriminel). Il s'agit notamment de:

— tentative de fraude;

— *phishing*;

— fraude au CEO;

— Microsoft *scam*;

— etc.

C. **Inleidende uiteenzetting van mevrouw Phédra Clouner (CCB)**

Het CCB is de nationale autoriteit voor cyberveiligheid; ze staat onder het gezag van de eerste minister. Sinds 1 januari 2017 beschikt het CCB over een operationele dienst, "CERT.be", die optreedt bij cyberincidenten.

Eén van de belangrijkste opdrachten van het CCB bestaat erin bij te dragen tot de uitbouw van een veiliger en beter beveiligd internet voor de burger en voor de consument. De opdrachtomschrijving van het CCB (vervat in artikel 3 van het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België – *Belgisch Staatsblad* van 21 november 2014) bevat twee taken die interessant zijn met betrekking tot het thema van deze hoorzitting, namelijk:

— "de coördinatie verzekeren tussen de betrokken diensten en overheden, en de publieke overheden en de private of wetenschappelijke sector";

— "informeren en sensibiliseren van gebruikers van informatie- en communicatiesystemen", dus van de burgers en van de consumenten.

De dreiging

Vervolgens belicht de spreekster de visie van het CCB op de "dreiging" (die niet noodzakelijk strookt met die van de Economische Inspectie en van de federale politie): het CCB houdt zich bezig met de problemen inzake cyberveiligheid, met name de pijnpunten in verband met vertrouwelijkheid, integriteit en de beschikbaarheid van de systemen. Die systemen zijn uiteraard vatbaar voor fraude of oplichting, want geld blijft nog altijd de belangrijkste drijfveer van de cybercriminelen.

Meldingen bij CERT.be

In 2019 ontving CERT.be 4 484 meldingen. Dat cijfer is niet exhaustief (niet iedereen stelt het CCB in kennis wanneer hij of zij het slachtoffer wordt van een cybercrimineel). Deze meldingen betroffen met name:

— poging tot fraude;

— *phishing*;

— ceo-fraude;

— Microsoft-*scam;*

— enzovoort.

Fraude et escroquerie économique et financière

— souvent basée sur le social engineering (c'est-à-dire qu'il s'agit plutôt d'un problème d'ordre humain en ne pas d'ordre technique);

— *phishing* et ses conséquences est à l'origine de 80 % des cyberincidents;

— les cybercriminels tentent d'accéder aux données, ou à l'appareil;

— l'accès est souvent donné par l'utilisateur;

— envoi d'un message contenant un lien ou une pièce jointe avec des offres alléchantes;

— l'utilisateur clique et introduit ses données: de cette façon, on va soutirer des informations bancaires, ou des log in et des mots de passe; grâce au *phishing* les cybercriminels ont accès aux comptes bancaires et autres des utilisateurs. Le *phishing* est aussi le vecteur pour la diffusion de malware sur tous types d'appareils, qui a pour conséquence par ex. des vols d'identifiants bancaires ou du *keylogging* (pour intercepter les log in et les mots de passe des utilisateurs);

— le *phishing* s'effectue via des mails mais de plus en plus aussi via SMS, messages WhatsApp etc.;

— attaques web-based (des sites officiels contrefaits, par exemple d'une banque);

— escroquerie nigériane;

— *scam* (par ex. les Microsoft *scams*: une personne est contactée par un opérateur de Microsoft qui demande accès à sa machine parce qu'elle aurait un problème qu'il va lui aider à résoudre);

— spam;

— *ransomware* (souvent diffusés par *phishing*);

— hacking des comptes, souvent dû au fait que le consommateur utilise des mots de passe faibles; ensuite, le compte est utilisé pour envoyer des spams, *phishing*, usurpation d'identité, etc. Comme cela le consommateur devient un acteur involontaire de la fraude;

— fraude au CEO (qui est une forme de *phishing*).

Economische en financiële fraude en oplichting

— deze berust vaak op *social engineering* (dat wil zeggen dat niet de techniek, maar veeleer de mens het probleem is);

— *phishing* en de gevolgen daarvan liggen ten grondslag aan 80 % van de cyberincidenten;

— de cybercriminelen proberen toegang te krijgen tot de gegevens of tot het toestel;

— de toegang wordt vaak door de gebruiker zelf verleend;

— er wordt een bericht verzonden dat een link of een bijlage met verleidelijke aanbiedingen bevat;

— de gebruiker klikt aan en vult zijn gegevens in: zo worden bankgegevens, logins en wachtwoorden opgehaald; dankzij *phishing* krijgen de cybercriminelen toegang tot de bank- en andere rekeningen van de gebruikers. Via *phishing* wordt tevens *malware* op alle soorten van toestellen verspreid, met als gevolg dat bankidentificatiegegevens worden gestolen of sprake is van *keylogging* (om de gebruikerslogins en de wachtwoorden van de gebruikers te onderscheppen);

— *phishing* gebeurt via e-mails, maar almaar vaker ook via sms, WhatsApp-berichten enzovoort;

— er worden *web-based*-aanvallen uitgevoerd (via vervalste officiële websites, bijvoorbeeld die van een bank);

— er zijn Nigeriaanse oplichters actief;

— er is sprake van *scams* (bijvoorbeeld de Microsoft-*scams*: een "Microsoft-operator" neemt contact op en vraagt toegang tot het toestel van de betrokkene omdat daarmee iets aan de hand zou zijn dat de "operator" zal helpen oplossen);

— er wordt spam verstuurd;

— er wordt *ransomware* verspreid (vaak via *phishing*);

— accounts worden gehackt, vaak omdat de consument zwakke wachtwoorden gebruikt; vervolgens wordt het account gebruikt om spam of *phishing* te versturen, identiteitsdiefstal te plegen enzovoort. Op die manier wordt de consument ongewild bij fraude betrokken;

— er wordt ceo-fraude (een vorm van *phishing*) gepleegd.

Toutes ces fraudes touchent tant les consommateurs que les organisations publiques et privées.

Actions du CCB et collaborations

Les publiques cibles du CCB sont les citoyens, les organisations, les institutions gouvernementales et les secteurs vitaux. Ici on se limite aux actions qui ciblent les citoyens et les consommateurs.

Belgian Cybersecurity Governance

Le CCB a déjà aujourd'hui des collaborations qui sont mises en place avec des acteurs technologiques, via la *Cyber Security Coalition*, mais aussi des collaborations concrètes avec des ISP (*internet service providers).*

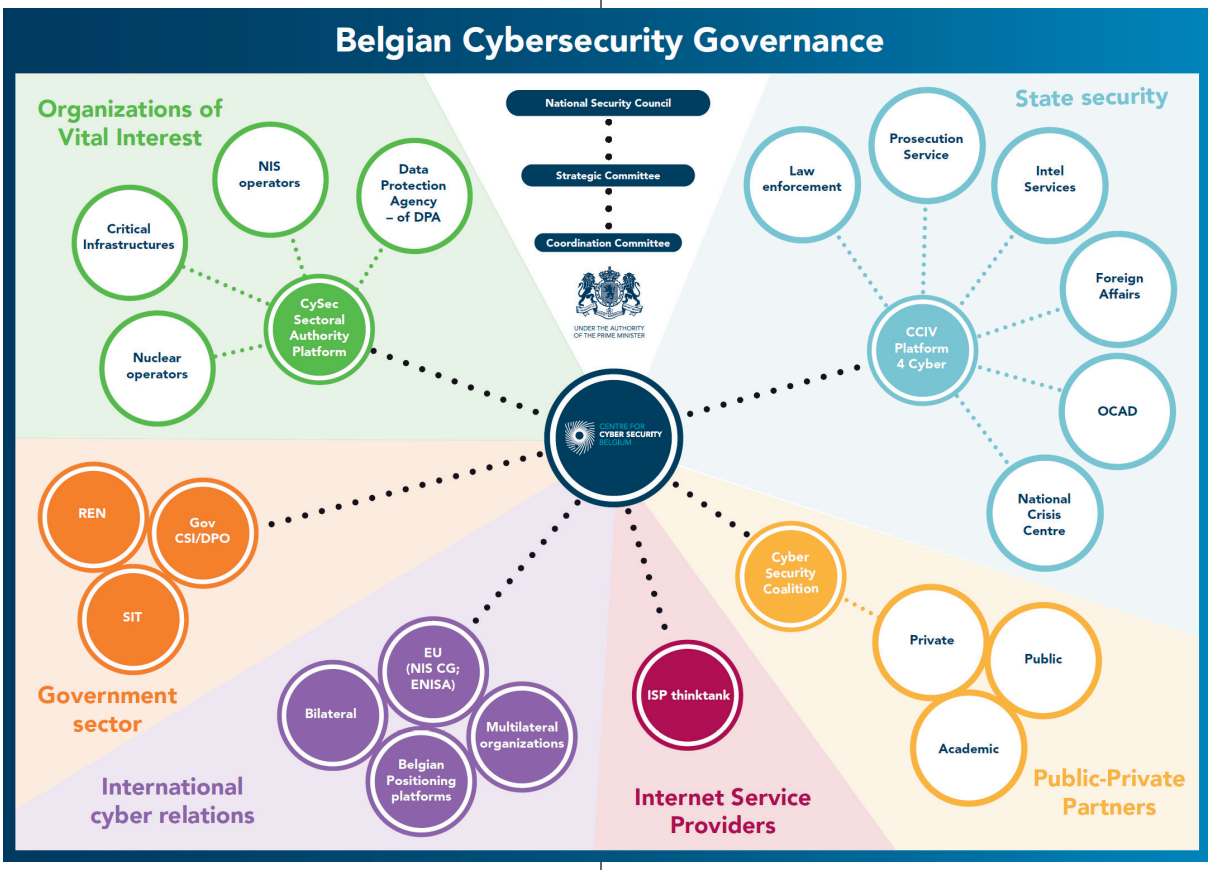
Al deze vormen van fraude treffen zowel consumenten als publieke en private organisaties.

Acties van het CCB en samenwerkingsverbanden

De doelgroepen van het CCB zijn de burgers, de organisaties, de overheidsinstellingen en de vitale sectoren. In dit verband beperkt de spreekster zich tot de acties die gericht zijn op de burgers en op de consumenten.

Belgian Cybersecurity Governance

Thans beschikt het CCB al over samenwerkingsverbanden die via de *Cyber Security Coalition* met technologische actoren worden opgezet. Tevens zijn er concrete samenwerkingsverbanden met de *internet service providers* (ISP's).



Actions

BePhish est l'un des grands projets du CCB:

— les citoyens sont invités à envoyer leurs mails suspects sur une adresse mail dédiée (*suspect@safeonweb.be, verdacht@safonweb.be*), qui fait l'objet des campagnes de sensibilisation;

Acties

BePhish is een van de grote projecten van het CCB:

— de burgers worden ertoe opgeroepen de ontvangen verdachte e-mails naar een daarvoor bestemd e-mailadres te sturen (*suspect@safeonweb.be, verdacht@safonweb.be*); daartoe worden bewustmakingscampagnes gevoerd;

— les URL et les pièces jointes sont extraites des mails et analysées automatiquement;

— si elles sont analysées comme étant frauduleuses, elles sont envoyées vers Google et Microsoft et bloquées au niveau du browser;

— en 2020 il y a jusqu'à présent 2 238 172 mails suspects reçus et 422 854 URL envoyées vers Microsoft et Google pour blocage.

Le CCB a à ce sujet une collaboration avec Google et Microsoft, qui est toujours basée sur la bonne volonté.

La sensibilisation est fondamentale car la fraude et l'escroquerie ne sont pas que des problèmes techniques (souvent basés sur le *social engineering*); par conséquent, la sensibilisation et l'information sont les clés.

Le CCB mène de grandes campagnes annuelles de sensibilisation en collaboration avec la *Cyber Security Coalition*:

— *phishing* (2017 et 2019) *suspect@safeonweb.be*;

— bons réflexes (2018): back up/ antivirus/ mises à jour/ mots de passe forts;

— authentification 2 facteurs (2020).

À travers la *Cyber Security Coalition*, il y a une collaboration effective avec des entreprises technologiques, dans le cadre de diverses actions, dont les campagnes annuelles de sensibilisation. Le CCB est également partenaire de *CyberSimple*, une action menée conjointement par Google et Test-Achats, avec notamment des conseils pour reconnaître des *web shops* qui sont fiables ou pas.

Par ailleurs, le CCB participe au projet *Nomoreransom.org*.

Spear Warning constitue une autre action du CCB. C'est un système qui harmonise certaines informations et permet d'envoyer des notifications à certains types d'organisations. Il s'agit d'une alerte ciblée en fonction des menaces qui sont identifiées. Ces notifications concernent les appareils qui sont infectés ou vulnérables et qui peuvent donc être utilisés pour lancer des campagnes de *phishing*:

— *BE-GUARD* (en cours de finalisation): app pour les PME et les *technical home users* pour recevoir des

— de URL's en de bijlagen worden automatisch uit de mails gehaald en geanalyseerd;

— indien wordt vastgesteld dat ze frauduleus zijn, worden ze doorgestuurd naar Google en Microsoft en worden ze door de browser geblokkeerd;

— in 2020 werden tot dusver 2 238 172 verdachte mails ontvangen en werden 422 854 URL's doorgestuurd naar Microsoft en Google om te worden geblokkeerd.

Het CCB werkt daartoe samen met Google en Microsoft. Dat gebeurt nog steeds op basis van welwillendheid.

Bewustmaking is van fundamenteel belang omdat fraude en oplichting niet louter technische problemen zijn (want veelal gebaseerd op *social engineering*); daarom zijn bewustmaking en voorlichting de sleutel tot succes.

Het CCB voert elk jaar grootschalige bewustmakingscampagnes in samenwerking met de *Cyber Security Coalition*:

— *phishing* (2017 en 2019) *mailto: suspect@safeonweb.be*;

— de juiste reflexen (2018): back-up/antivirus/updates/ sterke paswoorden;

— 2-factor-authenticatie (2020).

Via de *Cyber Security Coalition* bestaat er een effectieve samenwerking met technologiebedrijven, waarbij verschillende acties, waaronder de jaarlijkse bewustmakingscampagnes, worden gevoerd. Het CCB is bovendien partner van *CyberSimple*, een actie die gezamenlijk wordt geleid door Google en Test Aankoop waarbij tips worden gegeven om na te gaan of een webshop al dan niet betrouwbaar is.

Voorts neemt het CCB deel aan het project *Nomoreransom.org*.

Een andere actie van het CCB is *Spear Warning*, een systeem dat bepaalde informatie samenbrengt en de mogelijkheid biedt meldingen te versturen naar bepaalde soorten organisaties. Het betreft een gerichte waarschuwing naargelang van de vastgestelde bedreigingen. Die meldingen hebben betrekking op geïnfecteerde of kwetsbare toestellen waarvan misbruik zou kunnen worden gemaakt voor *phishing*campagnes:

— *BeGuard* (in de afwerkingsfase): een app voor kmo's en *technical home users* die informatie geeft over

informations au sujets des adresses IP infectées et des alertes générales.

— ERADICATION: éradication des *botnets* et des vulnérabilités. On alerte les clients des ISP via les ISP lorsque des appareils sont vulnérables ou infectés (via IP).

— ISP *Think Thank*: des réunions tous les deux mois avec les quatre plus grands ISP de Belgique (Proximus, Telenet, Orange and Voo) plus Belnet plus le CCB pour discuter de la coopération dans différents projets et les tendances en matière de cybersécurité, avec pour objectif de protéger les citoyens, les consommateurs et les organisations.

Concepts (en cours de développement)

— *Trusted Sender*: permettra d'avoir la certitude sur l'identité de celui qui envoie un message (ce n'est pas toujours le cas, cf. *phishing*, fraude au CEO, etc.);

— *Trusted Publisher*: permettra d'être certain de l'identité de celui qui est l'éditeur/responsable/propriétaire d'un site web (ce n'est pas toujours le cas, cf. fraude et escroquerie, *phishing*, attaques *web-based*, etc.). Un certificat n'est pas toujours la preuve que le site est fiable et que l'éditeur du site est bien celui qu'il affirme être (certificats faible niveau, une simple adresse suffit parfois à avoir un certificat, auto-déclaration, certificats gratuits sur internet). Une identité digitale sûre veut dire moins de fraude.

Conclusion

Le CCB a des collaborations avec des acteurs technologiques qui ne marchent pas mal mais qui sont basées sur la bonne volonté des acteurs (des ISP, Google, Microsoft, etc.). Pour l'instant il n'y a rien de structurel ni de formel dans ces collaborations et du moment que cela coûtera trop aux ISP de mettre en œuvre certaines mesures, on ne peut pas garantir que cette collaboration continuera de manière efficace.

D. **Exposé introductif de M. Robrecht De Keersmaecker (substitut du procureur général d'Anvers, coordinateur principal du réseau d'expertise Cybercrime)**

M. Robrecht De Keersmaecker (parquet général d'Anvers) explique que le ministère public considère comme une fraude à caractère économico-financier sur le web toute forme de manipulation illicite utilisant le web et visant à détourner des données ou des actifs

geïnfecteerde IP-adressen en algemene waarschuwingen uitstuurt.

— ERADICATION: verwijdert *botnets* en pakt kwetsbaarheden aan. De *internet software provider* (ISP) waarschuwt de ISP-clients wanneer hun toestellen kwetsbaar of geïnfecteerd zijn (via IP).

— ISP-denktank: tweemaandelijkse vergaderingen met de vier grootste ISP's van België (Proximus, Telenet, Orange en Voo), Belnet en het CCB om de samenwerking bij verschillende projecten en de tendensen inzake cyberveiligheid te bespreken met het oog op de bescherming van de burgers, de consumenten en de organisaties.

Concepten (in de ontwikkelingsfase)

— *Trusted Sender:* om zekerheid te bieden over de identiteit van de verzender van een bericht (wat elders niet altijd het geval is, cf. *phishing*, ceo-fraude enzovoort);

— *Trusted Publisher:* om zekerheid te bieden over de identiteit van de editor/verantwoordelijke/eigenaar van een website (wat elders niet altijd het geval is, cf. fraude en oplichting*, phishing*, *web-based* aanvallen enzovoort). Een certificaat is niet altijd een bewijs dat een website betrouwbaar is en dat de editor van de website wel degelijk is wie hij beweert te zijn (de certificaten zijn van een lage betrouwbaarheid, een gewoon adres volstaat soms om een certificaat te verkrijgen, editors leveren een certificaat af aan zichzelf of men verkrijgt het certificaat gratis op het internet). Een veilige identiteit leidt tot minder fraude.

Besluit

Het CCB werkt samen met technologische actoren. Die samenwerking verloopt naar behoren, maar berust op de welwillendheid van de actoren (ISP's, Google, Microsoft enzovoort). Die samenwerkingsverbanden zijn thans geenszins structureel noch formeel; zodra de tenuitvoerlegging van bepaalde maatregelen voor de ISP's te duur wordt, kan niet worden gewaarborgd dat die samenwerking efficiënt zal blijven verlopen.

D. **Inleidende uiteenzetting van de heer Robrecht De Keersmaecker (substituut-procureur-generaal te Antwerpen, hoofdcoördinator Expertisenetwerk Cybercrime)**

De heer Robrecht De Keersmaecker (parket-generaal te Antwerpen) legt uit dat het openbaar ministerie "financieel-economische internetfraude" opvat als elke vorm van ongeoorloofde manipulatie middels het internet waarbij gegevens of activa afhandig worden gemaakt

dans l'intention frauduleuse d'en retirer un avantage économique illicite pour soi ou pour le compte d'un tiers. Dans la majorité des cas de fraude sur le web, l'auteur s'efforce de soutirer de l'argent à sa victime, ou des données qu'il tente ultérieurement d'exploiter pour obtenir également de l'argent.

Parmi les nombreux exemples de fraude sur le web, on peut citer à titre non exhaustif:

1. le *phishing* ou hameçonnage: technique utilisée pour dérober des mots de passe et des identifiants et vider ensuite les comptes bancaires ou prendre frauduleusement le contrôle d'un système informatique par exemple;

2. les *ransomware* ou rançongiciels: logiciels malveillants qui bloquent des systèmes et les données qui y sont stockées à l'aide d'une clé et exigent le paiement d'une rançon en échange de cette clé;

3. la fraude aux achats: commande de produits, souvent onéreux, sans intention de les payer dans le seul but d'extorquer des informations financières;

4. la fraude aux valeurs virtuelles: incite les victimes à faire des placements apparemment très lucratifs, par exemple dans des bitcoins, ou à entrer dans des levées de fonds initiales (*initial coin offerings*) qui s'avèrent ensuite inexistantes, ou les fonds sont détournés par les exploitants de la plateforme (escroquerie de sortie ou *exit scam*);

5. la fraude relationnelle: envoi à la victime d'une demande d'aide financière en ligne pour aider un partenaire ou un ami – qui n'existe pas vraiment – dans un pays lointain;

6. la fraude nigériane: fait miroiter un gain très important – mais fictif – qui ne peut être remis que contre le paiement de frais administratifs;

7. la fraude au helpdesk: des escrocs se font passer pour de soi-disant représentants de Microsoft, par exemple, pour prendre frauduleusement le contrôle à distance du système de leur victime.

Les problèmes que pose la fraude sur le web sont connus.

Les fraudeurs ont recours à de nouvelles technologies afin de faire, en un temps record, un maximum de victimes avec un minimum d'efforts. Les auteurs

van slachtoffers, met het bedrieglijk oogmerk enig onrechtmatig economisch voordeel voor zichzelf of een ander te verwerven. In het gros van de gevallen van internetfraude is de dader erop uit gelden afhandig te maken van het slachtoffer, dan wel gegevens, die men dan later poogt te kunnen gebruiken om alsnog gelden te kunnen verwerven.

Enkele voorbeelden, niet limitatief, van dergelijke internetfraude zijn:

1. *phishing*, waarbij paswoorden en logingegevens afhandig gemaakt worden, om die vervolgens bijvoorbeeld te misbruiken om de bankrekeningen leeg te maken of om onrechtmatig toegang te krijgen tot een informaticasysteem;

2. *ransomware* of gijzelsoftware, waarbij systemen en de daarop opgeslagen gegevens worden versleuteld middels malware of *phishing* en er een losgeld moet worden betaald om deze sleutel al dan niet te verkrijgen;

3. aankoopfraude, waarbij vaak dure goederen worden besteld zonder de intentie te hebben deze ooit te betalen of waarbij men enkel poogt financiële informatie te ontfutselen;

4. virtuele-waardenfraude, waarbij men ogenschijnlijk zeer lucratieve beleggingen doet in bijvoorbeeld bitcoins of instapt in *initial coin offerings*, doch waarbij deze achteraf onbestaand blijken of waarbij de uitbaters van het platform met de gedeponeerde waarden verdwijnen (*exit scam);*

5. relatiefraude, waarbij men financiële hulp overmaakt om een online – doch in werkelijkheid niet-bestaande – partner of vriend in een ver land uit de nood te helpen;

6. Nigeriaanse fraude, waarbij men een zeer riante – maar fictieve – winst wordt voorgespiegeld, die echter enkel overgemaakt kan worden na betaling van administratieve kosten;

7. helpdeskfraude, waarbij slachtoffers worden opgebeld door ogenschijnlijke vertegenwoordigers van bijvoorbeeld Microsoft om zo vanop afstand onrechtmatig toegang tot hun systeem te verkrijgen.

De problemen met internetfraude zijn gekend.

Daders gebruiken de nieuwe technologieën om op zeer korte tijd een massa aan slachtoffers te bereiken met een minimale moeite. De daders hoeven zelfs niet

eux-mêmes ne doivent pas être des spécialistes en informatique. En effet, il existe un marché florissant de matériel et de logiciels prêts à l'emploi pour faciliter la fraude sur le web (*cybercrime as a service).* Ce type de fraude connaît dès lors une croissance exponentielle.

En outre, les auteurs peuvent se jouer des frontières nationales sans la moindre entrave, et peuvent, en un clic, transférer leur patrimoine vers des destinations lointaines après l'avoir transformé à de multiples reprises, ce qui complique considérablement l'enquête pénale dès lors que les services répressifs restent attachés à une conception dépassée de la juridiction territoriale. En tout état de cause, les décisions d'enquête européennes ou les commissions rogatoires internationales ralentissent l'enquête, pour autant qu'une collaboration existe.

Les services répressifs ne pourront jamais venir à bout de ce tsunami avec les moyens dont ils disposent. La prévention est donc primordiale. Celle-ci doit d'abord consister à sensibiliser durablement les victimes potentielles au fait que lorsqu'une offre paraît trop belle pour être vraie, elle est généralement mensongère.

Ensuite, il convient de miser, autant que faire se peut, sur la cybersécurité, afin que les sites et les courriels suspects puissent être bloqués à la source et au plus vite. La cybersécurité nécessite une étroite concertation entre les secteurs public et académique et le secteur privé des entreprises technologiques. Une entreprise est dite technologique lorsqu'elle vend et/ou développe de nouveaux produits ou services basés sur une nouvelle technologie ou sur de nouvelles applications d'une technologie existante. Leur développement doit intégrer la cybersécurité dès leur conception (*security by design*) et ce principe doit s'appliquer à tous les acteurs (conditions équitables).

En outre, il se recommande que les données à caractère personnel soient à nouveau sauvegardées de manière décentralisée, sous le contrôle des personnes elles-mêmes et grâce à la technologie, et non pas concentrées auprès des entreprises technologiques (cf. "*Solid project*"), afin d'éviter notamment la formation de monopoles et toute fuite de données.

Les entreprises technologiques ont pleinement profité du web. Elles peuvent, elles aussi, proposer leurs produits et services au-delà les frontières, mais la réglementation internationale fait défaut. En d'autres termes, elles peuvent s'installer n'importe où pour vendre leurs produits, mais elles ne veulent pas que les autorités locales demandent ce qu'ils contiennent. Elles disent "oui aux avantages mais non aux inconvénients", ce qui est source de conditions de concurrence inégales entre les entreprises belges et leurs concurrentes internationales.

kundig te zijn in informatica, vermits er een bloeiende markt ontstaan is die *plug-and-play* hardware en software ontwikkelt om internetfraude te faciliteren *(cybercrime-as-a-service).* Dit houdt in dat internetfraude exponentieel toeneemt.

Bovendien kunnen de daders ongehinderd over staatsgrenzen heen opereren en brengen zij hun illegale vermogensvoordelen met een muisklik onder in verre bestemmingen nadat ze vlot meermaals van vorm gewisseld zijn. Dit bemoeilijkt het strafonderzoek sterk, aangezien de rechtshandhavers gebonden zijn aan een achterhaald idee van territoriale jurisdictie. Het opstellen van Europese onderzoeksbevelen of internationale rechtshulpverzoeken zorgt hoe dan ook voor vertraging in het onderzoek, als er überhaupt wordt meegewerkt.

De rechtshandhavers kunnen deze tsunami nooit bolwerken met de beschikbare middelen. Daarom is preventie primordiaal. Eerst en vooral door het continu bewustmaken van de potentiële slachtoffers, dat wanneer iets te mooi lijkt om waar te zijn, dit meestal ook niet waar is.

Vervolgens door maximaal in te zetten op cyberveiligheid, zodat verdachte websites en mailberichten zo snel mogelijk bij de bron kunnen worden geblokkeerd. Dit dient te gebeuren in nauw overleg tussen de openbare, academische en private sector, namelijk de technologiebedrijven. Een technologiebedrijf is een bedrijf dat nieuwe producten of diensten verkoopt en/of ontwikkelt die zijn gebaseerd op nieuwe technologie of nieuwe toepassingen van bestaande technologie. Die ontwikkeling moet gebeuren met cyberveiligheid in het achterhoofd (*security by design*) en dit moet voor alle spelers gelden (*level playing field*).

Tevens strekt het tot aanbeveling dat de persoonsgegevens opnieuw gedecentraliseerd worden opgeslagen, onder controle van de personen zelf, door middel van technologie, en niet worden geconcentreerd bij die technologiebedrijven (bijvoorbeeld het *Solid-project*), teneinde onder meer monopolies en datalekken te vermijden.

De technologiebedrijven hebben ten volle geprofiteerd van het internet. Ook zij kunnen hun diensten en producten aanbieden over de grenzen heen, maar de internationale regulering blijft achterwege. Men kan met andere woorden in ieders achtertuin koekjes komen verkopen, maar men wil niet dat de lokale overheid vraagt wat er in die koekjes wordt gedraaid. Dit is een verhaal van wél de lusten, niet de lasten, en zorgt ook voor een ongelijk speelveld tussen Belgische bedrijven en hun internationale concurrenten.

En outre, ces entreprises technologiques sont de nature de plus en plus diverse, comme les chimères. Elles combinent souvent le rôle d'acteur financier, de commerçant, d'opérateur de télécommunications, etc., alors qu'elles ne se sentent pas liées par la législation associée à chacun de ces rôles. Cette situation perturbe également le marché et crée des zones grises favorables aux cybercriminels.

La Cour de Cassation a déjà estimé que les entreprises technologiques Yahoo et Skype devaient, en tant qu'opérateurs de télécommunications, se plier aux réquisitions conformément aux articles 46*bis*, 88*bis* et 90*ter* du Code d'instruction criminelle, mais le ministère public doit encore et toujours rappeler aux nouveaux opérateurs leurs obligations s'ils exercent des activités sur le marché belge. Ces opérateurs souhaitent également de plus en plus souvent organiser leur collaboration de leur propre manière, à savoir de manière minimale.

La plus grande confusion règne quant à la question de savoir qui doit être considéré comme fournisseur de services de télécommunications au sens des articles précités, ainsi qu'au sens de la loi du 13 juin 2005 relative aux communications électroniques. Cette question est essentielle pour la conservation des données. La possibilité pour le tribunal de demander directement les données n'a d'utilité que si ces données sont également conservées. Le récent arrêt de la Cour de Justice de l'UE du 6 octobre 2020 (affaires jointes C-511/18, C-512/18 et C-520/18, *La Quadrature du Net* notamment) à ce sujet est particulièrement pertinent et obligera le ministère public à repenser, dans un avenir proche, les méthodes existantes. Cela devra se faire de préférence en concertation étroite avec le secteur.

On ne comprend pas non plus pourquoi le refus de collaboration n'est pas punissable d'un emprisonnement, alors que cette peine est prévue dans l'équivalent de cet article pour les banques, l'article 46*quater* du Code d'instruction criminelle. L'amende maximale de 80 000 euros en cas de refus de collaboration est en effet souvent ridicule pour de telles multinationales. La seule sanction que ces opérateurs craignent est l'interdiction d'accéder aux utilisateurs belges.

Ce blocage des noms de domaine est actuellement déjà possible en Belgique mais uniquement pour la durée limitée de l'enquête en vertu de l'article 39*bis* du Code d'instruction criminelle. L'amende devrait au moins être proportionnelle au chiffre d'affaires de l'entreprise technologique.

Ce champ d'application est également imprécis pour les acteurs financiers. À quelles entreprises technologiques est-il possible d'adresser une réquisition en vertu

Bovendien zijn die technologiebedrijven steeds meer divers van aard, zoals chimaeren. Men combineert vaak de rol van financiële speler, handelaar, telecomoperator enzovoort, terwijl men zich niet gebonden voelt door de wetgeving die gepaard gaat met elk van die rollen. Ook dit zorgt voor een marktverstoring en creëert grijze zones waarin cybercriminelen goed gedijen.

Het Hof van Cassatie heeft al geoordeeld dat de technologiebedrijven Yahoo en Skype zich als telecomspeler moeten schikken naar de vorderingen overeenkomstig 46*bis*, 88*bis* en 90*ter* van het Wetboek van strafvordering, maar nog steeds moet het openbaar ministerie dagelijks gelijkaardige nieuwe spelers wijzen op hun plichten wanneer zij actief zijn op de Belgische markt. Dergelijke spelers willen ook steeds vaker een eigen, lees minimale, invulling geven aan hun medewerking.

Er heerst grote onduidelijkheid over wie als verstrekker van telecommunicatiediensten moet worden beschouwd in de zin van voormelde artikelen alsook van de wet van 13 juni 2005 betreffende de elektronische communicatie. Dit is van belang voor dataretentie. Dat het gerecht ze rechtstreeks kan bevragen, is alleen maar nuttig als ze ook gegevens bijhouden. Het recente arrest van het Hof van Justitie van de EU van 6 oktober 2020 (gevoegde zaken C-511/18, C-512/18 en C-520/18, *La Quadrature du Net e.a.*) hieromtrent is bijzonder relevant en zal het openbaar ministerie in de nabije toekomst ertoe verplichten de bestaande werkmethoden te herdenken. Dit zal bij voorkeur in nauw overleg met de sector moeten gebeuren.

Het is evenmin duidelijk waarom niet-medewerking niet strafbaar is met een gevangenisstraf, terwijl dit bij de evenknie van dit artikel voor de banken, artikel 46*quater* van het Wetboek van strafvordering, wél zo is. De maximale geldboete bij niet-medewerking van 80 000 euro is immers veelal een lachertje voor dergelijke multinationals. De enige sanctie waar deze spelers voor vrezen, is hen de toegang te ontzeggen tot de Belgische gebruikers.

Dergelijke blokkering van domeinnamen in België is nu reeds mogelijk, maar slechts voor de beperkte duur van het onderzoek onder artikel 39*bis* van het Wetboek van strafvordering. De geldboete zou minstens in verhouding moeten staan tot de omzet van het technologiebedrijf.

Ook voor financiële spelers is dit toepassingsgebied onduidelijk. Tot welke technologiebedrijven kan men een vordering richten overeenkomstig artikel 46*quater* van

de l'article 46*quater* du Code d'instruction criminelle? Qu'en est-il des nouveaux types de services tels que Apple Pay, Amazon Pay, Paypal, etc.?

Toutes ces nouvelles possibilités d'investigation supposent évidemment qu'il y ait réellement suffisamment d'enquêteurs spécialisés (au sein de la FCCU, de la RCCU et de la police locale) qui puissent enquêter sur les infractions liées à Internet et de magistrats du parquet spécialisés pour les poursuivre. En l'absence de recrutements supplémentaires dans ce sens, toutes ces possibilités resteront lettre morte.

E. **Exposé introductif de M. Geert Baudewijns (Secutec)**

M.Geert Baudewijns est le CEO van Secutec: il a commencé sa carrière en 1999 chez McAfee et travaille maintenant depuis 21 ans dans le secteur de la cybersécurité, qui a connu une croissance phénoménale. Il arrive que son entreprise soit appelée à deux heures du matin lorsqu'une école supérieure, par exemple, est victime d'un piratage informatique.

Secutec possède plusieurs sites dans le monde entier, mais ce sont les sièges implantés en Russie, aux États-Unis et en Israël qui sont les plus importants pour la cybersécurité. À Moscou, l'entreprise occupe 22 travailleurs chargés uniquement de la fraude à la carte de crédit et actifs sur le réseau obscur ("*darknet*") pour tenter de récupérer ("voler à nouveau") les cartes de crédit. À Tel Aviv, 18 personnes travaillent dans le domaine du *phishing* et proviennent toutes d'organisations militaires israéliennes.

En ce qui concerne la fraude sur Internet, M. Baudewijns distingue:

1. le rançongiciel (*ransomware*);

2. la fraude à la facturation et au CEO;

3. les mules financières (*Money mule accounts*).

Le rançongiciel

Secutec reçoit deux à trois notifications par semaine d'organisations piratées qui n'ont plus accès aux données de leur propre réseau. M. Baudewijns joue en quelque sorte le rôle de négociateur entre les pirates informatiques et la victime. Il a été toléré dans ce rôle par le précédent gouvernement.

Parfois, la victime n'a pas d'autre choix que de payer, faute de quoi elle n'a plus accès à ses données. Le client en décide évidemment toujours lui-même et Secutec

het Wetboek van strafvordering? Wat met nieuwsoortige diensten als Apple Pay, Amazon Pay, Paypal enzovoort?

Uiteraard veronderstellen al deze onderzoeksmogelijkheden dat er ook effectief voldoende gespecialiseerde onderzoekers (bij de FCCU, de RCCU en de lokale politie) zijn die internet-gerelateerde misdrijven kunnen onderzoeken, alsook gespecialiseerde parketmagistraten om ze te vervolgen. Zonder bijkomende aanwervingen in die zin blijft dit alles een dode letter.

E. **Inleidende uiteenzetting van de heer Geert Baudewijns (Secutec)**

De heer Geert Baudewijns is ceo van Secutec: hij is zijn carrière begonnen in 1999 bij McAfee er is ondertussen 21 jaar werkzaam in de cybersecuritysector, die een fenomenale groei heeft gekend. Zijn bedrijf wordt om twee uur 's nachts opgebeld wanneer bijvoorbeeld een hogeschool is gehackt.

Secutec heeft een aantal locaties in de hele wereld, maar het belangrijkst voor cybersecurity zijn de vestigingen in Rusland, de Verenigde Staten en Israël. In Moskou heeft het bedrijf 22 werknemers die enkel bezig zijn met kredietkaartfraude en die actief zijn op het zogenaamde *darknet,* waar zij pogen kredietkaarten "terug te stelen". In Tel Aviv werken 18 mensen rond *phishing,* die allemaal afkomstig zijn van militaire organisaties in Israël.

Wat internetfraude betreft, onderscheidt de heer Baudewijns:

1. *ransomware;*

2. factuur- en ceo-fraude;

3. *money mule accounts.*

Ransomware

Secutec krijgt twee à drie meldingen per week van gehackte organisaties die geen toegang meer hebben tot de gegevens op hun eigen netwerk. De heer Baudewijns treedt hier op als een soort onderhandelaar tussen de hackers en het slachtoffer. De heer Baudewijns werd door de vorige regering in deze rol gedoogd.

Soms kan het slachtoffer niet anders dan betalen, bij gebreke waarvan hij geen toegang meer heeft tot zijn gegevens. De klant bepaalt dit uiteraard steeds zelf

négocie avec les cybercriminels, ce qui prend en moyenne trois à quatre jours.

Dans 30 % des cas, les entreprises concernées paient la rançon. Il s'agit généralement de petites PME. Si elles ne paient pas, il existe un (important) dommage économique, qui a de toute façon un coût.

L'orateur renvoie au modèle économique hallucinant qui se cache derrière de telles organisations criminelles et estime qu'en Belgique, 100 millions d'euros de rançon sont payés sur une base annuelle. Secutec est impliqué dans des paiements pour un montant de 30 millions d'euros en Belgique; à cet égard, il faut savoir que Secutec ne traite que les cas dans lesquels la demande de rançon ne dépasse pas 75 000 euros (d'autres entreprises interviennent en Belgique pour les montants plus importants).

Secutec collabore avec le CCB et CERT.be, qui disposent de très nombreuses informations. Il n'existe toutefois pas de formes de collaboration standardisées. C'est en revanche le cas aux États-Unis, ce qui présente des avantages majeurs dans le cadre de la lutte contre ce phénomène.

M. Baudewijns conclut qu'il devrait être possible d'obliger légalement les *hackers* à rendre certaines données.

Fraude à la facturation et au CEO

Ces formes de fraude, qui ont déjà été abordées par d'autres orateurs, représentent, en Belgique, un montant de 65 millions d'euros par an. Pour le moment, il est possible, lors de l'ouverture d'un compte en banque en Belgique, de mentionner n'importe quel nom à côté du numéro IBAN; ce nom n'est pas contrôlé par la banque. Aux Pays-Bas, par contre, la banque est explicitement obligée de contrôler le lien entre le numéro de compte et le nom du titulaire du compte.

Cette fraude n'est pas très difficile à contrer; il faut seulement que les banques fassent preuve d'un certain courage. Les Pays-Bas sont beaucoup plus avancés sur ce point. La solution est assez simple: il suffit de créer une base de données (comparable au système de paiement Swift) répertoriant tous les numéros de comptes et les noms, qui permettra d'effectuer des contrôles sur la base du nom et du numéro de compte à la demande d'une banque.

Money mule accounts

Il s'agit en l'occurrence d'un compte en banque utilisé pour y virer des sommes clandestines provenant

en Secutec onderhandelt met de cybercriminelen, wat gemiddeld drie à vier dagen in beslag neemt.

30 % van de betrokkenen betaalt het losgeld. Meestal gaat het om kleine kmo's. Als ze niet betalen, is er vaak sprake van (grote) economische schade, die hoe dan ook een kostprijs heeft.

De spreker verwijst naar het hallucinante businessmodel achter dergelijke criminele organisaties en schat dat er in België 100 miljoen euro aan losgeld betaald wordt op jaarbasis. Secutec is betrokken bij betalingen ten belope van 30 miljoen euro in België; hierbij dient men te weten dat Secutec enkel gevallen behandelt waarbij maximum 75 000 euro losgeld wordt gevraagd (voor hogere bedragen zijn er andere bedrijven actief in België).

Secutec werkt samen met het CCB en CERT.be, die over zeer veel informatie beschikken. Er zijn echter geen geijkte samenwerkingsvormen. In de Verenigde Staten is dat wel het geval, hetgeen grote voordelen heeft in de bestrijding van dit fenomeen.

De heer Baudewijns besluit dat het mogelijk zou moeten zijn de hackers op legale wijze te verplichten bepaalde gegevens terug te geven.

Factuur- en ceo-fraude

Deze reeds door anderen besproken vormen van fraude belopen in België tot 65 miljoen euro per jaar. Momenteel kan men bij het openen van een bankrekening in België naast het IBAN-nummer een willekeurige naam opgeven; dit wordt niet door de bank gecontroleerd. In Nederland daarentegen is de bank expliciet verplicht het verband te controleren tussen het rekeningnummer en de naam van de rekeninghouder.

Deze fraude is niet zo moeilijk aan banden te leggen, er is alleen een bepaalde moed nodig bij de banken. In Nederland staat men op dit punt veel verder. De oplossing is vrij eenvoudig: de creatie van een database (vergelijkbaar met het Swift-betalingssysteem) waarin alle rekeningnummers en namen worden opgeslagen en waar bij een aanvraag door een bank een controle gebeurt op naam en rekeningnummer.

Money mule accounts

Het gaat hier om een bankrekening die gebruikt wordt om clandestiene gelden afkomstig uit *phishing*-activiteiten

d'activités de *phishing*. Cette forme de fraude représente, en Belgique, une somme allant jusqu'à 90 millions d'euros par an.

Auparavant, les criminels recouraient à des sans-abri; actuellement, ils font souvent appel à des étudiants: un jeune sur dix serait disposé à prêter sa carte de banque sans en parler à ses parents; 7 % de la population est confrontée à ce type de demande et 23 % y accèdent effectivement.

Chaque banque sait lesquels de ses comptes sont utilisés comme *money mule accounts*. Secutec traite en moyenne 1 000 cas de fraude par jour pour les banques belges. L'orateur indique qu'actuellement, le Règlement général sur la protection des données (RGPD) n'autorise pas les banques à échanger des données concernant ce type de comptes; pourtant, cela permettrait de contrer beaucoup plus rapidement ce type de fraude.

Conclusion

M. Baudewijns estime que la cybersécurité devrait devenir une orientation d'études au niveau universitaire. Sur ce plan, la Belgique est très en retard sur des pays comme les États-Unis, la Russie et Israël. Comme notre pays héberge le siège d'organisations internationales comme l'OTAN et l'UE, la Belgique est une cible de toutes sortes de cyberfraude au niveau mondial.

Par ailleurs, il convient de créer un service de cyberrenseignements, qui collabore avec tous les pays européens et qui puisse imposer des obligations aux hackers, en plus de l'échange d'informations avec d'autres pays. Israël, par exemple, est dans le top trois de la cybersécurité au niveau mondial parce que la cybersécurité y est organisée au niveau militaire. Pendant le service militaire (qui dure de deux à trois ans), il est possible de décider de faire des études universitaires en cybersécurité: il est impossible pour M. Baudewijns d'attirer en Belgique des collaborateurs ayant un niveau aussi élevé.

À cet égard, le statut de fonctionnaire, et en particulier, la rémunération qui y est liée, pose un gros problème dans notre pays. L'orateur a toutes les difficultés du monde à garder les bons éléments. Les enquêteurs devraient aussi avoir plus de liberté de mouvement dans leurs enquêtes, comme dans le modèle américain.

M. Baudewijns ajoute qu'il est souvent obligé de travailler dans une zone grise: heureusement, son entreprise entretient de bonnes relations avec les gestionnaires de noms de domaine belges, mais les choses sont bien sûr beaucoup plus difficiles quand il s'agit par exemple de l'Ukraine. Il en résulte que Secutec va, par exemple, op over te schrijven. Deze vorm van fraude beloopt in België tot 90 miljoen euro per jaar.

Vroeger werden hier voor daklozen aangesproken, nu doen de criminelen vaak een beroep op studenten: 1/10 van de jongeren zou bereid zijn om hun bankkaart uit te lenen zonder hierover iets tegen hun ouders te zeggen; 7 % van de bevolking komt hiermee in aanraking en 23 % gaat hier effectief op in.

Elke bank weet welke van haar rekeningen worden gebruikt als *money mule accounts*. Per dag behandelt Secutec gemiddeld 1 000 gevallen van fraude voor de Belgische banken. De spreker stelt dat de Algemene Verordening Gegevensbescherming (AVG) de banken momenteel niet toestaat gegevens met betrekking tot dergelijke accounts uit te wisselen; nochtans zou op die manier deze fraude veel vlugger aan banden kunnen worden gelegd.

Besluit

De heer Baudewijns is van mening dat cybersecurity een studierichting zou moeten worden op universitair niveau. België loopt hier ver achter op landen als de Verenigde Staten, Rusland en Israël. Omdat ons land de zetel huisvest van internationale organisaties als de NAVO en de EU, is België een doelwit van allerlei vormen van cyberfraude op wereldniveau.

Daarnaast moet een cyberinlichtingendienst worden opgericht, die samenwerkt met alle Europese landen en die de hackers verplichtingen kan opleggen, naast de uitwisseling van informatie met andere landen. Israël bijvoorbeeld staat in de top drie van cybersecurity op wereldvlak omdat cybersecurity op militair niveau is georganiseerd. Tijdens de legerdienst (twee à drie jaar) kan men ervoor opteren om universitaire studies in cybersecurity te doen: de heer Baudewijns kan in België onmogelijk medewerkers van een dergelijk hoog niveau aantrekken.

In dit verband is het ambtenarenstatuut en meer bepaald de ermee gepaard gaande verloning een groot probleem in ons land. De spreker heeft alle moeite van de wereld om goede krachten in dienst te houden. Speurders zouden naar Amerikaans model ook minder gebonden moeten zijn in een onderzoek.

De heer Baudewijns voegt eraan toe dat hij vaak verplicht is om in een zogenaamde grijze zone te werken: gelukkig heeft zijn bedrijf goede relaties met de Belgische domeinnaambeheerders, maar dat ligt uiteraard heel wat moeilijker wanneer het bijvoorbeeld om Oekraïne gaat. Het gevolg is dat Secutec een bepaalde website

essayer de neutraliser un site internet depuis Israël, car il est souvent impossible de réagir assez rapidement et adéquatement depuis l'Europe.

En tout cas, le FCA et CERT.be ont connu une évolution formidable ces cinq dernières années, parce qu'ils ont obtenu plus de personnes et de moyens. Des moyens supplémentaires sont toutefois aussi nécessaires pour les intermédiaires entre CERT.be et les entreprises, les *resellers*: selon la loi, une entreprise dispose de 72 heures pour déclarer qu'elle a été piratée, alors que les entreprises comme Secutec ont besoin de cinq à dix jours avant de savoir avec certitude d'où vient le piratage.

II. — **QUESTIONS ET OBSERVATIONS DES MEMBRES**

M. Michael Freilich (N-VA) rappelle que, selon M. Bogaert, il est question d'une augmentation générale des faits de 29 % entre 2018 et 2019 et de 80 % pour ce qui est du *phishing*. Que concernent exactement ces 29 %? S'agit de fraude générale?

M. Bogaert parle de la conservation de données pour une période de plus de neuf mois: les enquêtes durent-elles vraiment si longtemps? Quel délai est préférable selon la FCCU: 12 mois sont-ils suffisants ou bien faut-il deux ou trois ans?

M. Bogaert plaide en outre en faveur d'un accès gratuit aux données des opérateurs. Les sociétés commerciales ne se montrent sans doute pas toujours très coopératives à cet égard, mais si elles sont actives en Belgique et y obtiennent des avantages, elles ont le devoir d'offrir cet accès gratuit. Dispose-t-on de chiffres concrets sur les montants facturés par ces entreprises? M. Bogaert peut-il donner les noms des entreprises qui ne coopèrent pas?

À l'intention du SPF Économie, M. Freilich constate que l'on attend le *Digital Services Act* (loi sur les services numériques) de la Commission européenne. L'Inspection économique met par ailleurs en œuvre une procédure de notification et de retrait d'annonces (*notice and take down*): cette procédure s'applique-t-elle uniquement à Google ou vaut-elle également pour Facebook?

M. Freilich évoque une fausse campagne Facebook, en 2019, qui annonçait que Bart De Wever allait proposer des crypto-monnaies. Il a fallu beaucoup de temps pour que cette fausse campagne soit retirée du web. Quelle est la durée normale de la procédure de notification et de retrait?

zal proberen plat te leggen vanuit Israël, omdat men vanuit Europa zelf vaak niet snel en adequaat genoeg kan reageren.

In elk geval hebben het CCB en CERT.be de laatste vijf jaar een geweldige evolutie doorgemaakt omdat zij veel meer mensen en middelen hebben gekregen. Er zijn echter ook meer middelen nodig voor de tussenpersonen tussen CERT.be en de bedrijven, de zogenaamde *resellers:* volgens de wet heeft een bedrijf 72 uur de tijd om duidelijk te maken dat het gehackt is, terwijl bedrijven als Secutec vijf à tien dagen nodig hebben vooraleer zij met zekerheid kunnen stellen uit welke hoek de hacking afkomstig is.

II. — **VRAGEN EN OPMERKINGEN VAN DE LEDEN**

De heer Michael Freilich (N-VA) geeft aan dat volgens de heer Bogaert sprake is van een algemene toename van feiten met 29 % tussen 2018 en 2019 en van 80 % wat *phishing* betreft. Waarop slaat deze 29 % precies? Gaat dit over algemene fraude?

De heer Bogaert spreekt over het bijhouden van gegevens voor een periode langer dan negen maanden: duren de onderzoeksprocedures werkelijk zo lang? Welke termijn is verkieslijk voor de FCCU: volstaan 12 maanden of gaat het over twee of drie jaar?

Daarnaast pleit de heer Bogaert voor gratis toegang tot de gegevens van de operatoren. Commerciële bedrijven zullen hier wellicht niet altijd aan meewerken, maar als zij actief zijn in België en hier voordelen behalen, hebben zij de plicht om gratis toegang aan te bieden. Zijn er concrete cijfers over het bedrag dat deze bedrijven dan aanrekenen? Kan de heer Bogaert de naam geven van de bedrijven die niet meewerken?

Ter attentie van de FOD Economie stelt het lid vast dat gewacht wordt op de zogenaamde *Digital Services Act* van de Europese Commissie. De Economische Inspectie heeft een zogenaamde *notice and take down*-procedure voor het weghalen van advertenties; geldt dit enkel voor Google of ook voor Facebook?

De heer Freilich verwijst naar een valse Facebookcampagne in 2019 waarbij Bart De Wever *cryptocurrency* zou aanbieden: het heeft bijzonder lang geduurd om deze valse campagne offline te laten halen. Wat is de standaard duurtijd van de *notice and take down*-procedure?

L'Inspection économique a-t-elle eu accès au profil Facebook comme si elle était une sorte d'"administrateur", l'habilitant ainsi à épingler certaines annonces, et ce, plus qu'un utilisateur normal ne pourrait le faire? Cela s'applique-t-il également à des sites de vente tels que *2ememain.be*?

Que pensent par ailleurs les orateurs de l'identification obligatoire sur les sites de vente? Ces sites font souvent l'objet de tentatives d'escroquerie de la part d'internautes étrangers. Toute le monde peut en effet s'inscrire sur de tels sites, sans devoir fournir une copie de sa carte d'identité ni même un numéro de téléphone.

À l'intention du CCB, M. Freilich indique qu'il ne connaît pas la plate-forme de signalement *suspect@safeonweb.be*. Ne serait-il pas intéressant de faire un sondage pour savoir combien de personnes ont connaissance de cette plateforme? Il suggère en tout cas qu'après analyse, on informe les signaleurs par courrier électronique de la suite donnée à leur signalement, comme cela se fait généralement, notamment pour Twitter.

Enfin, M. Freilich a entendu M. Baudewijns parler d'opérations visant à aller récupérer les données de cartes de crédit chez ceux qui les ont volées. L'intervenant trouve cela très étrange et estime que ce n'est pas envisageable en Belgique. Secutec fait cela sur le "*darknet*" et parle également de "paralyser des sites web en passant par Tel Aviv". Tout cela serait probablement illégal en Belgique. Ne serait-il pas préférable de tendre vers un cadre légal par lequel une autorité disposerait d'un arsenal de moyens qu'elle serait seule habilitée à utiliser? À titre d'illustration, le membre fait référence à la police, qui dispose d'un monopole légal en matière de port d'armes. En tout cas, tout devra se faire au départ de la Belgique même, et non via un détour par l'étranger.

M. Albert Vicaire (Ecolo-Groen) conclut, sur la base des interventions d'au moins quatre orateurs, qu'ils préconisent d'obliger les entreprises technologiques à coopérer, alors que cette coopération est, pour l'instant, volontaire.

Quelles autres mesures législatives les intervenants jugent-ils nécessaires pour protéger les consommateurs dans ce domaine?

M. Roberto D'Amico (PVDA-PTB) indique que, face à l'ampleur du phénomène de la fraude financière et économique, notre pays devra opérer un tournant majeur, en particulier dans le recrutement de nouvelles personnes. Nous assistons en effet à une professionnalisation de ces pratiques criminelles sur internet. Ils utilisent à leur guise les ruses de la mondialisation et les failles du numérique pour mieux s'enrichir. Il peut ainsi s'agir de

Heeft de Economische Inspectie toegang gekregen tot het Facebookprofiel als een soort *administrator*, waarbij zij advertenties zou kunnen *taggen,* meer dan een reguliere gebruiker dat zou kunnen? Geldt dit ook voor de samenwerking op marktplaatsen zoals *2dehands.be*?

Wat denkt men voorts van een verplichte identificatie op marktplaatsen? Op dergelijke sites vindt men vaak fraude vanuit het buitenland. Iedereen kan zich immers registreren op een dergelijke site, zonder een kopie van de identiteitskaart of zelfs een telefoonnummer te moeten geven.

Ter attentie van het CCB stelt de heer Freilich dat hij het meldingsplatform *verdacht@safeonweb.be* niet kent. Zou het niet interessant zijn via een peiling na te gaan hoeveel mensen dit kennen? Hij stelt voor om melders in elk geval – eens de analyse gebeurd is – feedback te geven over hun melding via mail. Dit is gebruikelijk bij onder meer Twitter.

Ten slotte hoort het lid de heer Baudewijns gewag maken van het "terug stelen van creditcardgegevens": dit komt de heer Freilich heel eigenaardig voor en niet doenbaar in België. Secutec doet dit op het *darknet* en spreekt ook van het "platleggen van websites via Tel Aviv". Dit alles zou in België waarschijnlijk illegaal zijn; is het niet verkieslijk om een wettelijke omkadering na te streven, waarbij een instantie een arsenaal ter beschikking krijgt en dit als enige mag gebruiken? Ter illustratie verwijst het lid naar de politie die een wettelijk monopolie heeft op het dragen van wapens. In elk geval zou dit in België zelf moeten gebeuren en niet via een omweg naar het buitenland.

De heer Albert Vicaire (Ecolo-Groen) maakt uit het betoog van ten minste vier sprekers op dat zij ervoor pleiten de samenwerking door de technologiebedrijven, die thans vrijwillig is, verplicht te maken.

Welke wetgevende ingrepen achten de sprekers nog noodzakelijk teneinde de consument in dit verhaal te beschermen?

De heer Roberto D'Amico (PVDA-PTB) wijst erop dat ons land, gelet op de omvang van de financiële en economische fraude, het over een heel andere boeg zal moeten gooien, vooral wat de werving van nieuw personeel betreft. Het is immers duidelijk dat internetcriminelen almaar professioneler tewerk gaan. Om zich te verrijken, bedienen zij zich volop van de trukendoos van de mondialisering en van de manco's van de digitale

réseaux mafieux qui exploitent des personnes vulnérables ou encore d'entreprises malhonnêtes qui feraient tout pour grossir leur marge et s'imposer sur le marché.

Le pouvoir politique doit donc adopter une posture intransigeante contre cette forme de fraude, aussi variée soit-elle. La lutte contre la fraude financière et économique sur internet ne peut se faire sans une supériorité du politique sur les géants du numériques et sans la mise en place d'un cadre réglementaire stricte. Les multinationales actives sur internet ont des comptes à rendre, comme tout le monde. En ce sens, M. D'Amico rejoint l'avis de M. De Keersmaecker, qui dénonce une réglementation peu dissuasive, notamment lorsque certaines grandes entreprises refusent de coopérer avec les autorités.

Selon M. D'Amico, il est impératif de mettre en place des normes strictes. On doit encadrer les pratiques sur internet afin d'éviter les effets pervers qu'elles suscitent. Le membre se réfère à ce titre au sentiment d'impunité de certaines entreprises, mais également à la fraude contre les particuliers. Celle-ci a augmenté de 30 % l'an passé et elle touche en particulier des personnes fragiles. Il faudra donc revoir les pratiques du commerce en ligne, et inévitablement investir dans les moyens humains.

Le membre souhaite poser quelques questions à l'ensemble des intervenants.

Lorsque la fraude provient d'une entreprise, ne faudrait-il pas drastiquement renforcer les sanctions, notamment au niveau des peines d'emprisonnement? Ne devrait-on pas également généraliser le système de sanctions liant le montant de l'amende au chiffre d'affaires de l'entreprise?

Ensuite, en ce qui concerne le commerce en ligne, ne devrions-nous pas revoir les règles qui régissent les pratiques? Comment pourrions-nous faire pour poser un nouveau cadre qui suscite moins la convoitise des fraudeurs?

Par ailleurs, la lutte contre la fraude financière et économique ne peut se faire sans un accès aux, et un contrôle des, données numériques. Néanmoins, les pouvoirs politiques sont dépossédés de la gigantesque masse d'informations qui sont stockées par les géants du numérique. Comment pourrions-nous améliorer l'accès à ces données? Sommes-nous assez coercitif? Devrions-nous renforcer le blocage des numéros de domaine, comme le suggère M. De Keersmaecker?

wereld. In dit verband kan sprake zijn van maffianetwerken die misbruik maken van zwakkeren, of nog van oneerlijke bedrijven die er alles voor over hebben om hun winstmarge aan te dikken en hun plaats in de markt af te dwingen.

Daarom moet de overheid zich onverzettelijk opstellen tegen dergelijke fraude, hoe divers die ook is. De financiële en economische fraude op het internet kan niet worden aangepakt zolang de overheid niet de overhand heeft op de digitale reuzen en zonder een strikt reglementair raamwerk. De multinationals die actief zijn op het internet dienen net als iedereen rekenschap af te leggen. In die zin is de heer D'Amico het eens met de heer De Keersmaecker, die aanklaagt dat de regelgeving te weinig ontradend is, meer bepaald met betrekking tot het feit dat bepaalde grote bedrijven weigeren samen te werken met de overheden.

Er moeten volgens de heer D'Amico onmiskenbaar strikte normen worden vastgelegd. De internetpraktijken moeten aan regels worden onderworpen om de kwalijke gevolgen ervan te voorkomen. Het lid verwijst in dat verband naar het gevoel van straffeloosheid van bepaalde bedrijven en naar de fraude ten aanzien van particulieren. Die fraude is vorig jaar met 30 % toegenomen en treft vooral kwetsbare personen. De onlinehandelspraktijken moeten dus worden herzien en er moet onmiskenbaar in personele middelen worden geïnvesteerd.

Het lid heeft ook enkele vragen voor alle sprekers.

Indien de fraude wordt gepleegd door een onderneming, rijst de vraag of de sancties niet fors zouden moeten worden verstrengd, meer bepaald wat de gevangenisstraffen betreft. Zou er geen veralgemening moeten komen van de sanctieregeling waarbij het bedrag van de geldboete afhangt van de omzet van de onderneming?

Zijn vervolgens de regels inzake onlinehandel niet aan herziening toe? Hoe kan een nieuw reglementair raamwerk worden uitgewerkt dat de hebzucht van de fraudeurs enigszins tempert?

Voorts kan financiële en economische fraude niet worden aangepakt zonder toegang tot en controle van de digitale gegevens. De overheden zijn echter niet langer in het bezit van de gigantische hoeveelheid informatie die de digitale reuzen hebben opgeslagen. Hoe kan de toegang tot die gegevens worden verbeterd? Zijn we streng genoeg? Moeten de domeinnamen vaker worden geblokkeerd, zoals de heer De Keersmaecker oppert? Moeten de digitale reuzen ertoe worden verplicht hun

Devrions-nous imposer des bases de données publiques aux géants du numérique? Quelle rôle l'Europe pourrait jouer dans ce domaine?

À côté du volet répressif, il y a l'aspect tout aussi important, voir plus encore, de la prévention. Qu'est-ce que les orateurs recommanderaient-ils à ce niveau-là? Vers quel public cible devrions-nous diriger les efforts?

Concernant le manque de moyens humains et financiers dont dispose notre pays en matière de lutte contre la fraude financière et économique sur internet, les intervenants pourraient-ils préciser les principaux manquements? Le nouveau gouvernement ne mentionne pas explicitement la problématique de la fraude économique et financière dans l'accord de gouvernement, mais il affirme vouloir renforcer la prévention contre la fraude en ligne. Qu'est-ce que le pouvoir politique doit impérativement mettre en place durant cette législature?

En matière de cybersécurité, l'accord du gouvernement Michel prévoyait différentes mesures, comme le fait de rendre opérationnel le CCB ou de renforcer les moyens des différents services compétents en la matière. Le gouvernement s'était même fixé trois objectifs stratégiques. Près de six ans après cet accord, quel constat les intervenants font-ils de l'évolution de la situation en Belgique en matière de cybersécurité?

Mme Melissa Depraetere (sp.a.) explique qu'il y a quelques mois, elle a demandé à la ministre de l'Économie de l'époque, Mme Nathalie Muylle, des chiffres sur la fraude par Internet en période de coronavirus (QRVA 55 024, p. 163). La réponse de la ministre a révélé une nette augmentation du nombre de cas de fraude via les boutiques en ligne. Entre le 1er mars et le 30 juin 2019, le SPF Économie a en effet reçu en moyenne 447 signalements par mois, alors que sur la même période en 2020, on a en a dénombré 1 213 par mois. Très souvent, il s'agissait de boutiques en ligne étrangères. Notre pays peut demander à l'autorité compétente d'un autre État membre de prendre des mesures contre une boutique en ligne, mais l'autorité en question peut décider de donner suite ou non à cette demande. Mme Coppin peut-elle donner davantage d'informations sur la coopération européenne mise en place dans ce domaine? L'intervenante a déposé une proposition de résolution appelant le gouvernement à préconiser une approche coordonnée au niveau européen dans la lutte contre la fraude sur Internet, y compris par la création d'une autorité européenne chargée de veiller à l'application de la législation, qui pourrait intervenir de manière efficace et infliger des sanctions (DOC 55 1140/001). Que pense la représentante du SPF Économie de cette initiative?

gegevensbanken openbaar te maken? Welke rol is ter zake voor Europa weggelegd?

Naast het repressieve aspect is er het even belangrijke, zo niet nog belangrijker aspect van de preventie. Wat bevelen de sprekers in dat verband aan? Op welke doelgroep dienen de inspanningen zich toe te spitsen?

Kunnen de sprekers duidelijker aangeven wat de belangrijkste problemen zijn inzake het gebrek aan personele en financiële middelen van ons land om financiële en economische internetfraude aan te pakken? De nieuwe regering heeft het probleem van de financiële en economische fraude niet uitdrukkelijk in het regeerakkoord opgenomen, maar geeft wel aan meer te willen doen inzake de preventie van onlinefraude. Wat moeten de beleidsmakers absoluut verwezenlijken tijdens deze regeerperiode?

Inzake cyberveiligheid voorzag het regeerakkoord van de regering-Michel reeds in diverse maatregelen, zoals het operationeel maken van het CCB, of nog het optrekken van de middelen van de verschillende ter zake bevoegde diensten. De regering had zelfs drie strategische doelstellingen vastgelegd. Hoe is de situatie in België inzake cyberveiligheid volgens de sprekers geëvolueerd, nu bijna zes jaar na dat akkoord?

Mevrouw Melissa Depraetere (sp.a) heeft enkele maanden geleden cijfers opgevraagd bij de toenmalige minister bevoegd voor Economie, mevrouw Nathalie Muylle, omtrent internetfraude in tijden van corona (QRVA 55 024, blz. 163). Uit het antwoord van de minister kwam een duidelijke stijging naar voren van het aantal fraudegevallen via webshops. In de periode van 1 maart tot 30 juni 2019 ontving de FOD Economie gemiddeld 447 meldingen per maand; over dezelfde periode in 2020 was dat aantal toegenomen tot 1 213 per maand. Heel vaak betrof het buitenlandse webshops. Ons land kan aan de bevoegde autoriteit van een andere lidstaat vragen om actie te ondernemen tegen een webshop, maar die autoriteit kan dan beslissen daar al dan niet gevolg aan te geven. Kan mevrouw Coppin meer informatie geven over de Europese samenwerking die op dit vlak bestaat? Het lid heeft een voorstel van resolutie ingediend waarin de regering wordt verzocht op Europees niveau te pleiten voor een gecoördineerde aanpak in de strijd tegen internetfraude, inclusief het oprichten van een Europese handhavingsautoriteit die effectief kan optreden en sancties kan opleggen (DOC 55 1140/001). Hoe staat de spreekster van de FOD Economie tegenover dit initiatief?

Mme Coppin peut-elle également indiquer comment les entreprises technologiques pourraient contribuer à une meilleure coopération entre les États membres de l'UE?

L'oratrice peut-elle par ailleurs préciser si l'Inspection économique ne prend des mesures que lorsqu'elle reçoit une plainte (ou une série de plaintes) ou si elle intervient également de manière proactive dans la lutte contre la fraude sur Internet?

La numérisation croissante de ces dernières années a sans aucun doute créé des possibilités et des opportunités supplémentaires pour le SPF Économie et les autres institutions représentées à cette audition. Mais a-t-on prévu, d'autre part, des ressources supplémentaires pour le SPF Économie? Mme Coppin pourrait-elle également préciser quels sont les nouveaux outils utilisés et si les autres instances les utilisent aussi. Le SPF Économie recourt-il, dans ce domaine, à la technologie de l'intelligence artificielle?

Enfin, Mme Depraetere voudrait savoir si et dans quelle mesure les initiatives des différents acteurs sont coordonnées. Outre le point de contact général (*pointdecontact.belgique.be/meldpunt/fr/bienvenue*), géré par le SPF Économie, il existe également l'initiative Safeonweb.be du CCB. Les cybercriminels ne risquent-ils pas de tirer profit d'une telle approche morcelée? Quelle est la position du SPF Économie, en tant qu'entité faîtière, à cet égard? L'oratrice voit-elle l'intérêt de créer une banque-carrefour qui rassemblerait toutes les informations relatives à la fraude sur Internet?

M. Patrick Prévot (PS) estime que la présente audition constitue un enrichissement pour les travaux tant de cette commission que d'autres commissions, et que l'ampleur de la fraude financière et économique sur Internet impose de légiférer.

M. Prévot indique que, le 8 octobre 2020, la Chambre a adopté une proposition de loi visant à protéger les consommateurs contre l'usage sans limite des capteurs de santé et autres appareillages similaires à des fins d'assurance (DOC 55 0263/010). L'intervenant renvoie également à une série de tests que Test-Achats a réalisés sur un large éventail d'objets connectés (montres intelligentes, téléviseurs, babyphones, serrures, caméras, etc.). Les résultats de ces analyses sont systématiquement une source d'inquiétude, dès lors que de graves manquements ont été révélés dans le domaine de la sécurité et du respect de la réglementation relative à la protection de la vie privée.

Le membre aimerait savoir si un cadre légal est disponible en matière de cybersécurité des objets connectés, et quelles sont le cas échéant les obligations que les

Kan mevrouw Coppin voorts aangeven hoe de technologiebedrijven zouden kunnen bijdragen aan een verbeterde samenwerking tussen de EU-lidstaten?

Kan de genoemde spreekster ook verduidelijken of de Economische Inspectie enkel actie onderneemt wanneer zij een klacht (of een aantal klachten) heeft ontvangen, of dat zij ook proactief optreedt in de strijd tegen internetfraude?

De toenemende digitalisering van de laatste jaren heeft ongetwijfeld extra mogelijkheden en opportuniteiten gecreëerd voor de FOD Economie en de andere uitgenodigde instellingen. Staan daar echter ook bijkomende middelen voor de FOD Economie tegenover? Kan mevrouw Coppin tevens preciseren welke nieuwe tools worden gebruikt en of die ook worden gehanteerd door de andere instanties? Doet de FOD Economie ter zake een beroep op de technologie van de artificiële intelligentie?

Tenslotte wenst mevrouw Depraetere te vernemen of en in welke mate de initiatieven van de verschillende actoren gecoördineerd zijn. Zo is er naast het algemene Meldpunt (*www.meldpunt.belgie.be*), beheerd door de FOD Economie, het initiatief Safeonweb.be van het CCB. Bestaat niet het gevaar dat internetcriminelen hun voordeel doen met zulke versnipperde aanpak? Wat is het standpunt hieromtrent van de FOD Economie, als overkoepelende entiteit? Ziet de spreekster brood in de oprichting van een kruispuntbank, waarin alle informatie omtrent internetfraude zou worden verzameld?

De heer Patrick Prévot (PS) meent dat deze hoorzitting een verrijking vormt voor de werkzaamheden van deze en andere commissies, en dat de omvang van de financieel-economische internetfraude noopt tot een wetgevend optreden.

De heer Prévot wijst erop dat de Kamer op 8 oktober 2020 een wetsvoorstel heeft aangenomen dat ertoe strekt consumenten te beschermen tegen het ongebreidelde gebruik van gezondheidstrackers en soortgelijke apparaten voor verzekeringsdoeleinden (DOC 55 0263/010). Tevens verwijst hij naar een aantal testen die Test Aankoop uitvoerde op een ruime waaier aan geconnecteerde objecten (intelligente horloges, televisietoestellen, babyfoons, sloten, camera's enzovoort). De resultaten van die analyses geven steevast aanleiding tot bezorgdheid: er kwam ernstige tekortkomingen aan het licht op het vlak van de veiligheid en de naleving van de privacyregelgeving.

Het lid zou graag vernemen of er een wettelijk kader voorhanden is inzake de cyberveiligheid van geconnecteerde objecten, en welke desgevallend de verplichtingen

fabricants doivent respecter. L'Inspection économique réalisent-elles des contrôles sur ce point? Par ailleurs, des sanctions ont-elles déjà été infligées sur la base du non-respect des droits des consommateurs?

Mme Leen Dierick (CD&V) indique que la fraude sur Internet est un problème persistant et croissant qu'elle dénonce depuis longtemps déjà. Il s'agit d'un phénomène qui ne connaît pas de frontières et qui revêt des formes très diverses. La membre a la nette impression que les autorités courent généralement après les faits et que les cybercriminels sont souvent trop rapides pour elles.

Il s'agit dès lors d'une problématique dont le Parlement doit se saisir. Les exposés des orateurs ont montré qu'une multitude de choses sont déjà entreprises. Mme Dierick considère toutefois qu'il faut fournir encore plus d'efforts afin de parvenir à une meilleure coordination, tant au niveau national entre les différents acteurs en Belgique qu'au niveau international entre les différents pays.

La membre estime en outre qu'il faut encore miser davantage sur la sensibilisation des consommateurs. Des campagnes telles que tropbeaupouretrevrai.be montrent l'exemple; de telles initiatives devraient encore être beaucoup plus développées. Les orateurs admettent-ils qu'il faudrait accorder une attention accrue à la sensibilisation? L'autorité fédérale libère-t-elle à l'heure actuelle des budgets suffisants à cet effet?

Une autre piste consiste à détecter (pro)activement la fraude et à la sanctionner. Mme Dierick aimerait entendre des recommandations concrètes de la part des orateurs: quelles sont les mesures législatives nécessaires afin de pouvoir lutter plus efficacement contre la fraude sur Internet?

M. Erik Gilissen (VB) adresse une question à M. De Keersmaecker, qui a évoqué des logiciels qui sont mis en vente et qui permettent à des personnes sans connaissances préalables spécifiques de générer un logiciel rançonneur. Ce genre de logiciel est sans doute basé sur un modèle donné. Cela permet-il d'intercepter la communication de ce logiciel rançonneur et de la bloquer au niveau du fournisseur d'accès? Ce pourrait en effet être une piste afin de lutter contre la propagation de ce logiciel rançonneur et dès lors de miner son efficacité.

Le membre demande à M. Bogaert ou Mme Clouner s'il est possible de lutter contre les "*Microsoft scams*" en dressant des listes noires des numéros de téléphone utilisés par les fraudeurs, numéros qui pourraient ainsi être bloqués par tous les fournisseurs d'accès.

zijn waaraan fabrikanten zich moeten houden. Voert de Economische Inspectie daarop controles uit? En werden er reeds sancties opgelegd op grond van het niet-naleven van de consumentenrechten?

Mevrouw Leen Dierick (CD&V) geeft aan dat internetfraude een hardnekkig en toenemend probleem is dat zij al lang aan de kaak stelt. Het betreft een grensoverschrijdend en zeer divers fenomeen. Het lid heeft stellig de indruk dat de autoriteiten veelal op achtervolgen zijn aangewezen en dat de internetcriminelen hen vaak te snel af zijn.

Het gaat dus om een probleem waarin het parlement zijn tanden moet zetten. De uiteenzettingen van de sprekers hebben aangetoond dat er op dit moment al zeer veel gebeurt. Mevrouw Dierick meent evenwel dat er nog meer inspanningen moeten worden geleverd om tot een betere coördinatie te komen, zowel intern, tussen de verschillende actoren in België, maar ook op internationaal niveau, tussen de verschillende landen.

Voorts is het lid van mening dat er nog meer moet worden ingezet op de sensibilisering van consumenten. Campagnes als temooiomwaartezijn.be tonen de weg; zulke initiatieven zouden nog veel meer moeten worden ontwikkeld. Zijn de sprekers het ermee eens dat meer aandacht zou moeten gaan naar sensibilisering? Maakt de federale overheid hiervoor op dit moment voldoende budgetten vrij?

De andere piste is het (pro-)actief opsporen van fraude en het bestraffen ervan. Mevrouw Dierick zou graag concrete beleidsaanbevelingen van de sprekers horen: welke wetgevende ingrepen zijn nodig om de strijd tegen internetfraude efficiënter te kunnen voeren?

De heer Erik Gilissen (VB) heeft een vraag voor de heer De Keersmaecker, die het had over softwarepakketten die te koop worden aangeboden en die mensen zonder specifieke voorkennis in staat stelt *ransomware* te genereren. Dergelijke *ransomware* heeft wellicht een bepaald patroon. Biedt dat de mogelijkheid om de communicatie van die *ransomware* te onderscheppen en te blokkeren op providerniveau? Dit zou immers een piste kunnen zijn om de verspreiding van die *ransomware* tegen te gaan en dus de effectiviteit ervan onderuit te halen.

Van de heer Bogaert of mevrouw Clouner zou het lid graag vernemen of de zogenaamde *Microsoft-scams* kunnen worden aangepakt door zwarte lijsten aan te leggen van de door de fraudeurs gebruikte telefoonnummers, die dan door alle providers zouden worden geblokkeerd.

Mme Kathleen Verhelst (Open Vld) se demande si la pratique accrue du télétravail à la suite de la crise du coronavirus n'a pas renforcé considérablement la possibilité de frauder sur Internet.

Elle souhaite également savoir si la législation relative à la protection de la vie privée, en particulier le RGPD, n'est pas excessive au point de constituer une entrave aux enquêtes dans le cadre de la fraude sur Internet.

Les orateurs ont-ils une idée des montants qui ont été versés aux criminels opérant sur Internet? Sont-ils en proportion avec ce qu'ils "rapportent"? Ces fonds restent-il en Europe ou partent-ils ailleurs? Quel montant récupère-t-on? De tels criminels se sont-ils déjà vu infliger des peines, et de quelles peines s'agit-il?

Il ressort de l'exposé des orateurs qu'il y a effectivement moyen de légiférer.

M. Baudewijns a prôné la mise en place d'une formation universitaire en cybersécurité. Peut-il indiquer de quels talents les étudiants ou futurs professionnels dans cette orientation devraient disposer?

Mme Katrien Houtmeyers (N-VA) indique que le mal est déjà fait lorsque CERT.be reçoit un signalement; l'objectif doit être d'agir de manière proactive dans la mesure du possible. Dans cette optique, la membre souhaite que Mme Clouner lui dise si CERT.be contrôle activement certaines entreprises vulnérables et, dans l'affirmative, si ces entreprises en sont informées. Ce contrôle éventuel concerne-t-il tous les secteurs ou seulement certains secteurs vitaux?

CERT.be a reçu 4 500 signalements en 2019, ce qui représente une augmentation considérable par rapport à la situation de 2018. Des chiffres sont-ils déjà disponibles pour 2020?

Mme Houtmeyers s'accorde à dire avec Mme Dierick que la sensibilisation est essentielle. Une campagne est en cours actuellement; d'autres campagnes sont-elles prévues?

Selon M. De Keersmaecker, les services policiers et judiciaires manquent de personnel et de moyens pour lutter de manière optimale contre la fraude sur internet. En est-il de même au service CERT.be?

M. Stefaan Van Hecke (Ecolo-Groen) renvoie à l'arrêt récemment rendu par la Cour de justice de l'Union européenne sur la rétention de données (affaires jointes C-511/18, C-512/18 et C-520/18, *La Quadrature du Net* et d'autres), qui indique, pour la deuxième fois, que la législation belge sur la rétention de données est contraire

Mevrouw Kathleen Verhelst (Open Vld) vraagt zich af of het ingevolge de coronacrisis toegenomen telewerk geen enorme boost heeft gegeven aan de mogelijkheid voor internetfraude.

Tevens wil ze weten of de privacywetgeving, in het bijzonder de AVG, niet dermate ver is doorgeslagen dat zij een belemmering vormt voor onderzoeken in het kader van internetfraude.

Hebben de sprekers zicht op de bedragen die betaald werden aan internetcriminelen? Staan deze in verhouding tot de "opbrengsten" daarvan? Blijven die gelden in Europa of gaan ze naar elders? Hoeveel wordt er gerecupereerd? Hebben zulke criminelen al straffen opgelegd gekregen, en over welke straffen gaat het dan?

Uit het betoog van de sprekers valt op te maken dat er wel degelijk ruimte is voor wetgevend ingrijpen.

De heer Baudewijns hield een pleidooi voor de invoering van een universitaire opleiding cybersecurity. Kan hij aangeven over welke talenten studenten, of toekomstige professionals in die richting, het best zouden beschikken?

Mevrouw Katrien Houtmeyers (N-VA) stelt dat wanneer CERT.be een melding ontvangt, het kwaad reeds is geschied; de betrachting moet zijn om zoveel mogelijk proactief op te treden. In dat opzicht wil het lid van mevrouw Clouner vernemen of CERT.be bepaalde kwetsbare ondernemingen actief opvolgt en, zo ja, of dat ook wordt teruggekoppeld naar die bedrijven. Heeft die eventuele monitoring betrekking op alle sectoren, dan wel slechts op bepaalde, vitale sectoren?

CERT.be ontving 4 500 meldingen in 2019, wat een zeer forste stijging inhoudt ten opzichte van de situatie in 2018. Zijn er reeds cijfers beschikbaar voor 2020?

Mevrouw Houtmeyers is het met mevrouw Dierick eens dat sensibilisering van essentieel belang is. Op dit moment loopt er een campagne; volgen er hierna nog campagnes?

Volgens de heer De Keersmaecker is er sprake van onvoldoende personeel en middelen bij politie- en gerechtelijke diensten om de internetfraude optimaal te bestrijden. Is dat ook het geval bij CERT.be?

De heer Stefaan Van Hecke (Ecolo-Groen) verwijst naar het recente arrest van het Hof van Justitie van de Europese Unie omtrent dataretentie (gevoegde zaken C-511/18, C-512/18 en C-520/18, *La Quadrature du Net e.a.*), waarin de Belgische wetgeving inzake dataretentie reeds voor de tweede maal strijdig werd bevonden met het

au droit européen. M. Van Hecke peut comprendre que la réduction du délai de rétention des données pourrait compliquer la recherche de certaines formes de criminalité (en particulier de criminalité classique), mais se demande si c'est également vrai pour la fraude sur internet. Généralement, cette forme de criminalité fait l'objet de constats rapides, l'enquête étant dès lors menée dans la foulée des faits. Qu'en pense M. Bogaert?

Plusieurs membres ont fait observer qu'il n'était pas idéal que la coopération avec les géants du web s'opère sur une base volontaire. M. Van Hecke a entendu des juges d'instruction tenir également des propos similaires. M. De Keersmaeker ou Mme Clouner peuvent-ils préciser en quoi cette coopération volontaire consiste exactement? Existe-t-il est accords verbaux ou également des contrats écrits? Y a-t-il des personnes de contact fixes?

Le membre ne s'oppose à la suggestion formulée par M. De Keersmaecker consistant à refuser l'accès au marché, en guise de sanction ultime, aux entreprises technologiques refusant systématiquement toute coopération. Comment la coopération avec les géants du web pourrait-elle être améliorée? Faudrait-il légiférer ou d'autres solutions existent-elles?

III. — **RÉPONSES DES ORATEURS**

M. Olivier Bogaert (FCCU) répond d'abord à la question de M. Freilich concernant l'évolution des chiffres entre 2018 et 2019. Il fait observer que les statistiques sont établies sur une base annuelle: à la fin de l'année, on examine combien de dossiers ont été ouverts sur un sujet donné. Cela permet de comparer les chiffres d'une année à l'autre. L'augmentation de quelque 30 % du nombre de cas entre 2018 et 2019 est liée à diverses formes de fraude sur le web (bitcoin, carte bancaire, etc.).

Il ne faut par ailleurs pas perdre de vue que tout citoyen ou toute entreprise victime d'une fraude sur internet ne le signale pas toujours aux autorités. À l'heure actuelle, les entreprises peuvent s'assurer contre la fraude sur le web, les entreprises qui y sont confrontées faisant alors appel à leur compagnie d'assurance en vue d'être partiellement indemnisées pour les dommages qu'elles ont subis, et étant moins enclines à s'adresser à la police. Les entreprises craignent en effet les atteintes qui seraient ainsi portées à leur image de marque.

Ce n'est qu'en 2021 que nous connaîtrons les chiffres de 2020 et que nous pourrons définir l'ampleur précise du pic enregistré en matière de fraude sur le web durant

Europees recht. De heer Van Hecke kan zich voorstellen dat een inkorting van de dataretentietermijn problematisch kan zijn voor de opsporing van bepaalde vormen van (met name klassieke) criminaliteit, maar vraagt zich af of dat ook het geval is voor internetfraude. Deze laatste vorm wordt immers meestal snel vastgesteld, waardoor het onderzoek ook snel na de feiten zal plaatsvinden. Wat is de mening van de heer Bogaert dienaangaande?

Verschillende sprekers hebben erop gewezen dat de vrijwillige aard van de samenwerking met de internetgiganten niet ideaal is. Gelijkaardige geluiden bereiken de heer Van Hecke ook vanwege de onderzoeksrechters. Kan de heer De Keersmaecker of mevrouw Clouner verduidelijken wat die vrijwillige samenwerking precies inhoudt? Bestaan er mondelinge overeenkomsten, of zijn er niettemin ook schriftelijke afspraken? Zijn er vaste contactpersonen?

Het lid is de suggestie van de heer De Keersmaecker om technologiebedrijven die systematisch weigeren mee te werken, de toegang tot de markt te ontzeggen, niet ongenegen, bij wijze van ultieme sanctie. Hoe zou de samenwerking met de internetgiganten kunnen worden verbeterd? Zou dit via wetgevend ingrijpen verlopen, of ook op andere manieren?

III. — **ANTWOORDEN VAN DE SPREKERS**

De heer Olivier Bogaert (FCCU) gaat eerst in op de vraag van de heer Freilich inzake de evolutie van de cijfers tussen 2018 en 2019. Hij wijst erop dat de statistieken op jaarbasis worden opgesteld; op het einde van het jaar wordt bekeken hoeveel dossiers er werden geopend omtrent een bepaald onderwerp. Aldus kunnen de cijfers van jaar tot jaar worden vergeleken. De stijging met ongeveer 30 % van het aantal gevallen tussen 2018 en 2019 slaat op verschillende vormen van internetfraude (bitcoin, bankkaart enz.).

Men moet ook in het achterhoofd houden dat niet elke burger of onderneming die slachtoffer is van internetfraude, dat meldt aan de autoriteiten. Ondernemingen kunnen zich tegenwoordig verzekeren tegen cyberfraude; bedrijven die daarmee te maken krijgen, zullen die verzekering inschakelen om een deel van de schade vergoed te krijgen, en zullen minder geneigd zijn om naar de politie te stappen. Ondernemingen zijn immers bevreesd voor de imagoschade die daarmee gepaard zou gaan.

Pas in 2021 zal men zicht hebben op de cijfers voor 2020 en dus ook de precieze omvang kennen van de piek in de internetfraude tijdens de coronacrisis.

la crise du coronavirus. Les fraudeurs présents sur le web ont clairement profité de l'augmentation du télétravail pour opérer. L'environnement IT des particuliers est généralement moins bien sécurisé que l'environnement IT des milieux professionnels. Il existe des logiciels qui permettent de s'introduire dans les systèmes et d'en extraire des données. On constate que les pirates informatiques visent de plus en plus les entreprises, non pas pour les bloquer, mais pour obtenir des informations sur des projets en cours ou sur de nouveaux produits, informations qui sont ensuite proposées à la vente aux entreprises concurrentes.

La réduction des délais de conservation des données pourrait bel et bien entraver ces enquêtes. Celles-ci génèrent des données qui doivent être analysées, pour lesquelles de nouvelles technologies ont parfois été utilisées ou dont la source doit être identifiée. Si le délai d'accès à ces données est trop court, cela posera évidemment un problème. À cet égard, il convient également de garder à l'esprit que les auteurs de ces faits utilisent parfois des outils qui les masquent ou les protègent. Les connexions VPN, par exemple, font en sorte que l'adresse IP visible est l'adresse d'un utilisateur tiers. Toutes ces choses doivent être analysées, ce qui prend évidemment du temps. Aussi la FCCU espère-t-elle que des délais de conservation des données plus longs seront maintenus et que ces délais correspondront aux délais en vigueur aujourd'hui en ce qui concerne la validité de l'enquête.

Sans pouvoir citer de montants, l'orateur confirme que, dans certains cas, les opérateurs ont facturé les coûts exposés dans le cadre de leur coopération à certaines enquêtes. Selon M. Bogaert, il conviendrait que, lorsqu'une demande judiciaire leur est adressée dans le cadre d'un cas de fraude sur le web, les opérateurs soient tenus d'y coopérer de la même manière que dans les dossiers classiques.

En réponse à la question de M. Freilich concernant les raisons pour lesquelles les fournisseurs d'accès à internet devraient offrir leurs services gratuitement à la police et à la justice alors que les opérateurs télécom facturent actuellement des coûts lorsqu'ils coopèrent aux écoutes téléphoniques, l'orateur indique qu'il vise essentiellement les données techniques concrètes dont certaines entreprises disposent. Les entreprises ne possèdent pas nécessairement les serveurs qui permettent aux clients de se connecter. Elles s'associent parfois, à cet effet, à de grandes entreprises qui proposent des services de serveurs. Et le fait est qu'il faut pouvoir

Internetfraudeurs hebben duidelijk geprofiteerd van het toegenomen telewerk om hun slag te slaan. De IT-omgeving bij de mensen thuis is veelal minder beveiligd dan op de werkvloer. Er bestaat software waarmee kan worden ingebroken in systemen om daaruit gegevens te halen. In toenemende mate ziet men dat internetpiraten hun pijlen richten op ondernemingen, niet zozeer om hen te blokkeren, maar wel om informatie te bekomen over lopende projecten of nieuwe producten, die dan te koop wordt aangeboden aan concurrerende ondernemingen.

Een inkorting van de dataretentietermijnen kan wel degelijk onderzoeken belemmeren. Die onderzoeken leveren gegevens op die moeten worden geanalyseerd, waarvoor soms nieuwe technologieën werden gebruikt of waarvan de bron moet worden geïdentificeerd. Als de termijn voor de toegang tot zulke gegevens te kort is, is dat uiteraard problematisch. In dat verband moet men ook rekening houden met het feit dat daders soms gebruik maken van instrumenten die hen verbergen of afschermen. VPN-verbindingen bijvoorbeeld zorgen ervoor dat het IP-adres dat zichtbaar is, datgene van een derde gebruiker is. Zulke zaken moeten allemaal worden onderzocht, wat uiteraard tijd vraagt. Daarom hoopt de FCCU toch langere dataretentietermijnen te kunnen behouden, die overeenkomen met de termijnen die vandaag van toepassing zijn inzake de geldigheid van een onderzoek.

Zonder bedragen te kunnen citeren, bevestigt de spreker dat er gevallen zijn geweest waarin operatoren de kosten die ze hebben gemaakt in het kader van hun medewerking aan onderzoeken, in rekening hebben gebracht. Het zou volgens de heer Bogaert aangewezen zijn dat operatoren, wanneer hen een gerechtelijk verzoek in het kader van een geval van internetfraude wordt voorgelegd, ertoe gehouden zouden zijn daaraan mee te werken, op dezelfde manier als dat het geval is in klassieke dossiers.

Op de vraag van de heer Freilich waarom men van internetproviders zou verlangen dat ze kosteloos hun diensten aanbieden aan politie en gerecht, terwijl telecomoperatoren vandaag toch kosten aanrekenen voor hun medewerking bij telefoontaps, antwoordt de spreker dat hij vooral doelt op concrete technische gegevens waarover bepaalde bedrijven beschikken. Ondernemingen bezitten niet noodzakelijk de servers die de klanten in staat stellen met hen verbinding te maken; soms gaan ze daarvoor in zee met grote bedrijven die serverdiensten aanbieden. Men moet echter kunnen rekenen op de medewerking van die bedrijven – de *hosts* – om te

compter sur la coopération de ces hébergeurs – *hosts* – pour savoir qui a conclu un contrat avec elles et à quel moment.

Quelques membres ont posé des questions à propos du rôle que l'Europe pourrait jouer. M. Bogaert plaide en faveur d'une coordination accrue, au niveau européen, qui permettrait 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. En effet, les législations nationales sont assez divergentes. Les commissions rogatoires prennent un temps considérable qui n'est pas toujours disponible, *a fortiori* si le délai de conservation des données devait encore être raccourci à l'avenir. Cette coordination entraînerait donc certainement une simplification qui serait la bienvenue.

Les fraudeurs visant les entreprises sur le web sont souvent basés en dehors de l'Europe. Il n'est cependant pas impossible, pour les autorités, de les rechercher et de les dénoncer auprès des autorités de leurs pays d'origine. Des procédures internationales sont parfois engagées, mais celles-ci sont toutefois très longues.

La Côte d'Ivoire est connue pour héberger des fraudeurs présents sur les sites de rencontre. Ce pays a mis en place une plateforme en ligne: la Plateforme de Lutte contre la Cybercriminalité (PLCC). La police belge peut inviter toute victime belge à y déposer plainte, mais aussi à remplir un formulaire sur la plateforme PLCC. Les autorités ivoiriennes peuvent dès lors également ouvrir une enquête, nos deux pays pouvant ensuite échanger des informations. Si les autorités ivoiriennes parviennent à retrouver un auteur, celui-ci sera poursuivi en Côte d'Ivoire. Cette coopération a déjà donné de bons résultats.

Les enquêtes relatives aux fraudes sur le web débouchent assez rarement sur des poursuites judiciaires en Belgique, de nombreux auteurs étant établis à l'étranger. Il arrive parfois que des fonds puissent être récupérés. Europol a mis en place une plateforme *No More Ransom* (*https://www.nomoreransom.org*). En plus des informations destinées aux entreprises, cette plateforme propose des outils de décryptage qui peuvent offrir une solution aux entreprises victimes de logiciels rançonneurs. Mais cela ne signifie pas que les auteurs, qui se trouvent parfois dans des pays comme l'Inde ou le Pakistan, seront arrêtés.

La sécurité des objets connectés soulève effectivement des questions. Le problème ne provient pas tant des fabricants que des utilisateurs (privés ou professionnels), en particulier en raison de la manière dont ces objets sont utilisés. L'orateur cite l'exemple d'un utilisateur qui

weten te komen wie wanneer met hen een overeenkomst heeft gesloten.

Enkele leden vroegen naar de rol die Europa zou kunnen opnemen. De heer Bogaert pleit voor meer coördinatie op Europees niveau, waardoor nationale politionele en gerechtelijke autoriteiten op het hele grondgebied van de EU de medewerking zouden kunnen opeisen van platformen om bepaalde concrete gegevens te verschaffen. Nationale wetgevingen zijn immers nogal uiteenlopend. Rogatoire commissies vergen veel tijd, die niet altijd voorhanden is, zeker niet wanneer de dataretentietermijn in de toekomst nog zou worden ingekort. Een dergelijke coördinatie zou dus zeker een welgekomen vereenvoudiging zijn.

De daders van internetfraude ten koste van ondernemingen zijn vaak gevestigd buiten Europa. Het is nochtans niet onmogelijk voor de autoriteiten om hen op te sporen en aan te geven bij de autoriteiten van hun land van oorsprong. Ook worden soms internationale procedures in gang gezet, die echter zeer tijdrovend zijn.

Ivoorkust is een bekende thuishaven van datingfraudeurs. Dat land heeft een onlineplatform opgezet, het *Plateforme de Lutte contre la Cybercriminalité* (PLCC). De Belgische politie kan het Belgische slachtoffer verzoeken een klacht in te dienen, maar ook een formulier in te vullen op het PLCC. Hierdoor kunnen de Ivoriaanse instanties eveneens een onderzoek opstarten. Beide landen kunnen dan informatie uitwisselen. Als de Ivoriaanse autoriteiten de dader kunnen aantreffen, zal hij worden vervolgd in dat land. Deze samenwerking heeft al tot goede resultaten geleid.

Onderzoeken naar internetfraude leiden relatief zelden tot rechtszaken in België, omdat veel daders in het buitenland zijn gevestigd. Soms gebeurt het dat gelden kunnen worden gerecupereerd. Europol heeft een platform *No More Ransom* in het leven geroepen (*https://www.nomoreransom.org*). Daarop zijn naast informatie voor bedrijven ook decryptietools te vinden, die een oplossing kunnen bieden voor bedrijven die het slachtoffer worden van *ransomware*. Maar dat wil nog niet zeggen dat de daders, die zich soms bevinden landen als India of Pakistan, worden gevat.

De veiligheid van geconnecteerde objecten roept inderdaad vragen op. Het probleem situeert zich echter niet zozeer bij de fabrikanten, maar vooral bij de (particuliere of professionele) gebruiker, en meer bepaald bij de manier waarop die de objecten gebruikt. De spreker

connecte une caméra de sécurité à son réseau wifi sans prévoir de normes de sécurité suffisantes. Dans ce cas, cet appareil constitue une source d'intrusion et dès lors un risque pour sa sécurité. Il est essentiel que tout utilisateur qui achète un objet connecté en lise attentivement le mode d'emploi et en modifie les modalités d'accès. Il faut savoir que tout objet pouvant être connecté au web est muni d'un numéro d'identification unique (adresse *media access control (Mac)*). Chaque utilisateur peut paramétrer son réseau wifi afin que seuls les appareils dont l'adresse MAC est reconnue puissent s'y connecter, à l'exclusion de tout autre appareil. Le projet Insecam, qui permet de visualiser en direct les images de centaines de caméras de sécurité non sécurisées partout dans le monde, illustre les dangers qu'il y a à ne pas suivre les précautions décrites ci-dessus. Toute caméra de sécurité piratée fournit un trésor d'informations aux candidats cambrioleurs.

Enfin, M. Bogaert a reçu quelques données de Google. Les robots Google chargés de lutter contre le *phishing* bloquent 240 millions d'emails par jour, dont 18 millions ont un rapport avec le COVID-19. Pour cela, il est fait appel à l'intelligence artificielle.

Mme Cécile Coppin (SPF Économie) évoque d'abord la demande de suggestions concrètes en vue de l'actualisation du cadre légal belge, demande formulée par plusieurs membres. L'oratrice ne peut en formuler aucune, pour la simple raison que les matières traitées par le SPF Économie relèvent des compétences de l'Union européenne. Conformément au principe du pays d'origine, l'entreprise n'est soumise qu'à la législation de l'État membre dans lequel elle est établie, et elle est contrôlée par les autorités de ce pays. Ce principe favorise la libre prestation des services au sein du marché intérieur.

Toute la procédure de notification et d'action (*notice and action*) et la désignation d'intermédiaires techniques de la société de l'information (plateforme, moteurs de recherche, etc.) feront l'objet d'un règlement européen, qui sera applicable directement et ne laissera plus guère de marge de manœuvre aux États membres. Nous devrons donc attendre de voir ce que nous réservera la Commission européenne en décembre 2020 dans le cadre du texte concernant les services numériques (*Digital Services Act*). Aucune grande plateforme n'étant établie en Belgique, notre pays sera de toute façon tributaire d'autres pays. Tel est toutefois aussi l'esprit de la coopération européenne: les autorités de contrôle des différents États doivent se faire mutuellement confiance et coopérer entre elles.

geeft het voorbeeld van een gebruiker die een beveiligingscamera verbindt met zijn wifinetwerk, zonder daaraan afdoende veiligheidsnormen toe te kennen, waardoor dit toestel een bron van intrusie en dus een veiligheidsrisico gaat vormen. Het is essentieel dat wie zich een geconnecteerd object aanschaft, de gebruiksaanwijzing grondig doorneemt en de toegangsmodaliteiten ervan wijzigt. Men moet weten dat elk object dat met het internet kan worden verbonden, uitgerust is met een uniek identificatienummer (*media access control* (MAC)-adres). Elke gebruiker kan zijn wifinetwerk zo instellen dat enkel toestellen waarvan het MAC-adres wordt herkend, daarmee verbinding kunnen maken, met uitsluiting van andere toestellen. Het Insecam-project, waarbij livebeelden van honderden onbeveiligde bewakingscamera's over de hele wereld te zien zijn, toont de gevaren aan van het niet-opvolgen van voormelde voorzorgen. Een gehackte beveiligingscamera levert een kandidaat-inbreker een schat aan informatie op.

De heer Bogaert ontving tot slot nog enkele gegevens van Google. Hun robots die vechten tegen *phishing* blokkeren elke dag 240 miljoen mails, waarvan 18 miljoen mails die te maken hebben met COVID-19. Hierbij wordt een beroep gedaan op artificiële intelligentie.

Mevrouw Cécile Coppin (FOD Economie) gaat vooreerst in op het verzoek van verschillende leden om concrete suggesties te formuleren inzake aanpassingen van het Belgische wettelijke kader. De spreekster heeft die niet, om de eenvoudige reden dat de materies die de FOD Economie behandelt, behoren tot de bevoegdheden van de EU. Overeenkomstig het oorsprongslandbeginsel is een onderneming alleen onderworpen aan de wetgeving van de lidstaat waarin ze is gevestigd, en wordt ze gecontroleerd door de autoriteiten van dat land. Dit beginsel bevordert de vrije dienstverrichting binnen de interne markt.

De hele *notice and action*-procedure en de aanwijzing van de technische tussenpersonen van de informatiemaatschappij (platformen, zoekmotoren enzovoort) zal het voorwerp uitmaken van een Europese verordening, die rechtstreekse werking zal hebben en de lidstaten nog amper manoeuvreerruimte zal laten. We zullen dus moeten afwachten waarmee de Europese Commissie in december 2020 op de proppen zal komen in het kader van de *Digital Services Act*. Geen enkele van de grote platformen is gevestigd in België, dus ons land zal in ieder geval aangewezen zijn op andere landen. Dat is echter ook de strekking van de Europese samenwerking: de controleoverheden in de verschillende landen moeten elkaar vertrouwen en met elkaar samenwerken.

Les différentes formes de coopération dans le cadre de la procédure "*notice and action*" seront donc également réglementées au niveau européen. L'Inspection économique n'applique pas la même approche aux différents prestataires de services. Pour l'instant, tout se passe encore sur une base volontaire. Les États membres ne peuvent pas, chacun de leur côté, adopter une législation distincte pour forcer les principales plates-formes à coopérer. L'Inspection dispose de personnes de contact auprès de ces plates-formes. Il existe également certaines procédures. Par exemple, dans les domaines de compétence (réglementés par l'UE) du SPF Économie, une adresse mail spécifique a été créée au niveau européen pour les demandes de collaboration concernant Facebook. Pour Google, il y a des personnes de contact spécifiques et on travaille avec un formulaire en ligne. Ces accords et procédures sont également importants du point de vue des plates-formes. Elles doivent en effet pouvoir être sûres que les demandes d'information émanent bel et bien d'autorités compétentes. C'est pourquoi le SPF Économie compte parmi ses agents des officiers de police judiciaire comme personnes de contact pour ces plates-formes.

Pour l'instant, le compte de superutilisateur n'existe encore que pour *2ememain.be*. À titre personnel, Mme Coppin est favorable à la poursuite du déploiement de ce système, étant donné que c'est beaucoup plus convivial que de travailler avec une adresse mail ou un formulaire en ligne. Les autorités de contrôle qui ont un compte de superutilisateur peuvent immédiatement épingler certains contenus, sous leur propre responsabilité, ce qui est une bonne chose.

Peut-on obliger des intermédiaires techniques à identifier les utilisateurs d'un service? Mme Coppin estime à cet égard qu'il convient de faire une distinction en fonction de la catégorie du service fourni. À l'heure actuelle, sur les sites de vente comme eBay, les utilisateurs sont priés de s'identifier. Le rôle de ces sites ne se limite pas à héberger des contenus: ils interviennent directement dans la transaction, une commission est prélevée sur les paiements, etc. Il est donc logique qu'ils identifient les utilisateurs, même si cela implique certains coûts supplémentaires (liés notamment à la mise en place d'une procédure d'authentification). Dans le cas de services où l'intermédiaire n'intervient pas dans la transaction mais se contente de réunir deux parties (un commerçant et un consommateur, ou deux professionnels, ou deux consommateurs), l'oratrice estime qu'il n'y a pas lieu d'imposer une obligation d'identification. De toute façon, cela doit être réglementé au niveau européen; les pays ne peuvent pas décider chacun de leur côté d'imposer des obligations supplémentaires aux prestataires de services qui agissent en qualité d'intermédiaires.

De verschillende samenwerkingsvormen in het kader van de *notice and action*-procedure zullen dus ook Europees worden geregeld. De Economische Inspectie hanteert niet dezelfde benaderingswijze voor de verschillende dienstenaanbieders. Alles gebeurt vooralsnog op vrijwillige basis. Individuele lidstaten kunnen niet elk apart wetgeving uitvaardigen om de grote platformen tot medewerking te dwingen. De Inspectie beschikt over contactpersonen bij die platformen. Er bestaan ook bepaalde procedures. Zo werd, wat de (door de EU geregelde) bevoegdheidsdomeinen van de FOD Economie betreft, op Europees niveau een specifiek e-mailadres ingesteld voor aanvragen tot medewerking die aan Facebook zijn gericht. Met Google zijn er specifieke contactpersonen en wordt er gewerkt met een onlineformulier. Die afspraken en procedures zijn ook belangrijk vanuit het perspectief van de platformen. Zij moeten er immers op kunnen vertrouwen dat de informatie-aanvragen wel degelijk afkomstig zijn van bevoegde autoriteiten. Om die reden telt de FOD Economie ook officieren van gerechtelijke politie in zijn rangen, die worden ingezet als contactpersoon voor die platformen.

Het *superuser*-account bestaat voorlopig enkel voor *2dehands.be*. Persoonlijk is mevrouw Coppin gewonnen voor een verdere uitrol van dit systeem; het is immers veel gebruiksvriendelijker dan werken met een e-mailadres of een onlineformulier. Controleoverheden die over een *superuser*-account beschikken, kunnen meteen bepaalde inhoud *taggen*, op eigen verantwoordelijkheid, wat een goede zaak is.

Kunnen we technische tussenpersonen ertoe verplichten de dienstafnemers te identificeren? Het komt mevrouw Coppin voor dat ter zake een onderscheid moet worden gemaakt naargelang van de categorie van dienstverrichting. Op marktplaatsen zoals eBay wordt gebruikers tegenwoordig gevraagd zich te identificeren. De rol van die marktplaatsen is niet beperkt tot het hosten van inhoud; zij komen rechtstreeks tussenbeide in de transactie, er wordt een commissie geheven op betalingen enzovoort. Het is dus logisch dat ze gebruikers identificeren, zelfs al houdt dat bepaalde meerkosten in (bijvoorbeeld de invoering van een authenticatieprocedure). Voor diensten waarbij de tussenpersoon niet tussenkomt in de transactie maar zich ertoe beperkt twee partijen (een handelaar en een consument, of twee handelaars, of twee consumenten) met elkaar in contact te brengen, is een identificatieverplichting volgens de spreekster niet aangewezen. Sowieso moet dit op Europees niveau worden geregeld; landen kunnen niet elk apart beslissen bijkomende verplichtingen op te leggen aan als tussenpersoon optredende dienstenleveranciers.

La question a été posée de savoir si l'autorité d'un État membre, à laquelle une demande est adressée par une autorité d'un autre État membre dans le cadre de la coopération régie par le règlement CPC, est libre de lui donner suite ou non. L'oratrice répond par la négative: le mécanisme établi par le règlement CPC prévoit une obligation de réponse pour la première autorité. Si – à titre d'exemple hypothétique – un site web allemand agit en contradiction avec la législation belge en matière de droit de la consommation, le SPF Économie ne peut pas intervenir lui-même. Il doit pour ce faire envoyer une demande à son homologue allemand via la plateforme CPC. Cet homologue ne peut ignorer cette demande ou la rejeter simplement en déclarant que le site en question ne porte pas préjudice aux consommateurs allemands. L'autorité allemande doit démontrer que le site n'enfreint pas la législation allemande (ce qui est possible, même s'il s'agit d'une matière qui est soumise à la réglementation européenne: en effet, les directives européennes fixent parfois des normes minimales et laissent aux États membres la liberté d'imposer un niveau de protection des consommateurs plus élevé lors de leur transposition). L'oratrice souligne par ailleurs que cette coopération CPC fonctionne bien.

Si, dans l'exemple ci-dessus, l'Allemagne estime qu'il n'y a pas eu d'infraction à sa législation mais que la Belgique soutient pour sa part que la protection des consommateurs est néanmoins compromise, la directive sur le commerce électronique prévoit que notre pays peut toujours prendre des mesures contre le site web concerné sans enfreindre les règles du marché intérieur. Notre pays doit alors démontrer qu'il a épuisé toutes les autres possibilités et qu'il existe un risque de préjudice collectif pour le consommateur belge, à la suite de quoi la Commission européenne en est informée. Cette procédure a déjà été appliquée à la vente en ligne de billets de concert par des prestataires de services néerlandais, un domaine dans lequel les règles sont plus strictes en Belgique qu'aux Pays-Bas.

Par ailleurs, l'Inspection économique n'intervient pas seulement après les notifications, mais agit également de manière proactive. Étant donné que l'Internet est par essence international, il existe des actions menées au niveau européen. Par exemple, au cours des journées "*sweepdays*", qui sont organisées chaque année, certaines pratiques douteuses sur Internet sont combattues de façon concertée et avec l'assistance mutuelle des pays participants, et ce, pendant une semaine. C'est un exemple d'action proactive. Par ailleurs, l'oratrice précise que l'Inspection économique peut également intervenir de manière proactive à la demande du ministre.

Toutes les autorités de contrôle en Europe disposent-elles des mêmes instruments? Mme Coppin répond par

De vraag werd gesteld of de autoriteit van een lidstaat waaraan in het kader van de samenwerking in het licht van de CPC-Verordening een verzoek wordt gericht door een autoriteit in een andere lidstaat, over de vrijheid beschikt daaraan al dan niet gevolg te geven. De spreekster antwoordt ontkennend; het mechanisme ingesteld door de CPC-Verordening voorziet in een verplichting van die eerste autoriteit om te reageren. Als – bij wijze van hypothetisch voorbeeld – een Duitse website handelt in strijd met de Belgische consumentenwetgeving, mag de FOD Economie niet zelf ingrijpen. Hij moet daartoe, via het CPC-platform, een verzoek richten aan zijn Duitse evenknie. Die laatste mag dat verzoek niet negeren of er zich vanaf maken door te stellen dat de site Duitse consumenten niet benadeelt. De Duitse autoriteit moet aantonen dat de website geen inbreuk uitmaakt op de Duitse wetgeving (die mogelijkheid bestaat, niettegenstaande het feit dat deze materie het voorwerp uitmaakt van Europese regelgeving; de EU-richtlijnen leggen soms minimumstandaarden vast en laten de lidstaten vrij bij de omzetting een hoger niveau van consumentenbescherming op te leggen). Die CPC-samenwerking verloopt goed, aldus de spreekster.

Wanneer, in voormeld voorbeeld, Duitsland meent dat zijn wetgeving niet is geschonden en België volhoudt dat de consumentenbescherming toch in het gedrang komt, dan voorziet de richtlijn inzake Elektronische Handel erin dat ons land alsnog kan optreden tegen de website, zonder dat dit ingaat tegen de regels van de interne markt. Ons land moet dan aantonen dat het alle andere mogelijkheden heeft uitgeput en dat er een collectief nadeel dreigt voor de Belgische consument. De Europese Commissie wordt daarvan op de hoogte gebracht. Deze procedure werd reeds toegepast bij de onlineverkoop van concerttickets door Nederlandse dienstenleveranciers, waarvoor in België strengere regels gelden dan in Nederland.

De Economische Inspectie treedt niet alleen op na meldingen, maar handelt ook proactief. Aangezien het internet in wezen internationaal is, zijn er Europese acties. Zo worden jaarlijks zogenaamde *sweepdays* georganiseerd, waarbij gedurende een week bepaalde misleidende praktijken op het internet gezamenlijk en met wederzijdse bijstand tussen de deelnemende landen worden aangepakt. Dit is een voorbeeld van een proactieve actie. Ook op verzoek van de minister kan de Inspectie proactief optreden.

Hebben alle toezichthoudende overheden in Europa dezelfde instrumenten te hunner beschikking?

l'affirmative. Les différentes autorités échangent des bonnes pratiques, dans le domaine des méthodes de recherche et d'automatisation par exemple. Il existe une banque de données de bonnes pratiques.

L'Inspection économique a l'intention d'utiliser l'intelligence artificielle afin de faciliter les contrôles.

Les initiatives Point de contact et *Safeonweb.be* n'ont pas la même finalité. La première est un guichet central visant à réunir les signalements et les plaintes de victimes tandis que *Safeonweb.be* tend à sensibiliser les citoyens au sujet de la sécurité sur Internet, et ainsi à empêcher qu'ils deviennent des victimes. Il n'est dès lors pas question de double emploi, mais plutôt de complémentarité. Chaque personne qui effectue une dénonciation par le biais du Point de contact reçoit d'ailleurs une réponse adaptée à son profil accompagnée de conseils.

Toujours dans le domaine de la sensibilisation, le SPF Économie organise des campagnes annuelles dans le cadre de projets internationaux. Le SPF participe ainsi chaque année en mars au Mois de la prévention de la fraude, autour duquel s'articule toute une campagne. Le SPF Économie a encore diffusé récemment un spot radio afin de mettre en garde contre les pièges des criminels qui opèrent sur Internet. Il y a quelques années, il y a eu aussi la campagne tropbeaupouretrevrai.be. La sensibilisation est et demeure dès lors absolument nécessaire, d'autant plus qu'il est extrêmement difficile de détecter les auteurs d'une fraude sur Internet.

Mme Phédra Clouner (CCB) constate que nombre de personnes utilisent l'adresse *suspect@safeonweb.be*, comme en témoigne le fait que plus de 2 millions de messages ont déjà été reçus à cette adresse en 2020, avec des pics en mars et avril de 300 000 messages par mois. Lors de chaque campagne de sensibilisation, le CCB fait également évaluer son impact par une entreprise spécialisée; il ressort de ces analyses que le CCB atteint annuellement entre 1 et 1,5 million de citoyens en moyenne, ce qui est loin d'être négligeable.

En raison du nombre élevé de signalements, les moyens disponibles ne permettent pas au CCB d'envoyer une réponse personnalisée à chaque citoyen qui a fait un signalement. Ce qui joue également un rôle à cet égard, c'est le fait que les fournisseurs de services, tels que Google et Microsoft, mettent souvent un certain temps avant de fermer des sites pratiquant le *phishing*. Le CCB n'en est pas non plus informé; il vérifie ultérieurement d'initiative si l'un ou l'autre site web signalé a déjà été bloqué. Depuis peu, le CCB dispose d'un système beaucoup plus performant pour ce faire.

Mevrouw Coppin antwoordt bevestigend. De diverse autoriteiten wisselen goede praktijken uit, bijvoorbeeld op het vlak van zoek- en automatiseringsmethodes. Er bestaat een databank van *best practices*.

De Economische Inspectie is van plan artificiële intelligentie in te zetten om de controles te vergemakkelijken.

De initiatieven Meldpunt en *Safeonweb.be* hebben een uiteenlopende doelstelling. Het eerste is een centraal loket om meldingen en klachten van slachtoffers te verzamelen; *Safeonweb.be* daarentegen streeft ernaar burgers te sensibiliseren omtrent internetveiligheid, en aldus te voorkomen dat ze slachtoffer worden. Er is dus geen sprake van een overlapping, eerder van een complementariteit. Elkeen die een aangifte doet via het Meldpunt, ontvangt overigens een aan zijn profiel aangepast antwoord met adviezen.

Nog op het vlak van sensibilisering organiseert de FOD Economie jaarlijkse campagnes in het kader van internationale projecten. Zo neemt de FOD elk jaar in maart deel aan de *Fraud Prevention Month*, waarrond dan een hele campagne wordt uitgerold. Recent verspreidde de FOD Economie nog een radiospot om mensen te waarschuwen niet in de val van internetcriminelen te lopen. Enkele jaren terug was er de campagne temooiomwaartezijn.be. Sensibilisering is en blijft dus absoluut nodig, temeer daar het uiterst moeilijk is de daders van internetfraude op te sporen.

Mevrouw Phédra Clouner (CCB) stelt vast dat heel wat mensen hun weg weten te vinden naar het adres *verdacht@safeonweb.be*, getuige daarvan het feit dat er in 2020 reeds meer dan 2 miljoen berichten werden ontvangen op dat adres, met pieken in maart en april van 300 000 berichten per maand. Bij elke sensibiliseringscampagne laat het CCB ook een gespecialiseerde onderneming de impact daarvan evalueren; die analyses leren dat het CCB jaarlijks gemiddeld tussen 1 en 1,5 miljoen burgers bereikt, wat verre van slecht is.

De beschikbare middelen in combinatie met het hoge aantal meldingen staan het CCB niet toe elke melder een gepersonaliseerd antwoord te sturen. Wat daarbij ook een rol speelt, is het feit dat dienstenaanbieders zoals Google en Microsoft er vaak een tijdje over doen om *phishing*-websites offline te halen. Het CCB ontvangt daaromtrent ook geen melding; het verifieert achteraf op eigen initiatief of deze of gene gemelde website reeds geblokkeerd is. Sinds kort beschikt het CCB in dit verband over een iets performanter systeem.

Une des pistes pour encore accroître l'efficacité de ce système est de travailler avec des listes noires de sites web qui sont manifestement frauduleux. L'utilisateur qui saisirait l'URL d'un tel site web recevrait un avertissement automatique. Le CCB travaille actuellement à un système de ce genre.

Concernant la mise en œuvre opérationnelle du CCB, M. D'Amico a rappelé les trois objectifs stratégiques que le gouvernement Michel proposait dans son accord de gouvernement, à savoir (i) garantir un cyberespace sûr et sécurisé dans le respect des droits fondamentaux et des valeurs d'une société moderne; (ii) garantir une sécurisation et une protection optimales des infrastructures critiques, du potentiel scientifique et économique et des systèmes publics contre la cybermenace, et (iii) le développement de capacités propres de cybersécurité pour une politique de sécurité indépendante et une réaction adaptée face aux incidents de sécurité. Au cours des cinq dernières années, le CCB s'est employé à réaliser ces objectifs. Il a développé une excellente collaboration avec tous les autres acteurs compétents, en ce compris la police et la justice.

Bien que le Point de contact et *Safeonweb.be* aient des objectifs différents, des discussions ont eu lieu avec le SPF Économie afin d'examiner quelle collaboration était possible dans le domaine de la sensibilisation et du workflow. La finalité de *Safeonweb.be* est de fournir des informations; il vise à protéger les citoyens contre la cybercriminalité en leur enseignant les réflexes adéquats.

Les objets connectés sont actuellement les instruments de prédilection des cybercriminels. Ces derniers utilisent ces objets pour mener des attaques par déni de service (attaques DDoS ou *Denial of Service attack*) car ces appareils ne sont généralement pas sécurisés par leurs utilisateurs. Comme M. Bogaert l'a déjà signalé, nombre de consommateurs conservent la configuration standard, ce qui rend les appareils vulnérables aux pirates informatiques. Le règlement sur la cybersécurité[3], qui entrera en vigueur en 2021, vise notamment à garantir un niveau adéquat de cybersécurité des produits TIC, services TIC et processus TIC dans l'Union en prévoyant un cadre pour la mise en place de schémas européens de certification de cybersécurité. Des schémas de certification s'appliqueront ainsi aux objets connectés, ce qui devrait remédier au problème précité. Tant le CCB que le SPF Économie joueront un rôle majeur dans la mise en œuvre du règlement sur la cybersécurité en Europe.

[3] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité).

Een van de pistes om de efficiëntie van dit systeem nog te verhogen, is te werken met *blacklists* van websites die aantoonbaar frauduleus zijn. De gebruiker die de URL van zo'n website intypt, zou dan een automatische waarschuwing krijgen. Het CCB werkt momenteel aan een dergelijk systeem.

Wat de operationele implementatie van het CCB betreft, herinnerde de heer D'Amico aan de drie strategische doelstellingen die de regering-Michel in het regeerakkoord vooropstelde, namelijk (i) streven naar een veilige en betrouwbare cyberspace met respect voor de fundamentele rechten en waarden van de moderne samenleving; (ii) streven naar een optimale beveiliging en bescherming van kritieke infrastructuren, het wetenschappelijk en economisch potentieel en overheidssystemen tegen de cyberdreiging; en (iii) de ontwikkeling van eigen cybersecuritycapaciteiten voor een onafhankelijk veiligheidsbeleid en een gepaste reactie op veiligheidsincidenten. Het CCB heeft de afgelopen vijf jaar hard gewerkt aan de realisatie van die doelstellingen. Het ontwikkelde een uitstekende samenwerking met alle andere bevoegde actoren, inclusief politie en justitie.

Hoewel het Meldpunt en *Safeonweb.be* uiteenlopende doelen nastreven, zijn er wel gesprekken met de FOD Economie geweest om te bekijken welke samenwerking mogelijk is op het vlak van de sensibilisering en de workflow. *Safeonweb.be* beoogt informatie te verstrekken; het wil de burgers beschermen tegen cybercriminaliteit door hen de juiste reflexen bij te brengen.

Geconnecteerde objecten zijn tegenwoordig een geliefkoosd instrument van cybercriminelen. Ze gebruiken ze voor *distributed-denial-of-service*-aanvallen (DDoS-aanvallen), vermits deze apparaten veelal niet beveiligd zijn door hun gebruikers. Zoals de heer Bogaert al opmerkte, behouden veel consumenten de standaardconfiguratie, wat de toestellen kwetsbaar maakt voor hackers. In juni 2021 zal de zogenaamde Cyberbeveiligingsverordening[3] in werking treden, die onder meer tot doel heeft een toereikend cyberbeveiligingsniveau van ICT-producten, -diensten en -processen in de EU te waarborgen door het bepalen van een kader voor de vaststelling van Europese cyberbeveiligingscertificeringsregelingen. Er zullen dus certificeringsregelingen komen voor geconnecteerde objecten. Dit moet tegemoetkomen aan voormeld probleem. Zowel het CCB als de FOD Economie zullen een belangrijke rol spelen in de implementering van de Cyberbeveiligingsverordening in Europa.

[3] Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013.

Il ne faut pas sous-estimer l'importance de la sensibilisation. Le CCB part du principe que dans le domaine de la cybersécurité, l'humain est le maillon fort, et non le maillon faible. C'est pourquoi le CCB investit beaucoup dans la sensibilisation. Il souscrit pleinement au Mois européen de la cybersécurité, une campagne de sensibilisation européenne organisée chaque année en octobre. Comme indiqué précédemment, le CCB touche jusqu'à 1,5 million de citoyens chaque année. Cette année, le CCB a publié une vidéo très largement partagée sur l'authentification multifacteurs, une méthode permettant de vérifier l'authenticité d'un utilisateur à l'aide de plusieurs facteurs et, partant, de renforcer la sécurité du contrôle d'accès. Le CCB mise fortement sur cette technologie et recommande l'utilisation de méthodes d'authentification fortes comme *itsme*. Il serait judicieux d'élaborer une stratégie européenne globale en la matière.

Het belang van sensibilisering kan niet worden overschat. Bij het CCB vertrekt men van de idee dat de mens de sterke – niet de zwakke – schakel is in het verhaal van cyberveiligheid. Het CCB investeert dan ook fors in sensibilisering. Het zet volop in op de Europese Maand van de Cyberveiligheid, een EU-sensibiliseringscampagne die elk jaar in oktober plaatsvindt. Zoals gezegd, bereikt het CCB elk jaar tot 1,5 miljoen burgers. Dit jaar heeft het CCB een zeer ruim gedeelde video gepost over multifactorauthenticatie, d.i. de methode om de authenticiteit van een gebruiker te verifiëren door meerdere factoren, waardoor de beveiliging bij toegangscontrole wordt aangescherpt. Het CCB zet hier sterk op in en beveelt sterke authenticatiemethodes zoals *itsme* aan. Het zou goed zijn mocht er hieromtrent een alomvattende Europese aanpak bestaan.

Le CCB dispose de ressources suffisantes pour la sensibilisation et les utilise pleinement, en collaboration ou non avec la Coalition pour lutter contre la cybercriminalité (*Cyber Security Coalition*). Il s'agit d'un partenariat au sein duquel 500 acteurs issus du monde universitaire, des organismes publics et du secteur privé conjuguent leurs forces pour lutter contre la cybercriminalité.

Het CCB beschikt over voldoende middelen voor sensibilisering, en maakt daarvan ook volop gebruik, al dan niet in samenwerking met de *Cyber Security Coalition*. Dat is een partnerschap waarbij 500 spelers uit de academische wereld, openbare instanties en de private sector de krachten te bundelen in de strijd tegen cybercriminaliteit.

Comme indiqué précédemment, CERT.be a enregistré environ 4 800 signalements en 2019. Ce nombre est plus élevé que les années précédentes, ce qui s'explique principalement par le fait que tant le CCB (qui n'existe que depuis 2015) que CERT.be (qui a été repris par le CCB en 2017) ont fortement gagné en notoriété ces derniers temps. Toutefois, ces 4 800 signalements ne sont que la pointe de l'iceberg, tous les incidents de cybersécurité n'étant pas signalés par crainte de porter atteinte à sa réputation, notamment.

Zoals eerder gezegd, telde men in 2019 ongeveer 4 800 meldingen op CERT.be. Dat aantal ligt hoger dan in de voorgaande jaren, wat vooral te verklaren is door het feit dat zowel het CCB (dat nog maar sinds 2015 bestaat) als CERT.be (dat in 2017 door het CCB werd overgenomen) de afgelopen tijd sterk aan bekendheid hebben gewonnen. Nochtans zijn die 4 800 meldingen maar het topje van de ijsberg, omdat lang niet alle cyberveiligheidsincidenten worden aangegeven, onder meer uit vrees voor reputatieschade.

Mme Houtmeyers a demandé si CERT.be surveille certaines entreprises. Ce n'est pas le cas, du moins pas de manière intrusive. Cependant, CERT.be dispose de nombreuses sources d'information (commerciales, accessibles) permettant d'identifier les systèmes vulnérables ou infectés. CERT.be avertit les citoyens et les organisations dont les systèmes sont infectés, par le biais notamment des fournisseurs d'accès à Internet. Dans des cas spécifiques, et pour autant qu'il s'agisse d'incidents susceptibles d'affecter des secteurs vitaux, des infrastructures critiques ou des fournisseurs de services essentiels, un suivi effectif est mis en place, en coopération avec la police et la justice.

Mevrouw Houtmeyers vroeg of CERT.be bepaalde ondernemingen monitort. Dat is niet het geval, althans niet op intrusieve wijze. Wel beschikt CERT.be over talloze (commerciële, toegankelijke) informatiebronnen, waardoor kwetsbare of geïnfecteerde systemen kunnen worden opgespoord. Onder meer via de internetproviders waarschuwt CERT.be burgers en organisaties met geïnfecteerde systemen. In specifieke gevallen, in zoverre het incidenten betreft die bepaalde vitale sectoren, kritische infrastructuren of aanbieders van essentiële diensten kunnen treffen, wordt er wel effectief gemonitord, in samenwerking met de politie en de justitie.

Les actions concrètes de protection proposées par CERT.be s'adressent aux secteurs, infrastructures et prestataires précités, ainsi qu'au potentiel scientifique et économique et aux organismes publics. Cela ne

Concrete beschermingsacties van CERT.be zijn gericht op voornoemde sectoren, infrastructuren en aanbieders, evenals op het wetenschappelijk en economisch potentieel en overheidsinstellingen. Dat wil

signifie toutefois nullement que CERT.be reste sourd aux demandes d'aide émanant d'autres organisations; comme l'a également souligné M. Baudewijns, CERT.be intervient souvent auprès d'organisations qui ne font pas partie des secteurs énumérés.

En ce qui concerne la coopération volontaire avec les différents acteurs, l'oratrice indique que le CCB y a très souvent recours – faute d'une autre base plus contraignante. Cette coopération n'est pas mauvaise mais pourrait néanmoins être plus efficace. Pour certains acteurs, elle implique un investissement parfois considérable en temps et en moyens. Lorsque le CCB constate par exemple l'existence d'un problème affectant spécifiquement les adresses IP dans le giron d'un grand opérateur, celui-ci est censé avertir ses clients, ce qui nécessite un sérieux effort de sa part. Il arrive que ces opérateurs coopèrent mais il arrive aussi qu'ils ne coopèrent pas. Selon Mme Clouner, il serait déjà utile de prévoir un incitant pour encourager ces acteurs à coopérer, même si une obligation légale serait bien entendu préférable.

M. Robrecht De Keersmaecker (parquet général d'Anvers) ne voit pas l'intérêt de la piste proposée par M. Gilissen, qui consisterait à intercepter les logiciels de rançon en se basant sur des modèles et à les bloquer au niveau des fournisseurs. Il existe des logiciels de rançon qui permettent à l'utilisateur de choisir de nombreux paramètres: l'algorithme de cryptage, l'adresse Bitcoin à laquelle la "rançon" sera envoyée, le message électronique, les destinataires, etc. À moins d'utiliser des URL connues, les techniques de détection actuelles ne permettent pas de déterminer s'il existe un même modèle sous-jacent derrière tous ces paramètres. De plus, la prise de connaissance d'une communication au niveau du fournisseur enfreint le principe du secret de la communication. En outre, le chiffrement de bout en bout (*end-to-end encryption*) permet à peine aux fournisseurs de savoir quelles données circulent sur leurs réseaux.

S'il y a bien une chose dans laquelle croit M. De Keersmaecker, c'est dans l'érosion de la confiance dans le *darknet*. Les initiatives menées à cet effet doivent être mûrement réfléchies et organisées dans un cadre légal. On pourrait par exemple songer à des initiatives légales habilitant les instances compétentes à inonder les plateformes présentes sur le *darknet* avec de faux messages ou de fausses offres, afin d'y semer la pagaille.

Le récent arrêt de la Cour de justice de l'Union européenne (affaires jointes C-511/18, C-512/18 et C-520/18, *La Quadrature du Net* e. a.) est muet quant aux délais de conservation des données relatives au trafic et à la localisation; la Cour déclare simplement que les fournisseurs ne peuvent pas être obligés de conserver ces données.

overigens geenszins zeggen dat CERT.be doof blijft voor hulpverzoeken vanuit andere organisaties; zoals ook de heer Baudewijns al aangaf, komt CERT.be vaak tussen bij organisaties die geen deel uitmaken van de opgesomde sectoren.

Wat de vrijwillige samenwerking met de verschillende spelers betreft, geeft de spreekster aan dat het CCB daarop zeer vaak een beroep doet – bij gebreke aan een andere, dwingender basis. Deze samenwerking verloopt niet slecht, maar zou toch efficiënter kunnen. Voor bepaalde actoren impliceert de medewerking een soms aanzienlijke investering van tijd en middelen. Wanneer het CCB bijvoorbeeld vaststelt dat er een probleem is dat specifiek de IP-adressen 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. Het voorzien in een stimulans voor die actoren om mee te werken, zou volgens mevrouw Clouner al soelaas bieden; een wettelijke verplichting zou uiteraard nog beter zijn.

De heer Robrecht De Keersmaecker (parket-generaal te Antwerpen) ziet geen heil in de door de heer Gilissen aangereikte piste om *ransomware* via patronen te onderscheppen en te blokkeren op providerniveau. Er bestaat *ransomware* die de gebruiker ertoe in staat stelt tal van parameters te kiezen: het encryptiealgoritme, het bitcoinadres waarop het "losgeld" zal worden ontvangen, de mailboodschap, de bestemmelingen geadresseerden enzovoort. Tenzij hiervoor gekende URL's worden gebruikt, kan met de huidige opsporingstechnieken niet worden achterhaald of achter al die zaken eenzelfde patroon zit. Daarenboven is het zo dat men bij het kennisnemen van communicatie op providerniveau stoot op het communicatiegeheim. Door *end-to-end*-encryptie kunnen providers bovendien amper nog weten welke data er over hun netwerken lopen.

Waar de heer De Keersmaecker wel in gelooft, is het onderuithalen van het vertrouwen op het *darknet*. Dit moet weloverwogen en binnen een wettelijk kader gebeuren. Zo kan worden gedacht aan wettelijke initiatieven die de bevoegde instanties ertoe in staat zouden stellen platformen op het *darknet* te overspoelen met valse berichten of vals aanbod, zodat men op die illegale platformen door de bomen het bos niet meer ziet.

Het recente arrest van het Hof van Justitie van de EU (gevoegde zaken C-511/18, C-512/18 en C-520/18, *La Quadrature du Net e.a.*) zegt niets over termijnen inzake verkeers- en lokalisatiegegevens; het Hof stelt gewoon dat men providers niet mag verplichten die gegevens bij te houden. Voor IP-adressen en gebruikersgegevens mag

Les adresses IP et les données des utilisateurs peuvent être conservées, mais seulement pendant une période limitée. L'orateur évoque le problème des connexions VPN, qui obligent parfois les enquêteurs à sauter d'une adresse IP à l'autre comme s'ils suivaient une piste de cailloux dans une forêt, avec la période de rétention des données comme une épée de Damoclès au-dessus de leur tête. Les enquêteurs doivent presque espérer que les criminels ont été désinvoltes une fois et n'ont pas utilisé de connexion VPN afin de connaître leur véritable adresse IP. Toutefois, si le délai est trop long, les autorités judiciaires ne peuvent plus contacter le fournisseur pour connaître l'identité sous-jacente. L'orateur s'attend à ce que le jugement oblige les services de police et de justice à travailler différemment – c'est-à-dire de manière plus moderne – dans le cadre des enquêtes téléphoniques. Selon lui, un problème particulièrement préoccupant est que les requêtes en temps réel seront limitées aux enquêtes liées au terrorisme. À l'avenir, il ne sera plus possible de localiser en temps réel le téléphone portable d'un adolescent suicidaire en fuite. Cette question devra être examinée au sein du groupe de travail sur la conservation des données.

Comment se passe la coopération volontaire avec les opérateurs? Le FCCU travaille avec des personnes de contact uniques qui envoient toutes les requêtes aux opérateurs. Les opérateurs peuvent ainsi s'assurer que ces demandes sont fiables. Le problème de la coopération volontaire est que les opérateurs se posent parfois eux-mêmes en juges et décident de leur propre chef d'accéder ou non à l'une ou l'autre requête. C'est parfois compréhensible; dans des pays comme les États-Unis, la liberté d'expression est interprétée de manière plus absolue qu'en Belgique, si bien que certaines demandes sont parfois problématiques pour les plateformes qui y sont établies.

Des négociations discrètes avec les fournisseurs sont menées en permanence; à l'heure actuelle, par exemple, c'est le cas pour certains nouveaux fournisseurs de taille plus modeste. Le message des autorités judiciaires est que, sur la base de la jurisprudence Yahoo et Skype précitée, elles pourraient obliger les fournisseurs à communiquer certains éléments, mais qu'elles préfèrent néanmoins pouvoir les obtenir sur une base volontaire, sans citation, moyennant certaines conditions. L'expérience montre que cela fonctionne souvent, mais sans aucune garantie. Selon l'orateur, une espèce de label de qualité pour les ISP pourrait être envisagée, par analogie avec la sécurité alimentaire. Les fournisseurs pourraient alors obtenir un label de confiance à condition qu'ils acceptent, d'une manière compatible avec le RGPD, d'obtenir l'accord de leurs clients pour que leurs données soient conservées pendant un certain temps

dat wel, maar slechts voor een beperkte tijd. De spreker verwijst ter zake naar het probleem van de VPN-verbindingen, die speurders soms ertoe verplichten van IP-adres naar IP-adres te springen als waren het kruimeltjes in een bos, en dit met de datarentietermijn als zwaard van Damocles boven het hoofd. De speurders moeten bijna hopen dat de criminelen een keer nonchalant zijn geweest en geen VPN-verbinding hebben gebruikt, om het échte IP-adres te kennen. Als dat echter te ver in de tijd ligt, kunnen de gerechtelijke autoriteiten niet meer bij de provider terecht om de onderliggende identiteit te achterhalen. De spreker verwacht dat het arrest de politie- en gerechtelijke diensten ertoe zal dwingen anders – lees: moderner – te gaan werken bij telefonieonderzoeken. Bijzonder problematisch is volgens hem dat *realtime*-bevragingen zullen worden beperkt tot terrorismeonderzoeken. Het zal in de toekomst niet meer mogelijk zijn in *realtime* de gsm te lokaliseren van een weggelopen suïcidale tiener. Dit zal moeten worden bekeken binnen de werkgroep dataretentie.

Hoe verloopt de vrijwillige samenwerking met de operatoren? Er wordt gewerkt met unieke contactpersonen van waaruit alle verzoeken voor de operatoren worden verzonden. Op die manier kunnen de operatoren erop vertrouwen dat die verzoeken betrouwbaar zijn. Het probleem met de vrijwillige samenwerking is dat de operatoren soms zelf voor rechter spelen en op eigen houtje beslissen dat ze aan deze of gene vraag al dan niet gevolg geven. Soms is dit ook begrijpelijk; in landen zoals de Verenigde Staten wordt de vrijheid van meningsuiting absoluter geïnterpreteerd dan in België, wat maakt dat aldaar gevestigde platformen soms problemen hebben met bepaalde verzoeken.

Er wordt voortdurend discreet onderhandeld met providers; thans is dat bijvoorbeeld het geval met enkele kleinere, nieuwe providers. De boodschap vanwege de gerechtelijke diensten is daarbij dat zij, op grond van de eerder aangehaalde cassatierechtspraak inzake Yahoo en Skype, de providers zouden kunnen dwingen bepaalde zaken vrij te geven, maar dat ze niettemin verkiezen dit op vrijwillige basis, zonder dagvaarding, te kunnen afhandelen, onder bepaalde voorwaarden. De ervaring leert dat dit vaak werkt, maar het biedt geen garanties. Volgens de spreker kan worden overwogen, naar analogie met de voedselveiligheid, een soort van kwaliteitslabel voor ISP's in te voeren. Providers zouden dan een *trusted*-label kunnen krijgen wanneer ze er ermee instemmen, op een wijze die compatibel is met de AVG, het akkoord vanwege hun klanten te bekomen dat hun gegevens gedurende een bepaalde tijd zullen worden

et puissent être partagées avec les services répressifs à la demande d'une autorité compétente.

À la demande de plusieurs membres, M. De Keersmaecker a fait un certain nombre de suggestions de modifications concrètes du cadre juridique. Par exemple, on pourrait œuvrer à une uniformisation des articles 46*bis* et 46*quater* du Code d'instruction criminelle en partant du principe que tout fournisseur de services de télécommunications doit pouvoir partager certaines données de ses clients sur la base d'une requête. En outre, un durcissement de l'arsenal répressif devrait également être envisagé: les prestataires de services qui refusent de coopérer pourraient, en dernier recours, se voir refuser l'accès à l'utilisateur belge.

L'article 39*bis* du Code d'instruction criminelle concerne les recherches informatiques et n'autorise aujourd'hui le blocage de certains sites internet que dans le cadre d'enquêtes en cours. Cette mesure ne peut, dans le cadre du jugement, être imposée à titre de sanction. Pour les fournisseurs de DNS, cela n'offre que peu de repères. Après la clôture de l'enquête, ils doivent rétablir le lien coupé entre l'adresse IP contestée et l'URL.

Très récemment, le législateur a fourni aux parquets un nouvel instrument dans l'article 46*sexies* du Code d'instruction criminelle, à savoir l'infiltration virtuelle. Toutefois, cette disposition n'autorise pas le pseudo-achat, par exemple l'achat prétendu d'une quantité de drogue sur le *darknet* par un enquêteur.

M. Geert Baudewijns (Secutec) réagit à l'observation de l'intervenant précédent proposant d'inonder le *darknet* de faux messages. Son entreprise s'attaque notamment à des campagnes de hameçonnage en les inondant de milliers de comptes factices, cette pratique étant à la limite de l'acceptable. Contrairement à leurs homologues américaines, les banques belges se montrent extrêmement réticentes à cet égard. L'orateur estime qu'il serait judicieux d'appliquer également cette technique au *darknet*, même s'il reste à déterminer comment elle pourrait être organisée sur le plan légal.

Secutec analyse près de 30 000 URL par jour, dont la majorité pour le CCB et CERT.be, mais aussi pour d'autres pays. Secutec constate que son bilan déclenche parfois une partie de ping-pong, l'utilisateur voulant savoir s'il a affaire à un problème de hameçonnage ou non. Secutec omet délibérément de répondre à cette demande car cela multiplierait par cinq les échanges de courriels.

S'agissant d'adaptations du cadre légal, Secutec a besoin d'une zone grise qui doit lui permettre d'aller un

bijgehouden en op verzoek van een bevoegde autoriteit kunnen worden gedeeld met de rechtshandhaving.

Op vraag van verschillende leden formuleert de heer De Keersmaecker enkele suggesties voor concrete wijzigingen van het wettelijk kader. Zo zou kunnen worden gestreefd naar een eenvormigheid van de artikelen 46*bis* en 46*quater* van het Wetboek van strafvordering, waarbij als principe geldt dat elke dienstverlener van telecommunicatiediensten bepaalde gegevens van zijn klanten moet kunnen delen op basis van een vordering. Daarnaast moet ook worden gedacht aan een verstrenging van het straffenarsenaal: dienstverleners die weigeren mee te werken, kan, als ultimum remedium, de toegang tot de Belgische gebruiker worden ontzegd.

Artikel 39*bis* van het Wetboek van strafvordering betreft de informaticazoeking en laat vandaag de dag enkel toe bepaalde websites te blokkeren in het kader van lopende onderzoeken. Deze maatregel kan niet, bij het vonnis, als straf worden uitgesproken. Voor DNS-providers biedt dit weinig houvast. Na het afsluiten van het onderzoek moeten zij de doorgeknipte link tussen het gewraakte IP-adres en de URL opnieuw herstellen.

De wetgever heeft de parketten zeer recent een nieuw instrument aangereikt in artikel 46*sexies* van het Wetboek van strafvordering, namelijk de virtuele infiltratie. Deze bepaling laat evenwel geen pseudokoop toe, bijvoorbeeld de voorgewende aankoop van een partij drugs op het *darknet* door een speurder.

De heer Geert Baudewijns (Secutec) pikt in op de opmerking van de vorige spreker over het overspoelen van het *darknet* met valse berichten. Zijn bedrijf gaat *phishing*-campagnes onder meer te lijf door er duizenden valse accounts in te pompen. Dit bevindt zich opnieuw op de grens van het toelaatbare. Belgische banken staan, in tegenstelling tot hun Amerikaanse tegenhangers, erg huiverachtig tegenover deze praktijk. Het zou volgens de heer Baudewijns een goed idee zijn deze techniek ook toe te passen op het *darknet*, al valt nog te bezien hoe dit wettelijk kan worden georganiseerd.

Secutec analyseert ongeveer 30 000 URL's per dag, waarvan het merendeel voor het CCB en CERT.be, maar ook voor andere landen. Secutec stelt vast dat er zich bij het geven van feedback soms een pingpongspel ontspint, waarbij de eindgebruiker wil weten of het al of niet *phishing* betreft. Secutec antwoordt hier doelbewust niet op, want dit zou een vervijfvoudiging van hun e-mailverkeer betekenen.

Wat aanpassingen aan het wettelijk kader betreft, heeft Secutec nood aan een grijze zone, die het bedrijf

peu plus loin dans les actions qu'elle mène pour le CCB et les parquets, sans crainte pour ces derniers que leurs enquêtes puissent en pâtir.

Á l'heure actuelle, la sécurisation des appareils connectés (IoT) ne fait l'objet d'aucune disposition légale. Il serait pourtant judicieux de légiférer dans ce domaine.

La sensibilisation est et demeure cruciale, mais elle n'est parfois malheureusement pas très utile. Secutec a ainsi constaté que malgré toutes les mesures de sensibilisation, certaines personnes sont victimes de fraude bancaire plusieurs fois par an.

Mme Verhelst a demandé quels étaient les talents requis pour faire carrière dans la cybersécurité. Ces talents sont difficiles à définir, selon M. Baudewijns. Il considère qu'il s'agit plutôt d'une passion: beaucoup de gens sont passionnés par l'IT en général, et par la cybersécurité en particulier. Une formation universitaire dans ce domaine permettrait sans aucun doute de développer et d'affiner ce potentiel.

Les pirates informatiques exploitent les vulnérabilités ou les failles des entreprises. Avec un investissement minimal, ils peuvent se procurer, sur des sites spécialisés, une vue complète des entreprises belges exposées à une vulnérabilité donnée. Lorsqu'une vulnérabilité est rendue publique, le hacker dispose de deux à trois semaines pour commettre son méfait. C'est en effet le délai nécessaire à l'entreprise pour y remédier.

Secutec est également abonnée à ces sites web et partage des listes avec CERT.be, ce qui permet de prendre des mesures. Cette opération est toutefois parfois compliquée. Lorsque Secutec contacte certaines entreprises en leur annonçant que leur infrastructure IT est vulnérable, elle n'est pas toujours prise au sérieux ou passe parfois elle-même pour un pirate informatique.

À la demande de Mme Houtmeyers, M. Baudewijns ajoute que l'estimation de 100 millions d'euros de rançon par an est basée sur une extrapolation du "marché" actuel, dont Secutec est aujourd'hui la référence – en grande partie malgré lui – et dont il prend environ 30 % en charge. L'orateur rappelle que la collaboration réciproque avec le CCB est excellente.

Mme Verhelst s'enquiert du montant récupéré auprès des cybercriminels. M. Baudewijns ne connaît pas les montants, mais confirme que le taux de récupération est généralement très faible: dans ce type de criminalité, l'argent file très vite. Secutec a déjà été associée à plusieurs reprises à des enquêtes menées par Europol.

ertoe in staat moet stellen iets verder te gaan in zijn acties voor het CCB en de parketten, zonder dat die laatste bevreesd moeten zijn dat hun onderzoeken erdoor zouden worden geschaad.

De beveiliging van *internet of things*-apparaten maakt thans niet het voorwerp uit van enige wettelijke bepaling. Wetgeving daaromtrent zou nochtans welgekomen zijn.

Sensibiliseren is en blijft cruciaal, maar zet helaas soms weinig zoden aan de dijk. Zo moet Secutec vaststellen dat, spijts alle sensibilisering, sommige mensen meerdere keren per jaar het slachtoffer worden van bankfraude.

Mevrouw Verhelst vroeg over welke talenten mensen die carrière willen maken in de cyberveiligheid, moeten beschikken. Talent valt moeilijk te definiëren, aldus de heer Baudewijns. Voor hem gaat het eerder over een passie; veel mensen zijn gepassioneerd door IT in het algemeen en cyberveiligheid in het bijzonder. Met een universitaire opleiding cyberveiligheid zou dat potentieel ongetwijfeld verder kunnen worden ontwikkeld.

Hackers werken op basis van *vulnerabilities* of kwetsbaarheden bij bedrijven. Voor een minimale investering kunnen zij op gespecialiseerde websites een volledig overzicht krijgen van Belgische bedrijven die openstaan voor een bepaalde kwetsbaarheid. Als zo'n kwetsbaarheid publiek bekend wordt, beschikt de hacker over twee tot drie weken om zijn slag te slaan; zolang heeft dat bedrijf immers nodig om die kwetsbaarheid te patchen.

Ook Secutec heeft abonnementen op die websites en deelt lijsten met CERT.be, waardoor acties kunnen worden ondernomen. Dat is nochtans niet altijd eenvoudig. Als Secutec bedrijven benadert met de melding dat hun IT-infrastructuur kwetsbaar is, wordt het bedrijf niet altijd ernstig genomen of wordt het soms zelf(s) gehouden voor hacker.

Op vraag van mevrouw Houtmeyers verduidelijkt de heer Baudewijns nog dat de schatting van 100 miljoen euro losgeld per jaar in België gebaseerd is op een extrapolatie van de huidige "markt", waarop Secutec – goeddeels ongewild – de referentie is en waarvan het ongeveer 30 % voor zijn rekening neemt. De spreker herhaalt dat er een uitstekende wederzijdse samenwerking is met het CCB.

Mevrouw Verhelst vroeg hoeveel gelden er konden worden gerecupereerd van internetcriminelen. De heer Baudewijns heeft geen weet van bedragen, maar bevestigt dat er doorgaans zeer weinig kan worden gerecupereerd; de gelden vertrekken immers zeer snel bij de internetcriminelen. Secutec is reeds enkele malen

Or, celles-ci prennent souvent deux à trois ans, de sorte qu'au moment de clore les enquêtes, il n'y a plus grand-chose à récupérer.

betrokken geweest bij onderzoeken met Europol. Die nemen echter al snel twee à drie jaren in beslag. Op het moment dat een dergelijk onderzoek wordt afgesloten, valt er dan ook niet veel meer te rapen.

Imprimerie centrale – Centrale drukkerij