CENTRE FOR CYBER SECURITY BELGIUM

GIDS OVER HET BELEID VOOR DE GECOÖRDINEERDE BEKENDMAKING VAN KWETSBAARHEDEN

DEEL II: WETTELIJKE ASPECTEN

COORDINATED VULNERABILITY DISCLOSURE POLICIES - "CVDP"
RESPONSIBLE DISCLOSURE POLICIES - "RDP"

CENTRUM VOOR CYBERSECURITY BELGIË
Wetstraat 16
1000 Brussel

info@ccb.belgium.be
www.ccb.belgium.be

UNDER THE AUTHORITY OF THE PRIME MINISTER

.be

CENTRE FOR CYBER SECURITY BELGIUM

A. Inhoudsopgave

B. Toepassing van het Belgisch strafrecht 4

C. Indringing in een informaticasysteem 5

Afdeling 1. Externe indringing 5
Afdeling 2. Interne indringing 10
Afdeling 3. Verzwarende omstandigheden van de indringing 13
Afdeling 4. Beleid voor de gecoördineerde bekendmaking van kwetsbaarheden en indringing 15

D. Inbreuk in verband met informaticagegevens 17

Afdeling 1. Materiële constitutieve elementen 18
Afdeling 2. Moreel element 18
Afdeling 3. Verzwarende omstandigheden 19
Afdeling 4. Ter beschikking stellen van middelen om de inbreuk in verband met gegevens mogelijk te maken 19
Afdeling 5. Poging 20
Afdeling 6. Beleid voor de gecoördineerde bekendmaking van kwetsbaarheden en inbreuk in verband met informaticagegevens 20

E. Valsheid in informatica en informaticabedrog 21

Afdeling 1. Valsheid in informatica en het gebruik van valse stukken in informatica 21
Afdeling 2. Informaticabedrog 23
Afdeling 3. Beleid voor de gecoördineerde bekendmaking van kwetsbaarheden, valsheid in informatica en informaticabedrog 24

F. Misdrijven betreffende het geheim van communicatie 24

Afdeling 1. Misdrijven betreffende het geheim van niet voor het publiek toegankelijke communicatie en gegevens van een informaticasysteem 24
Afdeling 2. Voorbereidende handelingen 27
Afdeling 3. Helen van onrechtmatig verkregen communicatie 28
Afdeling 4. Poging 29
Afdeling 6. Beleid voor de gecoördineerde bekendmaking van kwetsbaarheden en communicatie 33

G. Naleving van andere wettelijke bepalingen 35

Afdeling 1. Begrippen in verband met persoonsgegevens 35
Afdeling 2. Juridische invulling van de rol van deelnemer 37
Afdeling 3. Gevolgen voor de inhoud van het CVDP 39

H. Juridische referenties 41

CENTRE FOR CYBER SECURITY BELGIUM

<u>Opgelet</u>:

In deze gids vindt u een overzicht van de begrippen, doelstellingen, juridische vraagstukken en goede praktijken rond de invoering van een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden (of Coordinated Vulnerability Disclosure Policy – "CVDP") in de huidige stand van de Belgische wetgeving – zie de voorbeelden op de website van het CCB.

We wijzen erop dat de door het CCB opgestelde documenten geenszins de bestaande wettelijke regels wijzigen. Het ongeoorloofd binnendringen in het informaticasysteem van een derde, zelfs met goede bedoelingen, blijft een strafrechtelijk misdrijf.

De deelnemer aan een CVDP moet zich ervan bewust zijn dat hij zich niet kan beroepen op een algemene uitsluiting van aansprakelijkheid wanneer hij deelneemt aan dat beleid: hij moet behoedzaam te werk gaan en alle voorwaarden van het beleid en de toepasselijke wettelijke bepalingen nauwgezet naleven.

Designed by CCB and Intigriti (2020)

B. Toepassing van het Belgisch strafrecht

De toepassing van het Belgisch strafrecht hangt voornamelijk af van de lokalisering van het misdrijf. Volgens de objectieve ubiquiteitstheorie wordt een misdrijf gelokaliseerd op de plaats waar de daad heeft plaatsgevonden en op de plaats(en) waar het resultaat ervan verschijnt.[1]

Daarvoor volstaat het dat een van de materiële constitutieve of materiële verzwarende elementen[2] van een misdrijf plaatsvond op Belgisch grondgebied, zonder dat het misdrijf volledig in België moet zijn gepleegd. Zo kan het Belgisch strafrecht worden toegepast als de dader materiële handelingen heeft gesteld in België, als het informaticasysteem of de gegevens zich in België bevinden, of als de eventuele schade in België is aangebracht.

In die context kunnen de in deze gids beschreven regels worden toegepast als de dader zich in België bevindt tijdens zijn deelname aan het beleid voor gecoördineerde bekendmaking of als het bezochte informaticasysteem zich in België bevindt.

Gezien de gemeenschappelijke regels van het Cybercrimeverdrag van Boedapest[3] en de Europese wetgeving[4] zijn sommige elementen van deze juridische analyse in België ook toepasselijk op andere landen, met name in Europa. Niettemin moet telkens bij de bevoegde nationale autoriteiten worden nagegaan of dat wel degelijk het geval is.

[1] Cass., 23 januari 1979, *Pas.*, I, 1979, p. 582; Cass., 4 februari 1986, *Pas.*, 1986, blz. 664.
[2] En niet louter intentionele elementen.
[3] Cybercrimeverdrag van de Raad van Europa, opgemaakt in Boedapest op 23 november 2001, in werking getreden op 1 juli 2004.
[4] Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad, Pb., 14 augustus 2013.

C. Indringing in een informaticasysteem[5]

Afdeling 1. Externe indringing

Artikel 550*bis*, § 1, van het Strafwetboek bestraft degene die, wetende dat hij er niet toe gerechtigd is, zich toegang verschaft tot een informaticasysteem of zich daarin handhaaft.

1. Materiële constitutieve elementen

1.1. Toegang tot of handhaving in een informaticasysteem

a) Informaticasysteem

De wet van 28 november 2000 inzake informaticacriminaliteit, die artikel 550*bis* heeft ingevoerd in het Strafwetboek, heeft niet bepaald wat moest worden verstaan onder "informaticasysteem".[6] Niettemin beschrijven de voorbereidende werkzaamheden van de wet enerzijds het begrip "informaticasysteem" als elk systeem voor de opslag, verwerking of overdracht van gegevens en anderzijds het begrip "gegevens" als voorstellingen van informatie, ongeacht de materiële vormgeving ervan (elektromagnetisch, optisch of anderszins) die geschikt zijn voor opslag, verwerking en overdracht via een informaticasysteem.[7]

We kunnen ook verwijzen naar de Europese richtlijn 2013/40/EU van 12 augustus 2013 over aanvallen op informatiesystemen[8], die deze twee begrippen definieert:

- een "informatiesysteem" is een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er een of meer op basis van een programma automatisch computergegevens verwerken, alsmede de computergegevens die met dat apparaat of die groep van apparaten

[5] Wij verkiezen hier de term "indringing" in plaats van "hacking" omdat "hacking" op informaticagebied niet volledig overeenstemt met het begrip "illegale informaticapiraterij" en ook kan verwijzen naar activiteiten die met de toestemming van de verantwoordelijke van het informaticasysteem worden uitgevoerd. Het begrip "indringing" betekent wel degelijk het binnendringen in (een deel van) een informaticasysteem, zonder daartoe gemachtigd te zijn.

[6] Op dit punt lijkt de wetgever met opzet onduidelijk te zijn gebleven om te vermijden dat de concepten al te snel achterhaald zouden zijn door de evolutie van de informatietechnologieën: cf. in dat opzicht, *Parl.St.*, Kamer, 1999-2000, nr. 50, 0213/001, blz. 12. De Belgische wetgever heeft rekening gehouden met de snelle evolutie van de technologie bij het opstellen van de wet van 28 november 2000 inzake informaticacriminaliteit, zodat de terminologie van de wet technologisch neutraal is: *Parl.St.*, Kamer, 2003-2004, nr. 1284/001, blz. 5.

[7] *Parl.St.*, Kamer, 1999-2000, nr. 50, 0213/001, blz. 12.

[8] Pb., 14 augustus 2013. Zie ook de definities in art. 1 van het Cybercrimeverdrag van de Raad van Europa, opgemaakt in Boedapest op 23 november 2001, in werking getreden op 1 juli 2004 en goedgekeurd door België (wet van 3 augustus 2012, B.S. van 21 november 2012, blz. 69092).

worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud daarvan[9];

- "computergegevens" zijn een weergave van feiten, gegevens of begrippen in een vorm die geschikt is voor verwerking in een informatiesysteem, met inbegrip van programma's die een informatiesysteem een bepaalde functie kunnen laten vervullen.

Het begrip "informaticasysteem" gaat dus verder dan dat van de gewone personal computer en betreft, in ruime zin, alle vormen van systemen die gegevens verwerken: een elektronische tablet, een gps, een smartphone, een elektronisch horloge, een netwerk, een server, een router, een decoder, een internettelevisie, de boordcomputer van een voertuig, een elektronische betaalterminal, een chipkaart, enz.

b) Toegang of handhaving

Aangezien de begrippen "toegang" of "handhaving" niet zijn gedefinieerd in het Strafwetboek of de parlementaire werkzaamheden, moeten ze worden begrepen in de zin van het normale taalgebruik, zonder het gebruik van een bijzondere techniek te vereisen.

Het begrip "toegang" impliceert een positieve indringingshandeling die met zekerheid de wil vertolkt om binnen te dringen in het informaticasysteem[10], zonder noodzakelijkerwijs complexe informaticamanipulaties te vereisen[11]: het volstaat bijvoorbeeld om een opdracht uit te voeren die het mogelijk maakt om een systeem op te starten, een programma te openen, een bestand op te zoeken of door een tekst te scrollen.

In geval van indringing handelt de dader van het misdrijf doorgaans van buiten het systeem via een telecommunicatie-infrastructuur en omzeilt hij daarbij beveiligingsmaatregelen.

Het begrip "toegang" vereist echter niet dat er gegevens zijn ingevoerd, gewijzigd of verwijderd in het informaticasysteem.

De handhaving betreft met name het geval waarbij een persoon zich door onachtzaamheid (zonder het te beseffen) zonder machtiging toegang verschaft tot een informaticasysteem, en zich daarin handhaaft nadat hij dit heeft ingezien. Het kan ook gaan om het geval waarbij een persoon zijn toegang

[9] Deze elementen zijn ook opgenomen in de definitie van "netwerk- en informatiesysteem" van richtlijn 2016/1148 van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (NIS-richtlijn).

[10] De geïnformatiseerde terminal van een banktransactiesysteem is, in de zin van deze bepaling, een informaticasysteem: Corr. Dendermonde, 14 mei 2007, *T. Strafr.*, 2007, blz. 403.

[11] Corr. Antwerpen, 10 november 2014, *T. Strafr.*, 2015, blz. 94.

tot het systeem behoudt hoewel zijn toegangsmachtiging is verlopen (door het verstrijken van een bepaalde termijn of door het einde van de uitoefening van een functie).[12]

c) Beveiliging van het informaticasysteem

Het misdrijf vereist niet dat de toegang tot of handhaving in een informaticasysteem plaatsvond ingevolge het doorbreken van het systeem of het omzeilen van beveiligingsmaatregelen (paswoord, firewall, identificatie, versleuteling, enz.). Het ontbreken van beveiligingsmaatregelen voor het informaticasysteem sluit het bestaan van een externe indringing dus niet uit.

Tijdens de parlementaire werkzaamheden werd deze keuze gerechtvaardigd door het feit dat het begrip "doorbreken" enerzijds een aantal praktische complicaties zou meebrengen (het bepalen van een vereist beveiligingsniveau en de noodzaak om beveiligingssystemen openbaar te maken bij de bewijsvoering) en anderzijds wellicht niet zinvol zou zijn door de toenemende standaardisering van systeembeveiliging.[13]

Een externe indringing kan dus bestaan in het loutere gebruik van een onbeveiligd draadloos netwerk om verbinding te maken met het internet zonder de toestemming van de beheerder van dat netwerk.[14]

d) Schade veroorzaakt aan het informaticasysteem

Het is niet vereist dat de indringing of handhaving schade heeft veroorzaakt aan het informaticasysteem. Een louter risico volstaat, ook als het zich niet realiseert.[15] De wetgever beschouwt externe indringing immers als "een gevaarzettingsdelict dat als zodanig strafwaardig is, ongeacht de bijzondere kwaadwillige bedoelingen of de gerealiseerde effecten".

De wetgever heeft de ongeoorloofde toegang tot een informaticasysteem als dusdanig strafrechtelijk willen bestraffen. Zo kan de loutere kennisneming van de inhoud of van de werkings- of beveiligingsparameters van het informaticasysteem van een derde, zelfs zonder deze te wijzigen of te schaden, een misdrijf zijn.

[12] Bijvoorbeeld het behoud van een verbinding met het informaticasysteem van een bedrijf door een ex-werknemer.
[13] *Parl.St.*, Kamer, 1999-2000, nr. 50, 0213/001, blz. 17.
[14] Corr. Dendermonde, 14 november 2008, *T. Straf.*, 2009, blz. 114.
[15] Overeenkomstig art. 550*bis*, § 3, 3°, van het Strafwetboek vormt het bestaan van schade niettemin een verzwarende omstandigheid van het misdrijf.

1.2. Totaal gebrek aan machtiging

Het begrip “machtiging” wordt niet verduidelijkt in het Strafwetboek en moet dus, volgens de interpretatiebeginselen in strafzaken, worden begrepen in de zin van het normale taalgebruik. In voorkomend geval betreft het de toestemming die een gemachtigd persoon aan een ander heeft gegeven om zich toegang te verschaffen tot het betrokken informaticasysteem of zich daarin te handhaven.

Concreet kunnen zich twee situaties voordoen: ofwel dringt een persoon bewust binnen in een informaticasysteem hoewel hij geen toegangsmachtiging heeft, zelfs geen gedeeltelijke, ofwel verschaft een persoon zich door onachtzaamheid toegang tot een informaticasysteem, of bewust na het verstrijken van zijn machtiging, en handhaaft hij zich daar onrechtmatig in.

De externe indringing is een aflopend misdrijf en bestaat dus vanaf het ogenblik dat het individu zich zonder machtiging toegang verschaft tot het informaticasysteem of zich daarin zonder machtiging handhaaft. De eventueel na de feiten verleende machtiging doet het bestaan van een strafrechtelijk misdrijf dus niet verdwijnen.

Om geldig te zijn, moet de toestemming om zich toegang te verschaffen tot een informaticasysteem of zich daarin te handhaven noodzakelijkerwijs komen van een persoon die daartoe gemachtigd is door de houder van de rechten op het systeem, namelijk de verantwoordelijke van dit systeem.[16] Het zijn tenslotte de verantwoordelijke van het systeem en zijn gedelegeerden die de taak hebben om de voorwaarden van een dergelijke machtiging toe te kennen, in te trekken en te bepalen. Deze machtiging kan uitdrukkelijk of stilzwijgend zijn, voor zover ze met zekerheid bestaat.

a) Uitdrukkelijke machtiging

De uitdrukkelijke machtiging bestaat erin dat de beheerder van het informaticasysteem een bepaalde natuurlijke of rechtspersoon uitdrukkelijk machtigt om zich toegang te verschaffen tot zijn informaticasysteem, bijvoorbeeld om er onderhoudswerkzaamheden, beveiligingstests of programma-updates uit te voeren. Deze uitdrukkelijke machtiging is doorgaans opgenomen in contractuele bepalingen of in interne documenten van de organisatie.

Als een organisatie een beveiligingsauditovereenkomst sluit die de uitvoering van binnendringingstests omvat[17], geeft ze uitdrukkelijk toestemming voor toegang tot – op zijn minst een deel van – haar

[16] Naargelang de structuur van de organisatie kan deze persoon bijvoorbeeld de eigenaar van het systeem zijn, het hoofd van de organisatie, de informaticaverantwoordelijke of de informatiebeveiligingsadviseur.
[17] "Pentesting"-overeenkomst.

informaticasysteem. In dat geval beschikt de dienstverlener, een informatiebeveiligingsspecialist, over een toegangsmachtiging en moet hij geen strafrechtelijke vervolging voor externe hacking vrezen.

b) Stilzwijgende machtiging

De stilzwijgende machtiging vloeit voort uit de bijzondere omstandigheden van de zaak. Bijvoorbeeld de uitoefening van een functie voor rekening van een bedrijf die noodzakelijkerwijs de toegang tot de informaticamiddelen ervan impliceert om de taken uit te voeren, zelfs zonder uitdrukkelijke machtiging.[18]

In dezelfde zin kan een stilzwijgende machtiging ook voortvloeien uit het bestaan van een informaticasysteem dat duidelijk ter beschikking van het publiek wordt gesteld.[19]

Uiteraard beschikken de eigenaar van het informaticasysteem en zijn wettelijke vertegenwoordigers over een – minstens stilzwijgende – toegangsmachtiging voor het betrokken informaticasysteem, zolang ze zich rechtsgeldig kunnen beroepen op die hoedanigheden.

De stilzwijgende machtiging verdwijnt evenwel vanaf het ogenblik dat de voor rekening van het bedrijf uitgeoefende functie, het publieke karakter van de toegang, de terbeschikkingstelling van de klanten of het eigendomsrecht afloopt. Indien de betrokkene zich achteraf handhaaft in het informaticasysteem of zich daar achteraf toegang toe verschaft, wordt dit dus beschouwd als een indringing.

2. Moreel element

2.1. Wil om zich toegang te verschaffen tot het systeem en kennis van het gebrek aan machtiging

Het misdrijf vereist eenvoudigweg de bewuste en vrije wil om zich toegang te verschaffen tot een informaticasysteem of zich daarin te handhaven hoewel men weet dat men er niet toe gerechtigd is. Artikel 550*bis* van het Strafwetboek vereist geen bijzonder opzet, zoals bijvoorbeeld een bedrieglijk opzet of het oogmerk om te schaden. De opzettelijke en ongeoorloofde indringing of handhaving in een informaticasysteem volstaat om het misdrijf te plegen. De indringing die het gevolg is van onachtzaamheid, verstrooidheid, een manipulatiefout of een onvoldoende beheersing van de

[18] Werknemers krijgen echter vaak wel een login en een paswoord van hun werkgever waardoor ze uitdrukkelijk worden gemachtigd om toegang te hebben tot het informaticasysteem.
[19] Bijvoorbeeld een draadloos netwerk in een openbare ruimte en zonder paswoord (hotspots), een draadloze computer of een draadloos netwerk van een instelling die/dat ter beschikking wordt gesteld van klanten, een automatische betaalkassa, een kiosk voor het inchecken van bagage door passagiers in een luchthaven, enz.

informaticatool (waarbij de persoon te goeder trouw heeft gehandeld) wordt daarentegen niet strafbaar gesteld (indien de persoon zich daarna niet met kennis van zaken handhaaft in het informaticasysteem).

De opzettelijke (ongeoorloofde) indringing met een eerbaar motief, zoals bijvoorbeeld het opsporen van informaticabeveiligingsgebreken in het informaticasysteem van een derde, wordt wel strafbaar gesteld.[20] De wetgever wilde immers elke indringing – behalve de onopzettelijke – in een informaticasysteem bestraffen zonder rekening te houden met het opzet van de indringer.[21] Doel is de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en van de gegevens die erin worden opgeslagen, verwerkt of overgedragen zoveel mogelijk te beschermen.

Het feit dat de indringer goede bedoelingen had of na de feiten de toestemming kreeg van de verantwoordelijke van het informaticasysteem, is dus geen rechtvaardigingsgrond voor het uitsluiten van een mogelijke strafrechtelijke veroordeling voor externe indringing. Het zou voor indringers inderdaad gemakkelijk zijn om zogenaamde goede bedoelingen aan te voeren na het begin van hun vervolging en het zou moeilijk zijn om deze a posteriori te controleren.

De rechtspraak heeft aldus bevestigd dat externe indringing met als doel louter na te gaan of de informaticabeveiligingsmaatregelen van een concurrent voor diens gegevensbescherming even onbetrouwbaar zijn als de zijne, wel degelijk een misdrijf is.[22]

Het bedrieglijk opzet van de dader geldt niettemin als een verzwarende omstandigheid van het misdrijf, die de opgelegde straf zal verzwaren.[23]

Afdeling 2. Interne indringing

Artikel 550*bis*, § 2, van het Strafwetboek betreft diegene die, met bedrieglijk opzet of met het oogmerk om te schaden, zijn toegangsbevoegdheid tot een informaticasysteem overschrijdt.

[20] Corr. Hasselt, 21 januari 2004, *Lim. Rechtsl.*, 2005, blz. 133; *Computerr.*, 2004, boek 3, blz. 131: het bestaan van een misdrijf is bijvoorbeeld niet uitgesloten wanneer een gebruiker die de beveiliging van het pc-bankingsysteem van zijn bank nagaat, ontdekt dat het mogelijk is om verrichtingen te doen die gebruikers van het systeem schade kunnen berokkenen (zoals lijsten met begunstigden van overschrijvingen van andere gebruikers downloaden, bankrekeningnummers van deze lijsten wijzigen en die gewijzigde lijst terug op hun harde schijf zetten, waardoor overschrijvingen naar andere rekeningnummers dan die van de begunstigden mogelijk zijn) en zijn bank daarvan op de hoogte brengt; Corr. Eupen, 15 dec. 2003, *R.D.T.I.*, 2004, blz. 61 en nota O. LEROUX; Corr. Leuven, 15 juni 2010, *T. Strafr.*, 2011, blz. 270; Corr. Dendermonde, 25 mei 2007, *T.G.R.*, 2007, blz. 351 e.v.
[21] Corr. Brussel, 8 jan. 2008, *J.T.*, 2008, blz. 337.
[22] Corr. Eupen, 15 dec. 2003, *R.D.T.I.*, 2004, blz. 61.
[23] Art. 550*bis,* § 1, tweede lid, van het Strafwetboek.

1. Materiële constitutieve elementen

1.1. Bestaan van een gedeeltelijke machtiging

Interne indringing veronderstelt het bestaan, vóór het plegen van het misdrijf, van een gedeeltelijke toegangsmachtiging voor het betrokken informaticasysteem.[24] Bij gebrek aan nadere toelichting in het Strafwetboek moet de machtiging worden begrepen in de gebruikelijke zin, net zoals bij de externe indringing (*supra*).

De aard en de omvang van de toegangsbevoegdheid tot een informaticasysteem worden immers in beginsel niet bepaald door de wetgever, maar overgelaten aan de beoordelingsbevoegdheid van de eigenaar van het systeem, aangezien deze het best geplaatst is om te bepalen wie toegangsbevoegdheid krijgt en binnen welke grenzen.[25]

De grenzen die aan de toegangsmachtiging worden gesteld, kunnen bijvoorbeeld "ruimtelijk" zijn, dat wil zeggen gelinkt aan bepaalde verboden delen van het informaticasysteem, of "functioneel", dat wil zeggen gelinkt aan bepaalde verboden verrichtingen of bepaalde verboden gegevenscategorieën voor het hele systeem. De beperking is duidelijk als het systeem bijvoorbeeld voorzien is van een voorafgaand identificatieproces om toegang te krijgen tot bepaalde gegevens of programma's.[26]

De finaliteit waarvoor een persoon een toegangsmachtiging voor een informaticasysteem krijgt, beperkt dit toegangsrecht niet, tenzij uitdrukkelijk anders is bepaald door de verantwoordelijke van het systeem. Er kan niet worden gesteld dat een persoon zijn toegangsrecht heeft overschreden in de zin van artikel 550*bis*, § 2, van het Strafwetboek enkel en alleen omdat hij deze machtiging heeft afgewend van de finaliteit ervan.[27] Bijgevolg pleegt de persoon die zijn toegangsrecht tot een informaticasysteem voor persoonlijke doeleinden gebruikt, hoewel hij een toegangsmachtiging heeft gekregen voor welbepaalde professionele doeleinden, geen interne indringing.

Het begrip betreft zowel personen met een permanente gedeeltelijke machtiging, zoals deze die wordt toegekend aan het personeel van een bedrijf, als personen die een gedeeltelijke machtiging hebben die beperkt is in de tijd, zoals deze die tijdelijk wordt toegekend aan een consultant van een extern bedrijf dat gespecialiseerd is in informaticabeveiliging.

[24] Corr. Leuven, 15 juni 2010, *T. Strafr.*, 2011, blz. 270: de rechtbank oordeelde dat het feit klant te zijn van een bank en een toegangsbevoegdheid te hebben voor het pc-bankingsysteem, die persoon geen toegangsbevoegdheid verleent voor het informaticasysteem van de bank.
[25] Arbitragehof, 24 maart 2004, nr. 51/2004, B.4.3, blz. 7.
[26] Corr. Brussel, 8 jan. 2008, *J.T.*, 2008, blz. 337.
[27] Cass., 24 januari 2017, P.16.0048.N, www.cass.be.

Hoewel vaak sprake is van een voorafgaande gedeeltelijke machtiging in het kader van een contractuele verbintenis, impliceert dit begrip niet noodzakelijk een band van ondergeschiktheid, een hiërarchische band of een contractuele band tussen de verlener van de machtiging en de begunstigde.

1.2. Overschrijden van de machtiging

Het misdrijf bestaat vanaf het ogenblik dat de dader zijn toegangsrechten overschrijdt om binnen te dringen of zich te handhaven in een deel van het informaticasysteem waarvoor hij geen toegangsmachtiging (meer) heeft op het ogenblik van het misdrijf.[28]

Dit geval betreft onder andere de situatie van een werknemer die een gedeeltelijke toegangsbevoegdheid tot de server van zijn bedrijf heeft gekregen om zijn taken te vervullen, maar de hem opgelegde grenzen overschrijdt.

Net als bij de externe indringing moet de interne indringing niet noodzakelijk schade hebben toegebracht aan het bezochte systeem om bestraft te worden.

2. Moreel element

2.1. Wil om zijn machtiging te overschrijden

Het misdrijf vereist de wil om zich, opzettelijk en met kennis van zaken, toegang te verschaffen tot een deel van het informaticasysteem of zich erin te handhaven hoewel de persoon weet dat hij zo zijn toegangsbevoegdheid voor het informaticasysteem overschrijdt.

2.2. Bijzonder opzet: bedrieglijk opzet of oogmerk om te schaden

Het louter zonder toestemming binnendringen in bepaalde delen van het informaticasysteem, bijvoorbeeld uit pure nieuwsgierigheid, wordt niet strafrechtelijk bestraft. De indringing moet zijn ingegeven door een bijzonder opzet, d.w.z. onrechtmatig winstbejag (fraude) of kwaadwillige bedoelingen (oogmerk om te schaden), om een misdrijf te zijn. Dat kan bijvoorbeeld het geval zijn wanneer een werknemer die toegang heeft tot een deel van het bedrijfsnetwerk, deze machtiging

[28] Zie Cass., 5 januari 2011, P.10.1094.F., www.cass.be: de vaststelling dat de vervolgde personen toegangsrecht hadden tot de litigieuze gegevens toen ze de kopie ervan vroegen en kregen, sluit de overschrijding van de toegangsbevoegdheid uit die bij artikel 550*bis*, § 2, Strafwetboek, strafbaar is gesteld.

overschrijdt om zich toegang te verschaffen tot het boekhoudprogramma en er ongeoorloofde bankverrichtingen te doen, of nog, bepaalde data voor eigen rekening te commercialiseren.[29]

De wetgever heeft dit onderscheid met het misdrijf van externe indringing verantwoord door het feit dat derden die niet over een toegangsmachtiging beschikken de veiligheid van het informaticasysteem meer in gevaar zouden brengen dan een persoon die een gedeeltelijke machtiging heeft.[30] Bovendien hebben de parlementaire werkzaamheden erop gewezen dat de verantwoordelijke van het systeem over andere sancties (burgerrechtelijke of contractuele sancties, of tuchtstraffen) beschikt tegen de begunstigde van een gedeeltelijke machtiging die zonder bedrieglijk of kwaadwillig opzet zou zijn overschreden.[31]

Afdeling 3. Verzwarende omstandigheden van de indringing

Artikel 550*bis*, § 3, van het Strafwetboek voorziet in een aantal verzwarende omstandigheden die gelden voor beide misdrijven met betrekking tot indringing.

1. Overname van gegevens

De eerste verzwarende omstandigheid is de overname, op enige manier, van gegevens die worden opgeslagen, verwerkt of overgedragen door middel van het bezochte informaticasysteem.[32] Het betreft het overnemen van informaticagegevens (origineel of kopie) uit het bezochte systeem om deze in voorkomend geval opnieuw te kunnen gebruiken.[33] De gebruikte formulering “op enige manier” is heel ruim en kan dus verwijzen naar het afdrukken, het via mail versturen, het kopiëren op een drager, het opslaan in een cloudsysteem, het maken van een screenshot, enz.[34] Doel van de wetgever was hier onder meer het stelen van industriële geheimen in het kader van bedrijfsspionage te bestrijden.[35]

Het begrip “overname” van gegevens lijkt ten slotte een moreel element te vereisen aangezien het voortvloeit uit het feit dat de dader zelf het initiatief neemt om deze gegevens op te halen en niet uit

[29] *Parl.St.*, Kamer, 1999-2000, nr. 50, 0213/004, blz. 6.
[30] *Parl.St.*, Kamer, 1999-2000, nr. 50, 0213/001, blz. 16.
[31] *Parl.*St., Senaat, 1999-2000, 2-392/3, blz. 6; *Parl.St.*, Kamer, 1999-2000, nr. 50, 0213/001, blz. 16.
[32] Corr. Dendermonde, 14 mei 2007, *T. Strafr.*, 2007, blz. 403.
[33] Dit gedrag wordt soms “bitnapping” genoemd, een verwijzing naar de kidnapping van gegevens.
[34] Er moet echter worden verduidelijkt dat deze bepaling niet verwijst naar het materieel meenemen van de drager waarop informaticagegevens waren afgedrukt of opgeslagen (bv. het stelen van afgedrukte gegevens, van een harde schijf of van een USB-stick) , wat een ander misdrijf is, namelijk het stelen van de drager zelf.
[35] *Parl.St.*, Kamer, 1999-2000, nr. 50, 0213/001, blz.17: een werknemer die zakengeheimen van zijn werkgever tracht te stelen, kan ook worden vervolgd voor het misdrijf van het meedelen van fabrieksgeheimen, zoals bedoeld in art. 309 van het Strafwetboek.

het louter automatisch opslaan van gegevens door het informaticasysteem dat voor de indringing wordt gebruikt.

2. Gebruik van het bezochte systeem

De tweede verzwarende omstandigheid is enig gebruik van een informaticasysteem van een derde of het feit dat gebruik wordt gemaakt van het informaticasysteem om toegang te krijgen tot het informaticasysteem van een derde. Enerzijds betreft de bepaling het benutten van de capaciteit van het bezochte informaticasysteem, waardoor de gebruiksmogelijkheden van andere gebruikers tijdelijk beperkt worden (bv. tijdsdiefstal of diefstal van bandbreedte).[36] Anderzijds betreft ze het feit zich toegang te verschaffen tot een ander informaticasysteem via het bezochte systeem, dat gebruikt wordt als tussenschakel voor een informatica-aanval waarbij de indruk wordt gewekt dat de aanval van een tussensysteem komt.[37]

De twee bedoelde gevallen veronderstellen wel degelijk een moreel element, nl. dat de dader wetens en willens de bedoeling had om voor deze doeleinden gebruik te maken van het informaticasysteem. Dit element sluit bijvoorbeeld het geval uit waarbij de vermindering van de capaciteit van het informaticasysteem onverwachts zou voortvloeien uit de indringing.

3. Schade aan het informaticasysteem of aan de gegevens

De derde verzwarende omstandigheid bestaat erin enige schade te veroorzaken, zelfs onopzettelijk, aan het informaticasysteem of aan de gegevens die erin worden opgeslagen, verwerkt of overgedragen, of aan het informaticasysteem of de informaticagegevens van een derde.

Dit omvat elke soort schade, zowel materiële (fysieke beschadiging van het systeem, kabels of randapparatuur) als immateriële (verzadiging van het systeem, onbeschikbaarheid) schade aan het bezochte informaticasysteem of aan de gegevens ervan.

In dit geval kan de schade opzettelijk of onopzettelijk zijn veroorzaakt, zodat er geen moreel element vereist is in hoofde van de dader.[38]

[36] *Parl.St.*, Kamer, 1999-2000, nr. 50, 0213/001, blz. 17.
[37] C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique", *op. cit.*, blz. 639. Het kan bijvoorbeeld gaan om het gebruik van het informaticasysteem in een botnet-netwerk, d.w.z. in een groep van geïnfecteerde computers ("zombies") die op afstand gecontroleerd worden door een hacker om andere informaticasystemen aan te vallen en daarbij de echte oorsprong van de aanval te verbergen.
[38] Niettemin moet het optreden van deze omstandigheid voor de dader wel voorzienbaar zijn en er moet een oorzakelijk verband zijn tussen deze omstandigheid en het plegen van het hoofdmisdrijf. De opzettelijk veroorzaakte schade die

Afdeling 4. Beleid voor de gecoördineerde bekendmaking van kwetsbaarheden en indringing

Zoals eerder uiteengezet, bestaat het misdrijf van externe indringing in een informaticasysteem zelfs als de dader geen kwaadwillige bedoelingen heeft, geen beveiligingsmaatregelen omzeilt, het bezochte systeem niet gebruikt, geen gegevens overneemt en geen schade veroorzaakt aan het systeem of aan de gegevens. De goede bedoelingen van de deelnemer aan een CVDP volstaan dus niet om het bestaan van dit strafrechtelijk misdrijf te vermijden.

Er is echter alleen sprake van externe indringing als de deelnemer niet beschikt over een machtiging van de verantwoordelijke organisatie om zich toegang te verschaffen tot haar informaticasysteem. Als de deelnemer in het kader van een machtiging handelt, is er geen sprake van externe indringing.

In het kader van een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden of een beloningsprogramma voor het opsporen van kwetsbaarheden bestaat een dergelijke – uitdrukkelijke of stilzwijgende – machtiging.

Bij de invoering van een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden, met inbegrip van een beloningsprogramma, wordt de facto op zijn minst een stilzwijgende en duidelijke machtiging verleend. Dat beleid verduidelijkt immers de samenwerkingsmodaliteiten tussen een organisatie die verantwoordelijk is voor het betrokken informaticasysteem en deelnemers die bereid zijn om haar te informeren over kwetsbaarheden van haar informaticasysteem. Deze samenwerking houdt noodzakelijkerwijs een machtiging in om zich toegang te verschaffen tot het betrokken informaticasysteem of om zich daarin te handhaven, met als doel de veiligheid ervan te verbeteren en met inachtneming van de vooraf bepaalde voorwaarden. Ook al is de begunstigde van de machtiging niet precies gekend op het ogenblik dat het beleid voor gecoördineerde bekendmaking wordt ingevoerd, gaat het wel degelijk om een machtiging die eenzijdig wordt toegekend door de verantwoordelijke van het informaticasysteem aan personen die wensen deel te nemen aan zijn programma voor gecoördineerde bekendmaking.

Gelet op het legaliteitsbeginsel moet het strafrecht restrictief worden geïnterpreteerd. In geval van twijfel over de draagwijdte van de gebruikte repressieve termen is de rechter dus verplicht om het toepassingsgebied ervan te beperken. Bijgevolg moet het gebrek aan machtiging, in de zin van artikel 550*bis* van het Strafwetboek, strikt worden geïnterpreteerd, d.w.z. in het geval dat geen enkele handeling derden terecht kan doen aannemen dat de verantwoordelijke organisatie de toegang tot haar informaticasysteem toestaat. Als de verantwoordelijke organisatie weloverwogen en bewust een beleid voor gecoördineerde bekendmaking heeft ingevoerd, is zij vooraf duidelijk bereid om de toegang tot haar informaticasysteem toe te staan, mits de vastgestelde voorwaarden worden

voortvloeit uit het invoeren, wijzigen of verwijderen van gegevens zal in voorkomend geval aanleiding geven tot een ander misdrijf, nl. de inbreuk in verband met informaticagegevens bedoeld in art. 550*ter* van het Strafwetboek.

nageleefd. Tevens moet worden opgemerkt dat een deel van de rechtspraak een extensieve uitleg geeft aan de voor de beklaagde gunstige bepalingen, wat ook het geval kan zijn voor het begrip "machtiging". Aangezien de machtiging gunstig is voor de dader van de feiten en het bestaan van een misdrijf uitsluit, moet ze worden geïnterpreteerd als zijnde inherent aan de invoering van een beleid voor gecoördineerde bekendmaking.

Het belang van een beleid voor gecoördineerde bekendmaking bestaat er dus in dat, voor zover de door de verantwoordelijke organisatie geformuleerde voorwaarden worden nageleefd, een van de materiële constitutieve voorwaarden voor het misdrijf van externe indringing, nl. het totale gebrek aan machtiging, wordt uitgesloten. De persoon die deelneemt aan een dergelijk beleid en de voorwaarden ervan naleeft, pleegt dus geen externe indringing.

De deelnemer die over een gedeeltelijke toegangsmachtiging voor een informaticasysteem beschikt, pleegt geen misdrijf van interne indringing als hij met goede bedoelingen beveiligingsgebreken opspoort in delen van dit systeem waarvoor hij geen toegangsmachtiging heeft. Zolang de deelnemer zijn toegangsmachtiging overschrijdt zonder bedrieglijk opzet of het oogmerk om te schaden, is er geen sprake van interne indringing, die strafrechtelijk wordt bestraft.

Hoewel het de bedoeling is dat een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden voornamelijk van toepassing is op personen buiten de verantwoordelijke organisatie die geen toegangsbevoegdheid voor het informaticasysteem hebben, kan dit beleid in voorkomend geval ook een kader bieden voor de handelswijze van deelnemers met goede bedoelingen binnen de organisatie. Bij gebrek aan contractuele regels voor deze gevallen of ingeval deze regels lacunes vertonen, kan een beleid voor gecoördineerde bekendmaking van de verantwoordelijke organisatie immers daadwerkelijk worden toegepast door de partijen. Een dergelijk beleid is dus niet enkel van belang voor personen die geen juridische banden met de verantwoordelijke organisatie hebben.

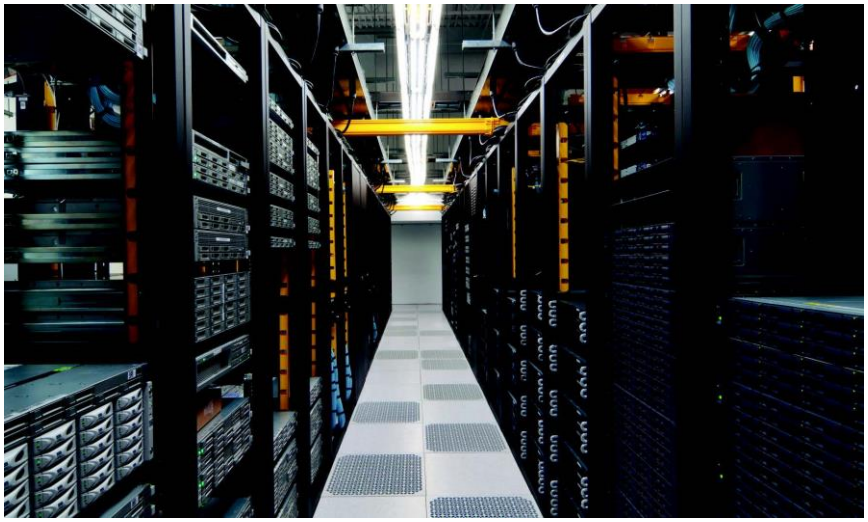
Uiteraard moeten de omstandigheden waarin een dergelijke "goedwillende" overtreding kan plaatsvinden en de in dat geval te volgen regels strikt worden begrensd in contractuele documenten[39] of in het beleid voor de gecoördineerde bekendmaking van kwetsbaarheden[40].

[39] Bijvoorbeeld een arbeidsovereenkomst, een statutaire relatie of een dienstenovereenkomst.
[40] Het kan gaan om het geval waarbij de begunstigde van een gedeeltelijke machtiging, bijvoorbeeld een werknemer van de informaticadienst, gegronde redenen heeft om te vermoeden dat er sprake is van een kwetsbaarheid, een virus, een worm, een Trojaans paard of ransomware in een deel van het systeem waarvoor hij in principe geen toegangsmachtiging heeft.

Opgelet:

De deelnemer moet er ook voor zorgen dat hij, zonder aanvullende machtiging, geen handelingen stelt met betrekking tot informaticasystemen of gegevens die worden beheerd door derden die niet onder het beleid voor gecoördineerde bekendmaking van de verantwoordelijke organisatie vallen.

Derden zijn immers niet onderworpen aan de inhoud van het beleid voor verantwoorde bekendmaking en kunnen gerechtelijke acties ondernemen wegens het gedrag van de deelnemer.



D. Inbreuk in verband met informaticagegevens[41]

Artikel 550*ter* van het Strafwetboek bestraft degene die, terwijl hij weet dat hij daartoe niet gerechtigd is, rechtstreeks of onrechtstreeks, gegevens in een informaticasysteem invoert, wijzigt of wist, of die met enig technologisch middel de normale aanwending van gegevens in een informaticasysteem verandert.

[41] De keuze voor de term "informaticasabotage" is niet ideaal aangezien hieruit ten onrechte afgeleid kan worden dat er schade is, wat geen constitutief element van het misdrijf is. Het misdrijf betreft in ruimere zin een inbreuk op de integriteit en de authenticiteit van informaticagegevens.

Afdeling 1. Materiële constitutieve elementen

1.1. Invoeren, wijzigen of verwijderen van informaticagegevens met enig technologisch middel

Het doel van het misdrijf is het invoeren, wijzigen, verwijderen van gegevens of het veranderen van de normale aanwending van gegevens met enig technologisch middel in een informaticasysteem. Deze bepaling is er hoofdzakelijk op gericht de integriteit van een informaticasysteem of van de gegevens die het systeem bevat, opslaat en overmaakt, te beschermen tegen informaticamanipulaties in ruime zin. De tussenkomst in het systeem kan rechtstreeks zijn, d.w.z. via het gebruik van een computer die rechtstreeks verbonden is met het netwerk, of onrechtstreeks, d.w.z. via een verbinding op afstand door middel van een telecommunicatienetwerk of een intermediaire computer.

In de praktijk kan het gaan om het invoeren van een virus, een logische bom, een worm, een Trojaans paard, het verwijderen of aanmaken van een bestand, het ontregelen van een besturingssysteem, het versleutelen van bestanden, het onbruikbaar maken van een harde schijf of eenvoudigweg het wijzigen van het paswoord van een gebruiker.

In tegenstelling tot wat men zou kunnen denken, is de schade geen constitutief element van het misdrijf, maar enkel een verzwarende omstandigheid. Het louter achterlaten van een vermelding in het systeem, zoals “X was hier”, is een inbreuk in verband met informaticagegevens. Er blijft echter sprake van een misdrijf ook al heeft het opzettelijk invoeren van gegevens in een computer zijn doel niet bereikt, bv. door een technische storing.

1.2. Gebrek aan machtiging

Het is de bedoeling om elke manipulatie van informaticagegevens[42] die niet vooraf werd toegestaan door de verantwoordelijke van het betrokken informaticasysteem te bestraffen. De machtiging moet betrekking hebben op de wijziging van gegevens in het informaticasysteem, ongeacht de vraag of de toegang tot het informaticasysteem al dan niet werd toegestaan.

Afdeling 2. Moreel element

De dader moet zich ervan bewust zijn geweest dat hij een ongeoorloofde handeling uitvoerde. De onopzettelijke en onbewuste overdracht van een virus als bijlage bij een mail is dus geen misdrijf in hoofde van de afzender.

[42] *Parl.St.*, Kamer, 1999-2000, nr. 50, 0213/001, blz. 19.

Afdeling 3. Verzwarende omstandigheden

1. Bedrieglijk opzet of oogmerk om te schaden

Hoewel het bestaan van een bijzonder opzet in hoofde van de dader niet vereist is voor het misdrijf, is het niettemin een verzwarende omstandigheid.[43]

2. Schade aan gegevens

De schade aan gegevens in het betrokken informaticasysteem of in enig ander informaticasysteem is een verzwarende omstandigheid van het misdrijf.[44] Het gaat hier om de wijziging van gegevens die door het informaticasysteem worden opgeslagen, overgedragen of verwerkt, in tegenstelling tot de schade aan het systeem zelf.

3. Belemmeren van de werking van het systeem

Deze verzwarende omstandigheid betreft de inbreuk met betrekking tot informaticagegevens die ertoe leidt dat de correcte werking van het betrokken of enig ander informaticasysteem geheel of gedeeltelijk wordt belemmerd.[45] Het gaat hier om de vernietiging van de inhoud, een totale of gedeeltelijke lamlegging van het informaticasysteem of een vertraging ervan, bijvoorbeeld het massaal versturen van query's om de server te overbelasten of zelfs het toebrengen, vanop afstand, van fysieke schade aan het informaticasysteem. Aangezien deze bepaling ook handelt over "enig ander informaticasysteem", betreft ze ook de uitwerking of verspreiding van computerwormen, die zichzelf automatisch kunnen vermenigvuldigen en kopiëren via communicatienetwerken. Er moet echter een oorzakelijk verband bestaan tussen het hoofdmisdrijf en de veroorzaakte voorzienbare schade.

Afdeling 4. Ter beschikking stellen van middelen om de inbreuk in verband met gegevens mogelijk te maken

Los van het misdrijf van de inbreuk in verband met informaticagegevens bestraft het Strafwetboek ook degene die onrechtmatig enig instrument, met inbegrip van informaticagegevens, dat hoofdzakelijk is ontworpen of aangepast om misdrijven van inbreuken in verband met informaticagegevens mogelijk te maken, bezit, produceert, verkoopt, verkrijgt met het oog op het gebruik ervan, invoert, verspreidt of op enige andere manier ter beschikking stelt terwijl hij weet dat deze gegevens aangewend kunnen worden om schade te berokkenen aan gegevens of, geheel of gedeeltelijk, de correcte werking van een informaticasysteem te belemmeren.[46]

[43] Zie de overwegingen over het bijzonder opzet dat vereist is voor het misdrijf van interne ongeoorloofde indringing; art. 550*ter*, § 1, van het Strafwetboek.
[44] Art. 550*ter*, § 2, van het Strafwetboek.
[45] Art. 550*ter*, § 3, van het Strafwetboek voorziet in een gevangenisstraf van één jaar tot vijf jaar en een geldboete van 26 tot 100.000 € of een van die straffen. Gelet op het belang van informaticasystemen in onze maatschappij wordt het belemmeren van de goede werking van een informaticasysteem overigens strenger bestraft dan het louter veroorzaken van schade aan gegevens.
[46] Art. 550 *ter*, § 4, van het Strafwetboek.

1. Materiële constitutieve elementen

Het misdrijf betreft het uitwerken, bezitten of ter beschikking stellen van instrumenten of informaticagegevens die hoofdzakelijk zijn ontworpen of aangepast om een inbreuk in verband met informaticagegevens te plegen. Het begrip “instrument” stemt hier overeen met dat met betrekking tot de middelen om een indringing mogelijk te maken.

2. Moreel element

Het misdrijf vereist een intentioneel element, namelijk dat de dader weet dat de instrumenten of gegevens kunnen worden aangewend om schade te berokkenen aan gegevens of de correcte werking van een informaticasysteem geheel of gedeeltelijk te belemmeren. De dader moet aldus met kennis van zaken handelen en bereid zijn om dergelijke instrumenten uit te werken, te bezitten of ter beschikking te stellen.[47] Bijgevolg is het onopzettelijk en onbewust bezitten van dergelijke instrumenten geen constitutief element van het misdrijf. Ook het louter bezitten van een programma dat zowel een wettig als een onwettig gebruik mogelijk maakt, is niet noodzakelijk een misdrijf.

Net als bij het misdrijf met betrekking tot hacker tools betekent de term “onrechtmatig” dat het opzettelijke bezit of de opzettelijke terbeschikkingstelling die wordt verantwoord door een academisch[48], wetenschappelijk of professioneel gebruik, niet strafrechtelijk wordt bestraft.

Afdeling 5. Poging

De poging wordt bestraft met dezelfde straffen als de inbreuk in verband met informaticagegevens zelf.[49]

De poging is echter maar gerealiseerd als de dader niet alleen voorbereidende handelingen maar ook eenduidige uitvoerende handelingen heeft gesteld.[50]

Afdeling 6. Beleid voor de gecoördineerde bekendmaking van kwetsbaarheden en inbreuk in verband met informaticagegevens

Door deel te nemen aan een beleid van gecoördineerde bekendmaking van kwetsbaarheden beschikt de deelnemer in principe over een machtiging om informaticagegevens in het betrokken systeem in te voeren of dit te proberen. Het is inderdaad moeilijk om veiligheidsgebreken op te sporen zonder ten

[47] O. LEROUX, "La Criminalité informatique", *op. cit.*, blz. 437.
[48] Bijvoorbeeld de opleiding informaticabeveiliging.
[49] Art. 550 *ter*, § 6, van het Strafwetboek.
[50] Zie de uiteenzetting over de poging tot indringing in een informaticasysteem.

minste te proberen gegevens in te voeren of opdrachten uit te voeren die dergelijke gegevens bevatten.

De machtiging om informaticagegevens te wijzigen of te verwijderen (of om dergelijke handelingen te proberen) hangt evenwel af van de manier waarop het beleid voor de gecoördineerde bekendmaking van kwetsbaarheden is opgesteld. Om een inbreuk in verband met informaticagegevens te vermijden, moet de deelnemer de voorwaarden van het beleid omtrent het wijzigen en verwijderen van informaticagegevens strikt naleven.

Naargelang de inhoud van het beleid voor de gecoördineerde bekendmaking van kwetsbaarheden en de naleving van deze voorwaarden door de deelnemer zal er al dan niet sprake zijn van een misdrijf betreffende een inbreuk in verband met informaticagegevens.[51]

Wat betreft de instrumenten die een inbreuk in verband met informaticagegevens mogelijk maken, kan de deelnemer dergelijke instrumenten uitwerken, bezitten of ter beschikking stellen in het kader van zijn deelname aan een beleid voor de bekendmaking van kwetsbaarheden. Die handelingen zijn niet ongeoorloofd, zolang ze verantwoord zijn door legitieme doeleinden met betrekking tot het opsporen van kwetsbaarheden met de toestemming van de organisatie van de verantwoordelijke van het betrokken informaticasysteem, en dus niet onrechtmatig worden gesteld.

Niettemin zal de deelnemer ook hier moeten bewijzen dat hij concreet deelneemt aan een bestaand beleid voor de bekendmaking van kwetsbaarheden en dat dat beleid duidelijk identificeerbaar is. De loutere intentie om hypothetisch en in het algemeen aan een dergelijk beleid deel te nemen, volstaat niet.

E. Valsheid in informatica en informaticabedrog

Afdeling 1. Valsheid in informatica[52] en het gebruik van valse stukken in informatica[53]

Artikel 210*bis* van het Strafwetboek bestraft de valsheid die erin bestaat gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, in te voeren in een informaticasysteem, te wijzigen, te wissen, of met enig ander technologisch middel de mogelijke aanwending van gegevens in een informaticasysteem te veranderen, waardoor de juridische draagwijdte van dergelijke gegevens verandert.[54]

[51] En dit misdrijf kan, in voorkomend geval, gepaard gaan met verzwarende omstandigheden.
[52] Art. 210 *bis*, § 1.
[53] Art. 550 *bis*, § 4.
[54] Art. 210*bis*, § 1, van het Strafwetboek.

Deze bepaling bestraft enerzijds ook het gebruik van gegevens verkregen door valsheid in informatica, terwijl men weet dat deze gegevens vals zijn[55], en anderzijds de poging tot het plegen van valsheid in informatica[56].

1. Materiële constitutieve elementen

1.1. Verdraaien van de waarheid op een van de manieren bepaald in de wet (invoeren, wijzigen of verwijderen van gegevens)

Valsheid is niet bij wet bepaald, maar de rechtspraak heeft verduidelijkt dat valsheid een verdraaiing van de waarheid inhoudt die rechten kan doen ontstaan tegenover derden waarvan laatstgenoemden in de praktijk onmogelijk de juistheid kunnen nagaan. Het kan bijvoorbeeld gaan om het aanmaken en gebruiken van een vals e-mailadres op naam van een derde persoon, een valse online verkoopadvertentie of een vals profiel op een sociaal netwerk. Gegevens die kunnen worden vervalst moeten dus een juridische draagwijdte hebben en zich aan de openbare trouw opdringen.[57]

Het kan gaan om informaticabestanden die zijn opgeslagen op de harde schijf van een terminal of op een optische of digitale drager (op voorwaarde dat deze wordt uitgevoerd op een systeem) of nog, om gegevens die in een netwerk worden overgedragen. De vervalsing van een papieren document waarop informaticagegevens afgedrukt zijn, valt daarentegen onder valsheid in geschrifte.[58]

1.2. Wijzigen van de juridische draagwijdte van de gegevens

Opdat het misdrijf voltrokken zou zijn, moet de manipulatie van de gegevens hebben geleid tot een wijziging van de juridische draagwijdte ervan. De juridische draagwijdte stemt overeen met de gewijzigde gegevens in hun geheel en niet met een eenheid. De wijziging kan betrekking hebben op de informaticagegevens zelf of op de gedachte die ze uitdrukken.

De parlementaire werkzaamheden vermelden bijvoorbeeld het namaken of vervalsen van kredietkaarten[59] en digitale contracten of het invoeren van een vals kredietkaartnummer in een informaticasysteem.

2. Moreel element

Het misdrijf vereist een bedrieglijk opzet of het oogmerk om te schaden.[60] Dit bijzonder opzet wordt verantwoord door het feit dat valsheid in informatica wordt gelijkgesteld met de andere categorieën van valsheid. Het bedrieglijk opzet bestaat in de wil om zichzelf of iemand anders een onrechtmatig

[55] Art. 210*bis*, § 2, van het Strafwetboek.
[56] Art. 210*bis*, § 3, van het Strafwetboek.
[57] *Parl.St.,* Kamer, 1999-2000, nr. 0213/001, blz. 10.
[58] Art. 194 e.v. van het Strafwetboek.
[59] Het betreft met name het bestraffen van "skimming", m.a.w. het illegaal kopiëren van de gegevens van een betaalkaart, dat vaak misdrijven m.b.t. valsheid in informatica, informaticabedrog en ongeoorloofde indringing in een derde informaticasysteem omvat.
[60] Zie artikel 193 van het Strafwetboek.

gewin of voordeel te verschaffen. Het oogmerk om te schaden betreft de wil om een natuurlijk of rechtspersoon schade te berokkenen.

Vergissingen, nalatigheden of onvoorzichtigheden alleen volstaan dus niet om een misdrijf van valsheid in informatica te vormen.

Ook het aanmaken of gebruiken van een vals stuk in informatica wordt niet strafrechtelijk bestraft als de dader handelt met het oog op wetenschappelijke, professionele of onderwijsdoeleinden.

3. Poging

De poging om valsheid in informatie te plegen wordt ook strafbaar gesteld, zonder dat er dus effectief schade moet zijn berokkend.

Niettemin houdt de poging zowel voorbereidende handelingen in als uitvoerende handelingen die geen twijfel laten bestaan over het misdadig opzet van de dader.[61]

Afdeling 2. Informaticabedrog

Artikel 504*quater* van het Strafwetboek stelt degene strafbaar die, met bedrieglijk opzet, beoogt een onrechtmatig economisch voordeel voor zichzelf of voor een ander te verwerven, door gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, in een informaticasysteem in te voeren, te wijzigen of te wissen of met enig technologisch middel de normale aanwending van gegevens in een informaticasysteem te veranderen.

1. Materiële constitutieve elementen

1.1. Manipuleren van gegevens

Het misdrijf impliceert het invoeren, wijzigen[62] of verwijderen van gegevens in een informaticasysteem of het gebruik van eender welke technologie om de normale aanwending van gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem te veranderen (zie *supra* valsheid in informatica).

1.2. Nastreven van een onrechtmatig economisch voordeel

Het misdrijf vereist niet dat het beoogde onrechtmatig economisch voordeel concreet verworven wordt, maar het louter nastreven van een dergelijk doel, ook al is dat doel uiteindelijk niet bereikt. Informaticabedrog is een misdrijf waarbij een louter risico volstaat of "formeel" misdrijf, waarbij enkel moet worden aangetoond dat de gegevensverwerking in oorzakelijk verband staat met het nastreven

[61] Zie de poging tot indringing in een informaticasysteem.
[62] Bijvoorbeeld het wijzigen van het saldo op een bankrekening.

van een onrechtmatig economisch voordeel. Het economisch voordeel[63] kan rechtstreeks of onrechtstreeks zijn en verschillende vormen aannemen: materiële goederen, immateriële goederen, dienstverlening. Het kan ten voordele van de dader of van een andere persoon zijn.

2. Moreel element

Informaticabedrog veronderstelt niet alleen dat de dader het misdrijf wetens en willens pleegde, maar ook dat hij een bijzonder opzet nastreefde, namelijk een bedrieglijk opzet om voor zichzelf of voor iemand anders een onrechtmatig economisch voordeel te verwerven.

3. Poging

De poging tot informaticabedrog wordt ook bestraft.[64]

Ook hier zal de poging pas bewezen zijn als het openbaar ministerie aantoont dat de dader niet alleen voorbereidende handelingen maar ook eenduidige uitvoerende handelingen heeft gesteld.

Afdeling 3. Beleid voor de gecoördineerde bekendmaking van kwetsbaarheden, valsheid in informatica en informaticabedrog

Aangezien valsheid in informatica een bedrieglijk opzet of het oogmerk om te schaden vereist, sluit de deelname aan een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden dit misdrijf in hoofde van de deelnemer uit. In dezelfde zin loopt de deelnemer aan een beleid voor gecoördineerde bekendmaking of een beloningsprogramma voor kwetsbaarheden in principe geen gevaar strafrechtelijk te worden vervolgd voor informaticabedrog, aangezien er geen sprake is van bedrieglijk opzet in hoofde van de deelnemer.

F. Misdrijven betreffende het geheim van communicatie

Afdeling 1. Misdrijven betreffende het geheim van niet voor het publiek toegankelijke communicatie en gegevens van een informaticasysteem

Artikel 314*bis* van het Strafwetboek bestraft eenieder die, opzettelijk en met behulp van enig toestel, niet voor het publiek toegankelijke communicatie, waaraan hij niet deelneemt, onderschept of doet onderscheppen, er kennis van neemt of doet van nemen, opneemt of doet opnemen, zonder de toestemming van alle deelnemers aan die communicatie.[65]

[63] Artikel 504*quater* vereiste voorheen dat de dader voor zichzelf of voor een ander een bedrieglijk vermogensvoordeel verwierf, wat niet volledig in overeenstemming was met artikel 8 van het Cybercrimeverdrag van de Raad van Europa: *Parl.St.*, Kamer, 2003-2004, 1284/001, blz. 6 en 8.
[64] Zie de overwegingen met betrekking tot een poging tot ongeoorloofde indringing.
[65] Art. 314*bis*, § 1, 1°, van het Strafwetboek.

1. Materieel element

1.1. Onderscheppen, kennisnemen van of opnemen met behulp van een toestel

Bij gebrek aan een wettelijke definitie moet het onderscheppen, kennisnemen of opnemen van communicatie worden begrepen in de zin van het normale taalgebruik. Eerst en vooral bestaat het onderscheppen erin communicatie die aan iemand anders is gericht, aan iemand anders wordt verstuurd of voor iemand anders is bestemd, onderweg, bij verrassing, op te vangen. Vervolgens betekent het kennisnemen van communicatie het op de hoogte zijn van het bestaan en de inhoud van communicatie tussen personen hoewel men niet de bestemmeling van deze communicatie is. Dit laatste begrip heeft een ruime betekenis en is ook toepasselijk op technische vormen van communicatie, zoals elektronische gegevensoverdracht. Tot slot betreft het opnemen het vastleggen van gegevens op een lokale materiële drager of op een materiële drager op afstand[66], om deze later te kunnen gebruiken.

De strafbaarstelling van het onderscheppen van communicatie heeft tot doel om naast de dader van het misdrijf ook de opdrachtgever ervan te bestraffen.[67]

De bepaling verduidelijkt nog dat het onderscheppen[68], kennisnemen van of opnemen moet gebeuren met behulp van enig toestel[69]. Dat is een ruime formulering, maar ze houdt noodzakelijkerwijs het gebruik van een technisch hulpmiddel in. Zo niet zijn de feiten niet strafbaar. Aan deze vereiste lijkt te zijn voldaan zodra een informaticamanipulatie wordt uitgevoerd of een programma wordt gebruikt.[70]

1.2. Niet voor het publiek toegankelijke communicatie waaraan men niet deelneemt

Artikel 314*bis* van het Strafwetboek verduidelijkt voortaan dat de bedoelde communicatie “niet voor het publiek toegankelijke communicatie” is en niet langer “privécommunicatie of -telecommunicatie”.[71] Dit begrip lijkt net als voorheen te kunnen worden geïnterpreteerd in functie

[66] Bijvoorbeeld via een cloudopslagdienst.
[67] *Parl.St.*, Senaat, 1992-1993, nr. 843/1, blz. 8-9.
[68] De bepaling vereist voortaan niet meer dat de communicatie “tijdens de overbrenging ervan” wordt onderschept. De parlementaire werkzaamheden verklaren deze aanpassing door het feit dat de nieuwe ontwikkelingen op informaticagebied het vaak onmogelijk maken om precies uit te maken wanneer communicatie nog in “overbrenging” is, dan wel reeds afgeleverd. Het is immers moeilijk te bepalen of een ongelezen e-mail moet worden beschouwd als afgeleverde communicatie of als communicatie die wordt overgebracht. *Parl.St.*, Kamer, 2015-2016, nr. 1966/001, blz. 54.
[69] *Parl.St.*, Senaat, 1992-1993, nr. 843/1, blz. 6.
[70] Omgekeerd valt het louter rechtstreeks op een computerscherm weergeven van een e-mail of een webpagina, die open worden gelaten en waarop geen enkele manipulatie wordt uitgevoerd, niet onder het misdrijf.
[71] Artikel 32 van de wet van 25 december 2016 houdende diverse wijzigingen van het Wetboek van strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties en tot oprichting van een gegevensbank stemafdrukken, *BS*

van de context en de bedoelingen van de deelnemers aan de communicatie.[72] Het niet voor het publiek toegankelijke karakter houdt in dat de communicatie niet bestemd is om door andere personen dan de correspondenten van de communicatie te worden gehoord.[73] Het al dan niet beroepsmatige karakter van een communicatie heeft in principe geen gevolgen voor het beoordelen van de niet voor het publiek toegankelijke aard.[74]

De communicatie betreft met name de elektronische gegevensoverdracht in computers en computernetwerken.[75] Hiermee worden met name e-mails bedoeld.

De bepaling stelt enkel de personen strafbaar die niet deelnemen aan de communicatie. Omgekeerd pleegt de persoon die deelneemt aan een niet voor het publiek toegankelijke communicatie en die deze communicatie opneemt, zelfs zonder dat de andere deelnemers dat weten, geen misdrijf in de zin van artikel 314*bis* van het Strafwetboek.

1.3. Ontbreken van de toestemming van de deelnemers

Om aan het misdrijf te ontkomen, moet men vooraf de toestemming hebben gekregen van alle deelnemers aan de elektronische communicatie en niet alleen van sommigen onder hen. De toestemming van de deelnemers, die voortvloeit uit een geheel van omstandigheden, kan uitdrukkelijk of stilzwijgend zijn, voor zover ze duidelijk is. Sommige auteurs voegen hieraan toe dat deze toestemming noodzakelijkerwijs op specifieke en individuele wijze moet zijn gegeven, en niet mag zijn afgeleid uit een voorafgaand akkoord dat bijvoorbeeld is opgenomen in een clausule van een arbeidsovereenkomst of van een huishoudelijk reglement. De toestemming zou tevens op eerlijke wijze moeten zijn verkregen en met inachtneming van het eventuele aan de deelnemers meegedeelde doel.

2. Moreel element

Het misdrijf vereist uitdrukkelijk dat de dader opzettelijk, dat wil zeggen wetens en willens, handelt. De parlementaire werkzaamheden vermeldden duidelijk dat louter toeval of onbescheidenheid niet

van 17 januari 2017, blz. 2738. De parlementaire werkzaamheden verantwoorden deze wijziging als een terminologische aanpassing, rekening houdend met de wijzigingen in de artikelen 90*ter* e.v. van het Wetboek van strafvordering.

[72] *Parl.St.*, Senaat, 1992-1993, nr. 843/1, blz. 6. De parlementaire werkzaamheden lichten ook toe dat het begrip "niet voor het publiek toegankelijke communicatie" betrekking heeft op communicatie of elektronische communicatie die zich in de privésfeer afspeelt. Het is dus een overkoepelend begrip dat ook de vroegere termen “privécommunicatie of -telecommunicatie” omvat: *Parl.St.*, Kamer, 2015-2015, nr. 1966/001, blz. 53.

[73] *Parl.St.*, Senaat, 1992-1993, nr. 843/1, p. 7. Commissie voor de bescherming van de persoonlijke levenssfeer, aanbeveling nr. 08/2012 van 2 mei 2012 betreffende de controle door de werkgever op het gebruik van elektronische communicatie-instrumenten op de werkvloer, www.privacycommission.be.

[74] *Parl.St.*, Senaat, 1992-1993, nr. 843/1, blz. 8 en nr. 843/2, blz. 10 en 36.

[75] In die zin: *Parl.St.*, Senaat, 1992-1993, nr. 843/1, blz. 7.

volstaat om van een misdrijf te spreken.[76] Bijgevolg is de louter toevallige ontdekking van niet voor het publiek toegankelijke communicatie niet strafbaar. Wie opzettelijk maar louter uit nieuwsgierigheid handelt, begaat evenwel een misdrijf.[77] Zo is bijvoorbeeld het toevallig kennisnemen van de inhoud van communicatie door een technicus tijdens de controle van de goede werking van een informaticasysteem niet strafbaar, behalve indien hij opzettelijk uit nieuwsgierigheid heeft gehandeld.

Afdeling 2. Voorbereidende handelingen

1. Opstellen van een toestel

1.1. Materieel element

Het Strafwetboek stelt degene strafbaar die enig toestel opstelt of doet opstellen dat het ongeoorloofd onderscheppen, kennisnemen of opnemen van communicatie mogelijk maakt.[78] Het toestel wordt immers niet noodzakelijk door of in opdracht van dezelfde personen geplaatst en gebruikt.[79]

1.2. Moreel element

Het misdrijf vereist dat de dader handelt met het opzet een ongeoorloofde onderschepping, kennisneming of opname te plegen.

2. Ter beschikking stellen van een instrument

2.1. Materiële constitutieve elementen

De wetgever bestraft degene die, onrechtmatig, een instrument, met inbegrip van informaticagegevens, dat hoofdzakelijk is ontworpen of aangepast om het ongeoorloofd onderscheppen van communicatie mogelijk te maken, bezit, produceert, verkoopt, verkrijgt met het oog op het gebruik ervan, invoert, verspreidt of op enige andere manier ter beschikking stelt.[80]

Onder het begrip "instrument" worden de toegangsmiddelen of andere tools verstaan die ontworpen zijn om bijvoorbeeld gegevens te wijzigen of te vernietigen, of om binnen te dringen in de werking van systemen, zoals virusprogramma's, ofwel programma's die ontworpen of aangepast zijn om binnen te dringen in informaticasystemen.[81]

[76] *Parl.St.*, Senaat, 1992-1993, nr. 843/1, blz. 6.
[77] *Parl.*St., Senaat, 1992-1993, nr. 843/1, blz. 6.
[78] Art. 314*bis*, § 1, 2°, van het Strafwetboek.
[79] *Parl.St.*, Senaat, 1992-1993, nr. 843/1, blz. 9.
[80] Art. 314*bis*, §2*bis*, van het Strafwetboek.
[81] *Parl.St.*, Kamer, 2003-2004, nr. 1284/001, blz. 6.

2.2. Moreel element

Zoals bij het ter beschikking stellen van middelen om een ongeoorloofde indringing mogelijk te maken, moet de dader wetens en willens een dergelijk instrument hebben ontwikkeld, in zijn bezit hebben gehad of ter beschikking hebben gesteld. Hij moet er dus van op de hoogte zijn geweest dat het strafbare instrument hoofdzakelijk werd ontworpen of aangepast om het ongeoorloofd onderscheppen, opnemen en kennisnemen van communicatie mogelijk te maken.

De term "onrechtmatig" betekent niettemin dat het bezitten of ter beschikking stellen van een dergelijk instrument voor legitieme doeleinden, zoals wetenschappelijke of professionele doeleinden op het gebied van de beveiliging van communicatiesystemen, niet strafbaar is.

Afdeling 3. Helen van onrechtmatig verkregen communicatie

Het Strafwetboek bestraft degene die wetens de inhoud van niet voor het publiek toegankelijke communicatie of van gegevens van een informaticasysteem die onwettig onderschept of opgenomen zijn of waarvan onwettig kennisgenomen is, onder zich houdt, aan een andere persoon onthult of verspreidt, of wetens enig gebruik maakt van een op die manier verkregen inlichting.[82]

1. Materieel element

1.1. Inhoud van niet voor het publiek toegankelijke communicatie of van gegevens van een informaticasysteem die onwettig onderschept of opgenomen zijn of waarvan onwettig kennisgenomen is

De persoon die bij vergissing of toevallig communicatie ontvangt die niet voor hem bestemd was, pleegt geen misdrijf.

1.2. Onder zich houden, aan een andere persoon onthullen of verspreiden of op enige manier gebruiken

Wat deze begrippen betreft, wordt verwezen naar de toelichting over het helen van onrechtmatig verkregen informaticagegevens.

2. Moreel element

Men moet "wetens" hebben gehandeld, dat wil zeggen opzettelijk en met kennis van zaken over de onwettigheid van de verkregen informatie.

[82] Art. 314*bis*, § 2, van het Strafwetboek.

Afdeling 4. Poging

De poging tot het ongeoorloofd onderscheppen van niet voor het publiek toegankelijke communicatie wordt eveneens bestraft.[83]

Hiervoor moet worden bewezen dat voorbereidende en uitvoerende handelingen zijn gesteld die geen twijfel laten over het misdadig opzet van de dader.

Afdeling 5. Geheimhouding van elektronische communicatie

Artikel 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie voorziet in strafrechtelijke sancties voor verschillende gedragingen die in strijd zijn met de geheimhouding van elektronische communicatie, die beschermd wordt door artikel 124 van dezelfde wet.

Deze verschillende sancties zijn gericht op het waarborgen van het vertrouwelijke karakter van de informatie die over een elektronische-communicatienetwerk wordt verzonden.[84]

1. Materiële constitutieve elementen

1.1. Toestemming van de direct of indirect betrokken personen

Ondanks de in de wet gehanteerde ruime formulering, die doet veronderstellen dat alle personen die direct of indirect betrokken zijn bij de communicatie en de inhoud ervan hun toestemming zouden moeten geven[85], lijkt het niettemin redelijker ervan uit te gaan dat enkel de personen aan wie de communicatie rechtstreeks of onrechtstreeks gelinkt is, moeten instemmen met de kennisneming, namelijk de afzender en de ontvanger(s). Wat verbindingsgegevens of gegevens van geraadpleegde webpagina's betreft, volstaat het de toestemming van de betrokken gebruiker te verkrijgen.

1.2. Met opzet kennisnemen door iemand van het bestaan van informatie van alle aard die via elektronische weg is verstuurd en die niet persoonlijk voor hem bestemd is[86]

1.2.1. Via elektronische weg verstuurde informatie

In de wet van 13 juni 2005 wordt het begrip "elektronische communicatie" onrechtstreeks gedefinieerd via de definitie van *elektronische-communicatiedienst*, zijnde "een gewoonlijk tegen vergoeding aangeboden dienst die geheel of hoofdzakelijk bestaat in het overbrengen, waaronder

[83] Art. 314*bis*, § 3, van het Strafwetboek. Zie Corr. Brussel, 8 januari 2008, *J.T.*, 2008, blz. 337, voor een voorbeeld van een poging tot het onderscheppen van communicatie d.m.v. een "keylogger", m.a.w. spyware die de activiteit (toetsaanslagen) van een computer registreert en doorstuurt naar een derde.
[84] *Parl.St*., Senaat, 2004-2005, nr. 1425-1426/01, blz. 76.
[85] Commissie voor de bescherming van de persoonlijke levenssfeer, advies nr. 8/2004 van 14 juni 2004 over het voorontwerp van wet betreffende de elektronische communicatie, blz. 7,www.privacycommission.be: de CBPL vroeg zich af of een persoon die in het bericht zelf wordt vermeld volgens de wet als zijnde indirect betrokken bij de communicatie moest worden beschouwd, wat veel verder ging dan de Europese tekst.
[86] Art. 124, eerste lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie.

schakel- en routeringsverrichtingen, van signalen via elektronische-communicatienetwerken (...)" en van *elektronische-communicatienetwerk*, zijnde "de transmissiesystemen en, in voorkomend geval, de schakel- of routeringsapparatuur en andere middelen, waaronder netwerkelementen die niet actief zijn, die het mogelijk maken signalen over te brengen via draad, radiogolven, optische of andere elektromagnetische middelen (...)"[87]. In het Wetboek van economisch recht wordt "elektronische post" gedefinieerd als een "tekst-, spraak-, geluids- of beeldbericht dat over een openbaar communicatienetwerk wordt verzonden en in het netwerk of in de eindapparatuur van de ontvanger kan worden opgeslagen tot het door de afnemer wordt opgehaald".[88]

Het begrip "elektronische communicatie" omvat telefonische communicatie, e-mails, sms'en, berichten die worden verstuurd via een draadloos netwerk of de uitwisseling van cellulaire gegevens, verbindingen met een netwerk of met een informaticasysteem. Dit begrip omvat dus e-mails en internetverbindingsgegevens die het mogelijk maken de geraadpleegde websites te identificeren.

De kennisneming betreft de informatie in haar geheel, met inbegrip van de inhoud van elektronische post.[89] De persoon die heeft kennisgenomen van het bestaan van elektronische post en er gebruik van heeft gemaakt, heeft immers noodzakelijkerwijs gelijktijdig kennisgenomen van de inhoud ervan. De kennisneming en het gebruik van de inhoud van een e-mail hangen samen met de kennisneming en het gebruik van het bestaan van die elektronische post.[90] We kunnen ervan uitgaan dat artikel 124 van de wet van 15 juni 2005 dus een belemmering vormt voor de kennisneming van de inhoud van elektronische communicatie.

1.2.2. Informatie van alle aard die niet persoonlijk voor hem bestemd is

De kennisneming van informatie van alle aard die persoonlijk bestemd is voor degene die ervan kennisneemt, vormt geen schending van artikel 124, eerste lid, van de wet van 13 juni 2005.

1.3. Met opzet identificeren van de personen die bij het versturen van de informatie en de inhoud ervan betrokken zijn

Artikel 124, tweede lid, verbiedt de identificatie van de personen die zowel bij het versturen van de informatie als bij de inhoud ervan betrokken zijn. Dit betreft zowel de identiteitsgegevens van de afzender, van de ontvanger(s) van de berichten als die van de bij de inhoud betrokken personen (bijvoorbeeld deze vermeld in de e-mail).

---

[87] Art. 2, 3° en 5°, van de wet van 13 juni 2005 betreffende de elektronische communicatie, *BS* van 20 juni 2005, blz. 28070.
[88] Wet van 15 december 2013 houdende invoeging van Boek XII, "Recht van de elektronische economie", in het Wetboek van economisch recht, en houdende invoeging van de definities eigen aan Boek XII en van de rechtshandhavingsbepalingen eigen aan Boek XII, in de Boeken I en XV van het Wetboek van economisch recht.
[89] Cass., 1 okt. 2009, C.08.0064.N, www.cass.be. De rechtsleer twijfelde of ervan moest worden uitgegaan dat artikel 124 niet alleen betrekking had op het bestaan van informatie, maar ook op de inhoud van de informatie zelf. Zie Commissie voor de bescherming van de persoonlijke levenssfeer, advies nr. 8/2004 van 14 juni 2004 over het voorontwerp van wet betreffende de elektronische communicatie, blz. 7, www.privacycommission.be: "Dit artikel heeft als doel de communicaties (zowel de inhoud als de verkeersgegevens) zodanig te beschermen dat er geen andere persoon kennis van kan nemen noch kan manipuleren dan de partijen die aan de communicatie hebben deelgenomen".
[90] *Ibidem.*

1.4. Met opzet kennisnemen van gegevens inzake elektronische communicatie en met betrekking tot een andere persoon[91]

Gegevens inzake elektronische communicatie zijn gegevens die via netwerken worden verzonden, zoals de e-mailadressen van afzender en ontvanger, het tijdstip van verzending en ontvangst, de routeringsgegevens, de grootte van het bericht, de aanwezigheid van bijlagen enz.[92]

De kennisneming bestaat in het op de hoogte zijn van het bestaan en de inhoud van gegevens inzake elektronische communicatie tussen personen hoewel men niet de ontvanger van deze communicatie is.

1.5. Wijzigen, schrappen, kenbaar maken, opslaan of op enige wijze gebruikmaken van de informatie, identificatie of gegevens die met of zonder opzet werden verkregen[93]

Het is verboden de informatie, de identificatie of de gegevens die met opzet maar ook toevallig werden verkregen te wijzigen, te schrappen, kenbaar te maken, op te slaan of er enig gebruik van te maken.

2. Moreel element

Deze bepaling houdt in dat de strafbaar gestelde handelingen met opzet moeten worden verricht door de dader van het misdrijf. Als wordt vastgesteld dat de kennisneming van elektronische communicatie toevallig heeft plaatsgevonden, ontbreekt het intentionele karakter van de ontdekking en is artikel 124 van de wet van 13 juni 2005 niet van toepassing.[94] Bijgevolg moet een onderscheid worden gemaakt tussen de actieve en de louter toevallige kennisneming van elektronische communicatie.

3. Uitzonderingen bepaald in artikel 125 van de wet

Artikel 125 van de wet van 13 juni 2005 betreffende de elektronische communicatie voorziet in een aantal uitzonderingen op de geheimhouding van communicatie bedoeld in artikel 124 van dezelfde wet en in artikel 314*bis* van het Strafwetboek. Deze bepaling maakt het onder andere[95] mogelijk om de in principe verboden handelingen te stellen wanneer ze nodig zijn om de goede werking van het netwerk na te gaan en om de goede uitvoering van een elektronische-communicatiedienst te garanderen. Door de algemene bewoordingen van de wet lijkt deze bepaling zowel toepasselijk te zijn op een openbaar elektronische-communicatienetwerk als op een privénetwerk.

[91] Art. 124, derde lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie.
[92] Arbh. Brussel, 10 februari 2004, R.G. 44002, www.juridat.be.
[93] Art. 124, vierde lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie.
[94] Arbh. Bergen, 8 dec. 2010, *JLMB*, 2011, blz. 715; *Chron. D.S.*, 2011, blz. 399; Arbh. Brussel, 4 december 2007, *J.T.T.*, 2008, blz. 179; Arbrb. Luik, 19 maart 2008, RG 360.454, www.juridat.be.
[95] Art. 125, § 1, 1°, van de wet van 13 juni 2005 betreffende de elektronische communicatie voorziet ook in de mogelijkheid van een afwijking wanneer de wet het stellen van de aangeklaagde handelingen toestaat of oplegt. Volgens de Privacycommissie zou artikel 16 van de wet van 3 juli 1978 betreffende de arbeidsovereenkomsten een wettelijke basis vormen mits bepaalde voorwaarden worden nageleefd.

Voor zover dit kan worden verantwoord door strikt technische maatregelen is het dus mogelijk om de handelingen bedoeld in artikel 124 te stellen. De informatie inzake elektronische communicatie die bij deze gelegenheid ontdekt wordt, mag echter niet voor andere doeleinden worden gebruikt dan het nagaan van de goede werking van het netwerk.

4. Bedrieglijke elektronische communicatie[96]

1. Materiële constitutieve elementen

Het gaat om het op bedrieglijke wijze tot stand brengen van elektronische communicatie door middel van een elektronische-communicatienetwerk.

2. Moreel element

Naast het wetens en willens handelen impliceert dit misdrijf ook dat de dader een bijzonder opzet had, namelijk zichzelf of een andere persoon wederrechtelijk een voordeel verschaffen.

3. Poging en voorbereidende handelingen[97]

De wet stelt ook de persoon strafbaar die op bedrieglijke wijze elektronische communicatie tot stand probeert te brengen of enig toestel opstelt dat bestemd is om dergelijke communicatie tot stand te brengen.

Net als de andere pogingen vereist ook deze poging dat wordt bewezen dat de dader voorbereidende en eenduidige uitvoerende handelingen heeft gesteld.

5. Ongeoorloofd gebruik van een elektronische-communicatienetwerk of -dienst[98]

1. Materiële constitutieve elementen

De wet bestraft de persoon die een elektronische-communicatienetwerk of -dienst of andere elektronische communicatiemiddelen gebruikt met een ongeoorloofd doel.

[96] Art. 145, § 3, 1°, van de wet van 13 juni 2005 betreffende de elektronische communicatie.
[97] Art. 145, § 3, 3°, van de wet van 13 juni 2005 betreffende de elektronische communicatie.
[98] Art. 145, § 3*bis*, van de wet van 13 juni 2005 betreffende de elektronische communicatie.

2. Moreel element

Het misdrijf houdt in dat de dader overlast wil veroorzaken aan zijn correspondent of schade wil berokkenen.

3. Poging en voorbereidende handelingen

De wet stelt ook de persoon strafbaar die enig toestel opstelt dat bestemd is om ongeoorloofd gebruik te maken van een elektronische-communicatienetwerk of -dienst, alsook de poging hiertoe.

Voor de poging moet worden aangetoond dat de dader voorbereidende handelingen en eenduidige uitvoerende handelingen heeft gesteld.

Afdeling 6. Beleid voor de gecoördineerde bekendmaking van kwetsbaarheden en communicatie

Het is de deelnemer niet toegestaan opzettelijk, met enig toestel, niet voor het publiek toegankelijke communicatie te onderscheppen, ervan kennis te nemen of op te nemen.[99] Dit is overigens niet noodzakelijk bij de uitvoering van een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden.

Het onderscheppen, kennisnemen of opnemen van niet voor het publiek toegankelijke communicatie door de deelnemer is evenwel geen misdrijf als dit ofwel toevallig, ofwel met de toestemming van alle deelnemers aan de betrokken communicatie[100], ofwel met de deelname van de deelnemer zelf aan de communicatie gebeurt.

Ook kan een deelnemer, zonder een misdrijf te plegen, een toestel opstellen of doen opstellen dat het mogelijk maakt om niet voor het publiek toegankelijke communicatie te onderscheppen, ervan kennis te nemen of op te nemen voor zover hij handelt zonder de bedoeling om het betrokken toestel te gebruiken voor bovengenoemde doeleinden of met de toestemming van alle deelnemers, ofwel zelf deelneemt aan de communicatie.

Bovendien kan een deelnemer een instrument dat het onderscheppen, kennisnemen of opnemen van niet voor het publiek toegankelijke communicatie mogelijk maakt, uitwerken, bezitten of ter beschikking stellen van een andere deelnemer. Dit is evenwel alleen gewettigd in het kader van een

[99] Art. 314*bis* van het Strafwetboek.
[100] Hoewel dit in veel situaties niet vanzelfsprekend is, is het niet uitgesloten dat de deelnemer in het kader van het beleid voor gecoördineerde bekendmaking beschikt over de toestemming van de deelnemers aan de communicatie.

werkelijke deelname aan een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden. Dit instrument kan immers aantonen dat kwetsbaarheden in het informaticasysteem kunnen leiden tot een ongeoorloofde kennisneming van communicatie.

De opzettelijke poging om niet voor het publiek toegankelijke communicatie te onderscheppen, op te nemen of er kennis van te nemen is daarentegen slechts verantwoord zijn in het kader van de uitvoering van een beleid voor gecoördineerde bekendmaking als de deelnemer over de toestemming van alle deelnemers beschikt of zelf deelneemt aan de communicatie.

Als de deelnemer redelijkerwijs niet kon weten dat de inhoud van niet voor het publiek toegankelijke communicatie of van gegevens van een informaticasysteem onwettig werd verkregen, kan hij deze gebruiken, bijhouden, onthullen of verspreiden. Omgekeerd moet de deelnemer die weet dat dergelijke informatie onwettig werd verkregen, zich er strikt van onthouden deze te helen in het kader van zijn deelname aan een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden.

Gelet op de goede bedoelingen van de deelnemer moet deze in principe geen bedrieglijke elektronische communicatie tot stand brengen of een elektronische-communicatienetwerk of -dienst op ongeoorloofde wijze gebruiken.

Tot slot heeft een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden zeker niet tot doel om opzettelijk kennis te nemen van informatie, van de identiteit van communicerende personen of van gegevens inzake elektronische communicatie of deze te wijzigen. Als de deelnemer deze handelingen moet stellen, gebeurt dit toevallig of met de toestemming van alle betrokken deelnemers, ofwel is de communicatie persoonlijk voor hem bestemd. De uitvoering van een beleid voor gecoördineerde bekendmaking heeft daarentegen tot doel de vertrouwelijkheid van de door de verantwoordelijke organisatie uitgewisselde elektronische communicatie te bevorderen.

Volgens ons kan de deelnemer aan een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden zich eventueel beroepen op de toepassing van artikel 125 van de wet van 13 juni 2005 betreffende de elektronische communicatie, dat het mogelijk maakt af te wijken van de geheimhouding van elektronische communicatie. De handelingen die door een deelnemer worden gesteld in het kader van een beleid voor gecoördineerde bekendmaking kunnen tot doel hebben de goede werking van een elektronische-communicatienetwerk of -dienst na te gaan, met inbegrip van de veiligheid ervan.

G. Naleving van andere wettelijke bepalingen

Naast de bepalingen inzake cybercriminaliteit moeten de deelnemers aan een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden rekening houden met andere wettelijke bepalingen, waaronder de wetgeving betreffende de verwerking van persoonsgegevens.[101]

Een beleid voor gecoördineerde bekendmaking heeft niet tot doel om intentioneel persoonsgegevens te verwerken. De verantwoordelijke organisatie zal echter hoogstwaarschijnlijk persoonsgegevens moeten verwerken als verwerkingsverantwoordelijke of als verwerker. Het is dus mogelijk dat de deelnemer, zelfs toevallig, persoonsgegevens moet verwerken die worden opgeslagen, verwerkt of overgedragen in het betrokken informaticasysteem. Het kan ook nodig zijn dat een deelnemer, in het kader van zijn onderzoek naar kwetsbaarheden, persoonsgegevens verwerkt om het bestaan van een kwetsbaarheid aan te tonen.

Afdeling 1. Begrippen in verband met persoonsgegevens

1. Persoonsgegevens

De AVG verstaat onder persoonsgegevens alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Gegevens zijn identificeerbaar indien ze het mogelijk maken om een natuurlijke persoon direct of indirect te identificeren, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.[102] Het "identificeerbare" karakter van de persoon hangt niet af van de loutere wil tot identificatie van de gegevensverwerker, maar van de mogelijkheid om de persoon direct of indirect te identificeren aan de hand van deze gegevens (bijvoorbeeld: een e-mailadres, identificatienummer, online identificator, IP-adres of nog, locatiegegevens).

2. Verwerking

De verwerking van persoonsgegevens heeft een ruime betekenis en omvat "een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door

[101] Europese verordening nr. 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Algemene verordening gegevensbescherming, hierna "AVG") en tot intrekking van Richtlijn 95/46/EG, alsook de Belgische wetten in dit verband waaronder de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, *BS* van 10 januari 2018, blz. 989.

[102] Art. 4, 1), van de AVG.

middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens".[103] Kortom, het begrip "verwerking" omvat nagenoeg alle bewerkingen die betrekking kunnen hebben op persoonsgegevens.

Zo wordt het gewoon verzamelen of raadplegen van persoonsgegevens als een verwerking van deze gegevens beschouwd.[104]

3. Verwerkingsverantwoordelijke

De verwerkingsverantwoordelijke is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.[105]

De hoedanigheid van verwerkingsverantwoordelijke vloeit dus voort uit de bevoegdheid om vast te stellen voor welke doeleinden persoonsgegevens worden verwerkt.

3.1. Bevoegdheid tot vaststelling

De bevoegdheid tot vaststelling betekent voor een entiteit dat ze ervoor kan kiezen persoonsgegevens te verwerken voor haar eigen doeleinden[106]. Het begrip "verwerkingsverantwoordelijke" is een functioneel begrip, dat is bedoeld om verantwoordelijkheden toe te kennen aan personen die een feitelijke invloed uitoefenen. Het is dus meer op een feitelijke dan op een formele analyse gebaseerd.[107]

In de praktijk dient dus te worden nagegaan waarom een verwerking plaatsvindt en wie concreet beslist heeft om deze uit te voeren.

---

[103] Art. 4, 2), van de AVG.
[104] C. DE TERWANGNE, Vie privée et données à caractère personnel, hoofdstuk 3.2 Analyse détaillée de la loi de protection des données et de son arrêté royal d'exécution, Brussel, Uitg. Politeia, blz. 23.
[105] Art. 4, 7), van de AVG: wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.
[106] C. DE TERWANGNE, Vie privée et données à caractère personnel, hoofdstuk 3.2 Analyse détaillée de la loi de protection des données et de son arrêté royal d'exécution, Brussel, Uitg. Politeia, blz. 26.
[107] Groep van artikel 29, advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", WP 169, blz. 10, (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_nl.pdf)

3.2. Vaststelling van het doel en de middelen

De verwerkingsdoeleinden zijn de doelstellingen van de verwerkingsacties. De middelen zijn de toegepaste technische en organisatorische methoden[108] om de verwerkingsdoeleinden te bereiken. In feite is het de bedoeling om het "waarom" en het "hoe" van de verwerkingsactiviteiten te bepalen.[109]

Deze beide elementen moeten voorhanden zijn om als verwerkingsverantwoordelijke te worden beschouwd.

De vaststelling van de middelen moet betrekking hebben op de technische en organisatorische wezenlijke aspecten van de verwerking (bijvoorbeeld, de te verwerken gegevens, de verwerkingsduur of de personen die toegang mogen hebben tot de gegevens).[110]

4. Verwerker

De verwerker is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.[111] De verwerker handelt ten behoeve van de verwerkingsverantwoordelijke door zijn instructies op te volgen, in ieder geval wat het doel van de verwerking en de wezenlijke aspecten van de middelen voor de verwerking betreft.

Afdeling 2. Juridische invulling van de rol van deelnemer

Het beleid voor verantwoorde bekendmaking is een vorm van toetredingsovereenkomst die de ethische hacker ten aanzien van de verwerkingsverantwoordelijke[112] bindt. Zo worden het doel van en de essentiële middelen voor de verwerking van persoonsgegevens, in principe, vastgesteld door de verantwoordelijke organisatie en niet door de deelnemer in het kader van een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden. In dat geval moet de deelnemer de wettelijke verplichtingen inzake bescherming van persoonsgegevens naleven in de hoedanigheid van verwerker van de verantwoordelijke organisatie.[113]

---

[108] C. DE TERWANGNE, *idem*, blz. 28.
[109] Groep van artikel 29, advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", WP 169, blz. 14, *idem*.
[110] *Ibidem*.
[111] Art. 4, 8), van de AVG.
[112] of ten aanzien van de verwerker, indien de verantwoordelijke organisatie de hoedanigheid van verwerkingsverantwoordelijke heeft.
[113] De verantwoordelijke organisatie kan een verantwoordelijke voor de verwerking van persoonsgegevens of zelf een verwerker van een verwerkingsverantwoordelijke zijn.

Volgens artikel 28, §3 (a) van de AVG moet de verwerker persoonsgegevens verwerken overeenkomstig de instructies van de verwerkingsverantwoordelijke. Algemeen wordt aangenomen dat de aan de verwerker toevertrouwde verwerking niettemin gepaard kan gaan met "een bepaalde handelingsvrijheid voor wat betreft de wijze waarop de belangen van de voor de verwerking verantwoordelijke het best kunnen worden gediend, zodat de verwerker de meest geschikte technische en organisatorische middelen kan kiezen".[114] Zo is het denkbaar dat de deelnemer een bepaalde keuzevrijheid geniet wat de door hem gebruikte middelen betreft om de beveiliging van de informatiesystemen van de verantwoordelijke organisatie na te gaan. De verantwoordelijke organisatie bepaalt welke systemen en diensten de deelnemer mag testen en tot welke hij geen toegang heeft.

Artikel 28, § 1, van de AVG bepaalt dat de verwerkingsverantwoordelijke procedures moet uitwerken voor de selectie van dienstverleners om zich ervan te vergewissen dat deze laatsten "afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen" bieden, met name op het gebied van deskundigheid, betrouwbaarheid en middelen. In het kader van een CVDP of van een beloningsprogramma voor het opsporen van kwetsbaarheden kan de verantwoordelijke organisatie de deelname immers beperken tot bepaalde ethische hackers of eisen dat de deelnemers de nodige deskundigheid en ervaring hebben om de systemen van de verantwoordelijke organisatie te testen, met inbegrip van haar eventuele persoonsgegevens.

De verwerkingsverantwoordelijke moet ook een zeker toezicht[115] kunnen uitoefenen op de dienst die namens hem wordt uitgevoerd om na te gaan of dit gebeurt in overeenstemming met de overeenkomst die met de verwerker is gesloten en met de AVG. Zo moet de deelnemer samenwerken met de verantwoordelijke organisatie en, op haar verzoek, alle relevante informatie kunnen bezorgen.

De deelnemer kan evenwel als verwerkingsverantwoordelijke worden beschouwd wanneer de essentiële middelen voor de verwerking van persoonsgegevens onvoldoende zijn vastgesteld in de CVDP of wanneer de deelnemer de instructies van de verantwoordelijke organisatie niet opvolgt. De deelnemer die op ongeoorloofde wijze gegevens verwerkt (of gegevens verwerkt voor andere doeleinden dan het opsporen van kwetsbaarheden) moet immers als verwerkingsverantwoordelijke worden beschouwd aangezien hij zelf een ander verwerkingsdoel en/of (essentiële) verwerkingsmiddelen vaststelt.

[114] Groep van artikel 29, advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", WP 169, blz. 27, *idem*.
[115] Groep van artikel 29, advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", WP 169, blz. 30.

Afdeling 3. Gevolgen voor de inhoud van het CVDP

Uit het voorgaande volgt dat het CVDP de verplichtingen van de partijen inzake de verwerking van persoonsgegevens, met name het doel van en de essentiële middelen voor eventuele verwerkingen, moet vermelden. Zo dient de inhoud van het beleid het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, alsook de rechten en verplichtingen van de verwerkingsverantwoordelijke te omschrijven.

De verantwoordelijke organisatie moet in haar CVDP regels opnemen die de deelnemer verplichten afdoende garanties te bieden voor het toepassen van passende technische en organisatorische maatregelen voor de verwerking van persoonsgegevens.[116] De deelnemer moet ervoor zorgen dat deze gegevens worden bijgehouden met waarborging van een op de risico's afgestemd beveiligingsniveau (bij voorkeur versleuteld) en dat ze onmiddellijk na afloop van de verwerking worden verwijderd.

Ook moet de verwerking van persoonsgegevens voor een ander doel dan het opsporen van kwetsbaarheden in de systemen, uitrusting of producten van de verantwoordelijke organisatie worden uitgesloten.

Voorts moet de deelnemer zich ertoe verbinden elk eventueel verlies van persoonsgegevens te melden aan de verantwoordelijke organisatie en/of aan de Gegevensbeschermingsautoriteit en dit zo snel mogelijk na kennisname ervan.

Het CVDP moet minstens de volgende verbintenissen van de deelnemer bevatten:[117]

- persoonsgegevens uitsluitend verwerken op basis van schriftelijke instructies van de verwerkingsverantwoordelijke;
- waarborgen dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen;
- ervoor zorgen dat natuurlijke personen die handelen onder het gezag van de verwerker en toegang hebben tot persoonsgegevens, deze slechts in opdracht van de verwerkingsverantwoordelijke mogen verwerken;[118]
- passende technische en organisatorische maatregelen nemen om een op het risico afgestemd beveiligingsniveau te waarborgen, rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de

[116] Art. 28, § 1, van de AVG.
[117] Zie met name de voorwaarden vermeld in artikel 28, § 3, van de AVG.
[118] Art. 32, § 4, van de AVG.

qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen;[119]

- de voorafgaande toestemming van de verwerkingsverantwoordelijke bekomen voor het in dienst nemen van een andere verwerker en deze laatste verplichten de inhoud van het bekendmakingsbeleid na te leven;

- de verwerkingsverantwoordelijke door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, bijstand verlenen bij het vervullen van diens plicht om verzoeken om uitoefening van de rechten van de betrokkene te beantwoorden;

- de verwerkingsverantwoordelijke bijstand verlenen bij het doen nakomen van de verplichtingen vermeld in de artikelen 32 tot en met 36 van de AVG (beveiliging, melding van inbreuken, impactanalyse, voorafgaande raadpleging), rekening houdend met de aard van de verwerking en de informatie waarover de deelnemer beschikt;

- de verwerkingsverantwoordelijke onverwijld informeren zodra de deelnemer kennis heeft genomen van een inbreuk in verband met persoonsgegevens;[120]

- na afloop van de deelname aan het beleid, alle persoonsgegevens wissen of deze terugbezorgen[121] aan de verwerkingsverantwoordelijke, en bestaande kopieën verwijderen;

- de verwerkingsverantwoordelijke alle nodige informatie ter beschikking stellen om de nakoming van de verplichtingen aan te tonen, waaronder een register van alle categorieën van verwerkingsactiviteiten die hij namens de verwerkingsverantwoordelijke heeft uitgevoerd;[122]

- het gebruik van persoonsgegevens voor een ander doel dan het opsporen van kwetsbaarheden in het systeem of het meedelen van deze gegevens aan derden uitsluiten.

[119] Art. 32, § 1, van de AVG.
[120] Art. 33, § 2, van de AVG.
[121] naargelang de keuze van de verwerkingsverantwoordelijke.
[122] waarvan de inhoud vermeld is in art. 30, § 2, van de AVG.

H. Juridische referenties

DE NAUW A. en KUTY F., *Manuel de droit pénal spécial*, Waterloo, Kluwer, 2014, blz. 1125-1145.
DECHAMPS F. en LAMBILOT C., *Cybercriminalité: Etats des lieux*, Limal, Anthémis, 2016, blz. 26-46.
DEHOUSSE F., VERBIEST T., ZGAJEWSKI T., "La criminalité dans la société de l'information" in *Introduction au droit de la société de l'information*, Brussel, Larcier, 2007.
DE VILLENFAGNE F. en DUSOLLIER S., "La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique", *A.M.*, 2001, blz. 60-81.
DOCQUIR B., "La loi du 15 mai 2006: nouvelles définitions des infractions en matière de criminalité informatique", *R.D.T.I.*, 2006, blz. 287-294.
EVRARD S., "La loi du 28 novembre 2000 relative à la criminalité informatique", *J.T.*, 2001, blz. 241-245.
HENRION T., *Mémento Droit pénal*, Brussel, Kluwer, 2016.
KUTY F., *Principes généraux du droit pénal*, t. 1, La loi pénale, Brussel, Larcier, 2009.
K. ROSIER, "Le traitement de données dans le cadre des communications électroniques" in X. *Vie privée et données à caractère personnel*, Brussel, Politeia.
LEROUX O., "La Criminalité informatique", *Les infractions contre les biens*, Brussel, Larcier, 2008, blz. 409-436.
LEROUX O., in X. *Postal Mémorialis. Lexique du droit pénal et des lois spéciales*, Brussel, Kluwer, 2014, blz. C 362/1-55.
LORENT A., "Destructions et dégradations autres que par incendie ou explosion", *Droit pénal et procédure pénale (DPPP)*, Kluwer, 2006, blz. 119-136.
MEUNIER C., "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique", *Rev. dr. pén.*, 2001, blz. 611-690.
MEUNIER C., "La loi du 28 novembre 2000 relative à la criminalité informatique" in *Actualités du droit des technologies de l'information et de la communication,* CUP, 2001, blz. 37-160.
OMRANI F. en DUMORTIER F., "Chronique de jurisprudence 2009-2011. Criminalité informatique", *R.D.T.I.*, 2012, blz. 198-208.
ROGER FRANCE E., "La criminalité informatique", *Actualités de droit pénal*, Brussel, Bruylant, 2005, blz. 101-133.
TULKENS F., VAN DE KERCHOVE M., CARTUYVELS Y. en GUILLAIN C., *Introduction au droit pénal*, 9e uitg., Brussel, Kluwer, 2010.
DE VILLENFAGNE F., "Chronique de jurisprudence 2002-2008. Criminalité informatique", R.D.T.I., 2010, blz. 9-28.
VANDER GEETEN V., "La criminalité informatique et les politiques de divulgation coordonnée des vulnérabilités" in *Les obligations légales de cybersécurité et de notifications d'incidents*, Politeia, Brussel, 2019, blz. 217 e.v.
VANDERMEERSCH D., "Eléments de droit pénal et de procédure pénale", La Charte, Brussel, 2012.

BAEYENS, E., "Informatica en recht: oude griffels - nieuwe leien", *T. Strafr.*, 2007, blz. 404-407.
DEENE J. en NERINCKX G., "Computercriminaliteit" in *Praktijkboek recht en internet*, Titel II – Hoofdstuk 10, Brugge, Vanden Broele, 2007, blz. 3-43.

DELBROUCK I., “Informaticacriminaliteit”, in X., *Postal Memorialis, Lexicon strafrecht, strafvordering en bijzondere wetten*, Antwerpen, Kluwer, 2007, I. 42/08-30.
DE HERT, P., “De wet van 28 november 2000 inzake informaticacriminaliteit en het materieel strafrecht. Een wet die te laat komt of een wet die er nooit had moeten komen?”, *T. Strafr.*, 2001, blz. 286-334.
J. DUMORTIER, *ICT-Recht*, Acco, Leuven, 1999, blz. 86 e.v.
KERKHOFS J. en VAN LINTHOUT P., *Cybercrime 3.0*, Brussel, Politeia, 2019.
KERKHOFS J. en VAN LINTHOUT P., *Cybercrime*, Brussel, Politeia, 2014.
KERKHOFS J. en VAN LINTHOUT P., “Cybercriminaliteit doorgelicht”, *T. Strafr.*, 2010, blz. 179 e.v.
KEUSTERMANS J., F. MOLS en T. DE MAERE, “Informaticacriminaliteit” in *Strafrecht en strafvordering*. *Commentaar met overzicht van rechtspraak en rechtsleer*, Mechelen, Kluwer, 2010, blz. 65-103.
KEUSTERMANS J. en MOLS F., “De wet van 28 november 2000 inzake informaticacriminaliteit: eerste overzicht”, *R-W*, 2001-2002, blz. 721-732.
KEUSTERMANS J. en DE MAERE T., “Tien jaar wet informaticacriminaliteit”, *R-W*, 2010-2011, blz. 562-568.
VAN EECKE, P., “De Wet Informaticacriminaliteit”, in X., *Elektronische handel, juridische en praktische aspecten*, Heule, UGA, 2004, blz.369-385.
VANSTEENHUYSE S. en T’JONCK P., “Cybercriminaliteit en privacy” in *Privacy en strafrecht*, Nieuwe en grensoverschrijdende verkenningen, Antwerpen, Maklu, 2007.

CENTRE FOR CYBER SECURITY BELGIUM

GIDS OVER HET BELEID VOOR DE GECOÖRDINEERDE BEKENDMAKING VAN KWETSBAARHEDEN
DEEL I: WETTELIJKE ASPECTEN

Dit document en de bijlagen werden opgesteld door het Centrum voor Cybersecurity België (CCB). Deze federale overheidsinstelling werd opgericht bij het koninklijk besluit van 10 oktober 2014 en staat onder het gezag van de Eerste Minister.

De vermelde informatie:
• is louter algemeen van aard en heeft niet tot doel alle specifieke situaties te behandelen;
• is niet noodzakelijk op alle vlakken volledig, nauwkeurig of up-to-date.

Verantwoordelijke uitgever:
Centrum voor Cybersecurity België
M. De Bruycker, Directeur
Wetstraat 16
1000 Brussel

Wettelijk depot:

D/2020/14828/015

2020