Bijdrage van de Raad van State van België

Veranderingen en aanpassingen – vanuit een rechtsstatelijk perspectief – van bestuur, regelgeving en rechtspraak, die noodzakelijk zijn als gevolg van digitalisering, automatisering en toepassing van informatie- en communicatietechnologie bij de overheid. Implicaties van deze ontwikkelingen voor de rechtshandhaving

Jo Baert, kamervoorzitter in de Raad van State van België
Benny De Sutter, bestuurlijk attaché-jurist bij de Raad van State van België

Inhoud

1. Strafrechtelijke rechtshandhaving

1.1. Een nieuw soort misdrijven: informaticamisdrijven

In België zijn in de loop van de jaren inzake informaticacriminaliteit (of computercriminaliteit) verschillende nieuwe strafbaarstellingen ingevoerd. Dit werd nodig geacht om de rechtsorde te handhaven. In een aantal gevallen konden de bestaande delictomschrijvingen ook worden toegepast op informaticamisdrijven, doch wanneer die niet voldoende technologieneutraal waren (bv. valsheid in geschrifte), diende de wetgever een nieuwe delictomschrijving in te voeren (valsheid in informatica).

Er wordt een onderscheid gemaakt tussen *atypische informaticamisdrijven* en *eigenlijke informaticamisdrijven*.

1.1.1. Atypische informaticamisdrijven

Tot de eerste categorie behoren de misdrijven waarbij informaticatechnologie (ICT) het *middel* is om een bestaand, "klassiek" misdrijf te plegen. Voorbeelden hiervan in het Belgisch strafrecht zijn valsheid in informatica (art. 210*bis*, §§ 1-4, van het Belgisch Strafwetboek, hierna afgekort tot Sw.; bv. het aankopen van goederen middels het internet door bedrieglijk gebruik te maken van andermans kredietkaartgegevens), informaticabedrog (art. 504*quater* Sw.; bv. het invoeren van programma-instructies in een satellietdecoder waardoor de gebruiker het voordeel van een ontcijferd signaal geniet) en het zich "met kennis van zaken" via een informaticasysteem of enig ander technologisch middel toegang verschaffen tot kinderpornografie (art. 383*bis*, § 2 Sw.).

1.1.2. Eigenlijke informaticamisdrijven

Bij de eigenlijke informaticamisdrijven is de informatica het *doel* zelf van het misdrijf. Hacking (art. 550*bis* Sw.) is een voorbeeld van een eigenlijk informaticamisdrijf. In het Belgische Strafwetboek wordt het omschreven als het zich toegang verschaffen tot een informaticasysteem of zich daarin handhaven, terwijl men weet dat men daartoe niet gerechtigd is. Ook de persoon "die, met bedrieglijk opzet of met het oogmerk om te schaden, zijn toegangsbevoegdheid tot een informaticasysteem overschrijdt", is volgens de Belgische strafwet strafbaar. Een ander voorbeeld van een eigenlijk informaticamisdrijf is datasabotage (art. 550*ter* Sw.). Datasabotage verschilt in wezen niet van het informaticabedrog. Enkel het moreel element van het misdrijf onderscheidt beide strafbaarstellingen: waar informaticabedrog als moreel element het bedrieglijk opzet vereist, bestaat het moreel element van datasabotage in het oogmerk om te schaden.

1.1.3. Toelichting bij de belangrijkste nieuwe misdrijven

Vooral met de wet van 28 november 2000 'inzake informaticacriminaliteit' werden heel wat aanpassingen doorgevoerd. Bedoeling van die wet was om het wettelijk arsenaal aan strafbepalingen en de middelen waarin is voorzien in het strafprocesrecht, aan te passen aan de noden van een effectieve bestrijding van criminaliteit die verband houdt met de informatietechnologie. Met de wet werden aldus twee precieze doelstellingen nagestreefd, namelijk enerzijds een aanpassing van de strafbepalingen, wanneer de klassieke rechtsbegrippen niet meer de mogelijkheid boden in te spelen op de specifieke noden in verband met computercriminaliteit en, anderzijds, een wijziging van de strafrechtelijke procedure om de politiediensten en gerechtelijke diensten aangepaste juridische middelen ter beschikking te stellen ter bestrijding van computercriminaliteit.[1]

[1] RvS, afd. Wetg., advies 28.029/2 van 31 mei 1999, *Parl.St.* Kamer 1999-2000, DOC 50 0213-0214/001, 42.

Hierna worden de belangrijkste informaticamisdrijven nader toegelicht.

- Valsheid in informatica (art. 210*bis* §§ 1-4 Sw.; wet van 28 november 2000 'inzake informaticacriminaliteit')

  Dit delict bestaat in het opzettelijk vermommen van de waarheid via datamanipulatie met betrekking tot juridisch relevante gegevens. De valsheid wordt gepleegd door het invoeren, wijzigen of wissen van gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem of door de mogelijke aanwending van die gegevens in een informaticasysteem te veranderen. Degene die gebruik maakt van gegevens waarvan hij weet dat ze zijn vervalst, wordt gestraft alsof hij de dader van de valsheid was.

- Informaticabedrog (art. 504*quater* Sw.; wet van 28 november 2000)

  Dit misdrijf vereist de vereniging van drie elementen, nl. het verwerven van een vermogensvoordeel, de materiële handeling van datamanipulatie en een bedrieglijk opzet. Het bedoelde vermogensvoordeel moet niet materieel van aard zijn. De materiële handeling die een constitutief bestanddeel van dit misdrijf uitmaakt, wordt gepleegd door gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, in een informaticasysteem in te voeren, te wijzigen, te wissen of met enig ander technologisch middel de mogelijke aanwending van gegevens in een informaticasysteem te veranderen.

- Hacking (art. 550*bis* Sw.; wet van 28 november 2000)

  Dit misdrijf dient te worden opgesplitst in een basismisdrijf en de gevolghandelingen. Het basismisdrijf kan worden voltrokken zonder de gevolghandelingen, maar omgekeerd kunnen de gevolghandelingen niet plaatsvinden zonder het basismisdrijf.

  Het basismisdrijf dient te worden onderscheiden in de hacking "van binnenuit" en de hacking "van buitenuit". Hacking van buitenuit doelt op een persoon die zich toegang verschaft tot een systeem zonder hiertoe gerechtigd te zijn. Hacking van binnenuit gebeurt door een persoon die reeds een gelimiteerde toegang heeft tot een bepaald systeem, maar zijn toegangsniveau op een onrechtmatige wijze overschrijdt.

  Hacking "van buitenuit" betreft het misdrijf waarbij de dader zich toegang verschaft tot een informaticasysteem of waarbij hij zich in een informaticasysteem handhaaft terwijl hij weet hiertoe niet gerechtigd te zijn. Hacking "van buitenuit" vereist als moreel element slechts een algemeen opzet (maar bedrieglijk opzet leidt wel tot strafverzwaring).

  Hacking "van binnenuit" betreft zoals aangegeven het overschrijden van een (gelimiteerde) toegangsbevoegdheid tot een informaticasysteem. Bij dit misdrijf wordt evenwel een bijzonder opzet vereist, nl. een bedrieglijk opzet of het oogmerk om te schaden.

  Verder zijn er nog enkele gevolghandelingen/verzwarende omstandigheden:

  - de gegevens die worden opgeslagen, verwerkt of overgedragen door middel van het informaticasysteem op een of andere manier overnemen;

- enig gebruik maken van een informaticasysteem van een derde of zich bedienen van het informaticasysteem om toegang te verkrijgen tot een informaticasysteem van een derde (zgn. tijdsdiefstal);
- veroorzaken – zelfs onopzettelijk – van enige schade aan het informaticasysteem of aan de gegevens die door middel van het informaticasysteem worden opgeslagen, verwerkt of overgedragen of aan een informaticasysteem van een derde of aan de gegevens die door middel van laatstgenoemde informaticasysteem worden opgeslagen, verwerkt of overgedragen.

Ook voorbereidende handelingen die een strafbare poging uitmaken worden even zwaar bestraft. Deze strafbaarstelling moet enerzijds worden gezien in het licht van de bekommernis van de wetgever om een antwoord te willen bieden aan het opsporen, verzamelen, verspreiden en verhandelen van logingegevens en wachtwoorden. Anderzijds werd met deze strafbaarstelling de handel in hackertools geviseerd.

Aanzetten tot hackingmisdrijven is eveneens strafbaar. De opdrachtgever wordt bovendien zwaarder gestraft dan de hacker zelf. Beweegreden hiertoe betreft de overweging dat waar de hacking op zich in veel gevallen een tijdverdrijf voor computerfreaks is of was, thans professionele criminelen dergelijke personen inzetten waar zij zelf niet over de vereiste expertise beschikken.

Naast de opdrachtgever wordt ook de heler van de "gehackte" gegevens gestraft.

- Informatica- en datasabotage (art. 550*ter* Sw.; wet van 28 november 2000)

Vernielingen en beschadigingen werden traditioneel in het Belgisch strafrecht enkel in aanmerking genomen wanneer ze betrekking hadden op tastbare voorwerpen. Dit is het geval wanneer het schade betreft aan een informaticasysteem zelf, maar beschadiging van data werd als zodanig niet rechtstreeks geviseerd in de bepalingen van het Strafwetboek. Daarom is een nieuwe bepaling ingevoerd die elke kwaadwillige manipulatie van gegevens strafbaar stelt.[2]

- "Bezit" van kinderpornografie (art. 383*bis*, § 2 Sw.; wet van 30 november 2011)

De betrokken strafbepaling luidde aanvankelijk als volgt: "Hij die wetens de in § 1 bedoelde zinnebeelden, voorwerpen, films, foto's, dia's of andere beelddragers bezit, wordt gestraft met gevangenisstraf van een maand tot een jaar en met geldboete van honderd euro tot duizend euro."

Door technologische ontwikkelingen is het mogelijk om met gebruik van informatietechnologie toegang te verkrijgen tot op afstand geplaatste bestanden waarop zich kinderpornografisch materiaal, al dan niet versleuteld, bevindt. Aldus bestaat er een mogelijkheid om over het materiaal te beschikken en dit desgewenst te bekijken, zonder dat daarbij het materiaal op de eigen computer wordt opgeslagen. De vraag rees of deze wijze van het verkrijgen van toegang tot kinderpornografie in alle gevallen onder de bestaande strafbaarstelling van "bezit" in artikel 383*bis*, § 2, van het Strafwetboek kon worden gebracht.

[2] *Parl.St.* Kamer 1999-2000, DOC 50 0213-0214/001, 19.

De strafbepaling werd daarom als volgt aangevuld: "Hij die wetens de in § 1 bedoelde zinnebeelden, voorwerpen, films, foto's, dia's of andere beelddragers bezit *of zich, met kennis van zaken, via een informaticasysteem of enig ander technologisch middel, de toegang daartoe verschaft*, wordt gestraft met gevangenisstraf van een maand tot een jaar en met geldboete van honderd euro tot duizend euro."

De uitdrukking "zich toegang verschaffen tot" impliceert een actieve handeling die op het opzettelijk verkrijgen van toegang is gericht (bv. online betaling om toegang te krijgen of beschikken over de nodige paswoorden en inloggegevens). Zoals in Nederland volstaat het louter bekijken van kinderpornografie als zodanig niet om strafbaar te zijn: wie ongevraagd ermee in aanraking komt, zou immers terughoudend zijn om aangifte te doen.[3]

1.2. Bevoegdheidsbepaling voor informaticamisdrijven[4]

Over lokalisering van misdrijven wordt door elk land, door middel van wetgeving of rechtspraak, in beginsel op unilaterale wijze beslist. Door de internationalisering van de criminaliteit bestaat de neiging om brede lokalisatiecriteria te gebruiken. Ook in België is dat het geval.

De Belgische strafwet is van toepassing op al wie op het Belgische grondgebied een misdrijf pleegt (*territorialiteitsbeginsel*).[5] Misdrijven gepleegd buiten het Belgische grondgebied worden in België niet gestraft dan in de gevallen bij wet bepaald.[6]

De Belgische strafwet bepaalt echter niet op grond van welke juridische criteria de plaats van het misdrijf moet worden bepaald; dergelijke criteria zijn uitgewerkt door de rechtsleer en overgenomen door de rechtspraak. De opkomst van nieuwe technologieën zoals het internet bemoeilijkt de plaatsbepaling van misdrijven nog verder.

In België neemt men, op grond van de *ubiquiteitsleer*[7], aan dat een misdrijf te situeren is op al die plaatsen waar zich een gedraging voordoet die een constitutief element van het misdrijf vormt.[8] In de praktijk lijkt deze leer overeen te komen met een combinatie van drie lokaliseringstheorieën, nl. de *theorie van de lichamelijke gedraging* die het feit situeert op de plaats waar de dader effectief en fysiek de handeling stelde, de *leer van het instrument* welke het misdrijf situeert waar het instrument van het misdrijf "zijn werk doet" en ten slotte de *leer van het gevolg* die vooropstelt dat de strafbare gedraging te situeren valt daar waar het uiteindelijke gevolg van een handeling zich manifesteert (indien het gevolg een constitutief element is van het misdrijf).[9]

Deze leer wordt aangevuld met de *leer van de ondeelbaarheid*, op grond waarvan wordt aangenomen dat de Belgische rechter kennis mag nemen van alle elementen van het misdrijf die een ondeelbaar geheel vormen met het misdrijf dat op het Belgisch grondgebied werd gepleegd (bv. deelneming in het buitenland aan een in België gepleegd misdrijf).

---

[3] *Parl.St.* Kamer 2010-2011, DOC 53 1639/001, 9-10.
[4] Voor het opstellen van dit onderdeel is in ruime mate gebruik gemaakt van het volgende werk: C. VAN DEN WYNGAERT, *Strafrecht en strafprocesrecht*, Antwerpen, Maklu, 2011, inz. 143-149.
[5] Art. 3 Sw.
[6] Art. 4 Sw.
[7] *Ubique* (Lat.) = overal.
[8] Zie o.a.: Cass. 29 januari 1979, *Arr.Cass.* 1979, 575; Cass. 4 februari 1986, *Arr.Cass.* 1985-86, 355; Cass. 21 juni 1989, *Arr.Cass.* 1988-89, 620.
[9] PH. VAN LINTHOUT, "Territoriale bevoegdheid in cyberspace", noot bij Corr. Dendermonde 29 september 2008, *T.Strafr.* 2009, 113.

De combinatie van de *ubiquiteitsleer* en de *leer van de ondeelbaarheid* kan tot een feitelijke toepassing van de zgn. *effectenleer* leiden, waarbij niet enkel de constitutieve gevolgen van een misdrijf in aanmerking worden genomen, maar ook de verder verwijderde gevolgen. (In de Verenigde Staten wordt traditioneel toepassing gemaakt van de effectenleer.)

Het op het eigen grondgebied lokaliseren van een misdrijf is aanlokkelijk: in dat geval is er immers geen beperking (bv. de voorwaarde van de dubbele incriminatie – in vele gevallen een basisvoorwaarde voor de toepassing van de strafwet op misdrijven die in het buitenland werden gepleegd – geldt niet) en kan de eigen strafwet worden toegepast zonder dat moet worden rekening gehouden met buitenlandse wetgeving of buitenlandse veroordelingen (*ne bis in idem*).

Die tendens doet zich uitdrukkelijk ook voor bij de lokalisering van informaticamisdrijven in België. Voorbeelden daarvan zijn o.a. de Yahoo-zaak (zie verder).[10]

1.3. Opsporing van misdrijven: nieuwe mogelijkheden

Ook op procedureel vlak werden een aantal nieuwigheden ingevoerd om een betere handhaving van het recht mogelijk te maken. Het gaat in het bijzonder om nieuwe opsporingsmogelijkheden en meewerkverplichtingen.

1.3.1. Databeslag

De bepalingen inzake databeslag (art. 39*bis* van het Wetboek van Strafvordering, hierna afgekort tot Sv.; ingevoegd bij de wet van 28 november 2000) bieden een pragmatische oplossing voor de inbeslagname van informaticabestanden (of gehele informaticasystemen) die immers niet (of niet altijd) ter hand genomen kunnen worden. Klassiek voorbeeld is dat van de agent die in het kader van een financieel dossier een huiszoeking moet verrichten in een bank en daar wordt geconfronteerd met een zaal vol computers. Het zou een hele klus zijn om elke computer als bewijsmateriaal in beslag te nemen. Bovendien stelt zich in dat geval ook de vraag naar de eventuele (economische of financiële) schade die wordt toegebracht wanneer alle hardware in beslag wordt genomen en waardoor het bedrijf niet langer kan functioneren.[11]

Het databeslag heeft betrekking op de in een informaticasysteem opgeslagen 'nuttige' gegevens, d.w.z. gegevens die kunnen bijdragen tot het ontdekken van de waarheid omtrent de vervolgde feiten.[12] Er dient dus een aantoonbaar verband te bestaan met het misdrijf waarop het strafonderzoek betrekking heeft, zodat een databeslag waarbij *a priori* geen enkele aandacht wordt besteed aan dit noodzakelijk verband, als disproportioneel en onwettelijk zou kunnen worden beschouwd.[13]

---

[10] Zie bv. ook Corr. Brussel 22 december 1999, *Auteurs & Media* 2000, 134-137 (in verband met racisme in nieuwsgroepen en discussiefora op het internet is de rechtbank van het rechtsgebied waar de berichten konden worden ontvangen territoriaal bevoegd); Corr. Dendermonde 29 september 2008, *T.Strafr.* 2009, 111-112 (territoriaal bevoegd is o.a. de rechter van de plaats waar het slachtoffer van een hacking zijn computer aanzet en dienvolgens de gevolgen van de hacking krijgt opgedrongen).

[11] J. KERKHOFS en PH. VAN LINTHOUT, "Inleiding tot het materieel en strafprocedureel cyberstrafrecht: uitdagingen voor de advocatuur", in DE MEULENAERE, B., *Internet &/@ Recht*, Gent, Larcier, 2013, 25.

[12] Art. 39*bis*, § 2 Sv.; F. MOLS, J. KEUSTERMANS, en T. DE MAERE, "Informaticacriminaliteit" in VANDEPLAS, A., ARNOU, P. en VAN OVERBEKE, S. (red.), *Strafrecht en strafvordering. Artikelsgewijze commentaar met overzicht van rechtspraak en rechtsleer*, Kluwer, Mechelen, 2010, 30.

[13] D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context", in VERSTRAETEN, R. en VERBRUGGEN, F. (eds.), *Straf- en strafprocesrecht*, Brugge, die Keure, 2010, 141.

In principe blijft de klassieke procedure, d.w.z. de inbeslagname van de gegevensdrager, gelden.[14] Wanneer de inbeslagname van de materiële dragers niet wenselijk is, kan beslag worden gelegd op de gegevens zonder daarbij het informaticasysteem zelf te viseren.[15] Meer concreet worden in dat geval de betrokken gegevens, evenals de gegevens noodzakelijk om de in beslag genomen gegevens te verstaan, gekopieerd naar materiële dragers van de overheid. Slechts in twee gevallen kunnen dragers die ter beschikking staan van personen bevoegd voor het gebruik van het systeem, worden aangewend, namelijk in geval van dringendheid of bij technische problemen.[16]

Nadat de relevante gegevens werden gekopieerd, wordt de toegang tot deze gegevens in het onderzochte informaticasysteem of op ter plaatse aanwezige dragers, geblokkeerd (bijvoorbeeld door versleutelingstechnieken). Er kan evenwel beslist worden, in het licht van het proportionaliteitsbeginsel, om gegevens of een deel daarvan niet te blokkeren, bijvoorbeeld om de continuïteit van de werking van een systeem of een organisatie niet in het gedrang te brengen. Het blokkeren van de gegevens kan worden vervangen door het wissen ervan, in twee gevallen, namelijk wanneer de procureur des Konings de gegevens strijdig acht met de openbare orde of de goede zeden (bijvoorbeeld kinderpornografie, racistische pamfletten) ofwel wanneer de procureur des Konings meent dat de gegevens een risico voor schade opleveren (bijvoorbeeld computervirussen of hackertools). Wanneer het niet mogelijk is om kopieën te nemen, bijvoorbeeld omdat de toepassingsprogrammatuur zeer complex is en elders niet beschikbaar of omdat de hoeveelheid data te omvangrijk is, worden de gegevens enkel geblokkeerd, wat in feite neerkomt op de informatica-variant van verzegeling. Als algemene waarborg is er in een informatieverplichting voorzien ten aanzien van diegene die verantwoordelijk is voor het informaticasysteem. Daarbij wordt een samenvatting meegedeeld van de operaties die ten aanzien van de gegevens werden uitgevoerd. Een uitputtende inventaris is immers in een geïnformatiseerde omgeving vaak niet realistisch.[17]

De wetgever is enigszins vaag gebleven bij het opstellen van artikel 39*bis* Sv.

Zo wordt het blokkeren en wissen van gegevens verbloemend omschreven als het aanwenden van de "passende technische middelen" om de toegang tot de betrokken gegevens te verhinderen of om die gegevens ontoegankelijk te maken. Wat onder "passende technische middelen" moet worden begrepen, is niet gedefinieerd. Deze vage omschrijving was evenwel een bewuste keuze van de wetgever, gelet op de specificiteit van de evolutie van de informatiemaatschappij. Het gaat immers om technische middelen, waarvan de aard afhankelijk is van de stand van de technologie, evenals van de specifieke vereisten van de data. Daarnaast hebben deze middelen als zodanig geen effect op de bewijswaarde van de data, maar betreffen zij de modaliteiten van de onttrekking of bewaring van de data, waardoor nodeloze bewijsbetwistingen voor de rechter kunnen worden voorkomen. Bovendien gaat het hier om een wettelijke vereiste met het oog op het beschermen van het bewijsmateriaal, die zelfs niet bestaat in het gemeen recht, maar net omwille van de eigenheid van de geïnformatiseerde omgeving, werd ingevoegd.[18]

In België heeft het Hof van Cassatie zich al uitgesproken over deze "passende technische middelen", meer bepaald in een zaak over de torrentswebsite "The Pirate Bay", die *peer-to-peer file*

[14] G. NERINCKX, "Computercriminaliteit" in DE CORTE, R. (ed.), *Praktijkboek Recht en Internet*, Titel II, Hoofdstuk 10, Brugge, Vanden Broele, 2006, 31; D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context", in VERSTRAETEN, R. en VERBRUGGEN, F. (eds.), *Straf- en strafprocesrecht*, Brugge, die Keure, 2010, 139.
[15] G. NERINCKX, "Computercriminaliteit" in DE CORTE, R. (ed.), *Praktijkboek Recht en Internet*, Titel II, Hoofdstuk 10, Brugge, Vanden Broele, 2006, 31.
[16] *Parl.St.* Kamer 1999-2000, nr. 50 0213/001, 20.
[17] *Parl.St.* Kamer 1999-2000, nr. 50 0213/001, 20-21.
[18] *Parl.St.* Kamer 1999-2000, nr. 50 0213/001, 22.

sharing mogelijk maakt.[19] In die zaak oordeelde het Hof dat de bedoelde "passende technische middelen" kunnen bestaan in het bevelen aan internettoegangleveranciers van het ontoegankelijk maken van de toegang tot de server waarop de betrokken gegevens zijn gehost. De passende technische middelen zijn volgens het Belgische Hof van Cassatie m.a.w. niet beperkt tot de gebruiksgerechtigde.[20]

Inmiddels heeft ook het Europees Hof van Justitie zich uitgesproken over een blokkeringsmaatregel.[21] Het Hof oordeelt dat een rechter die een internettoegangsleverancier verbiedt om zijn abonnees toegang te verschaffen tot een website waarop beschermde werken zonder toestemming van de rechthebbenden worden geplaatst, niet moet preciseren welke maatregelen de internettoegangsleverancier moet nemen en evenmin moet aangeven dat laatstgenoemde kan ontsnappen aan dwangsommen door aan te tonen dat hij alle redelijke maatregelen heeft genomen om te voldoen aan het bevel. Het Hof koppelt niettemin een dubbele voorwaarde aan de te nemen maatregelen. Allereerst mogen de door de internettoegangsleverancier genomen maatregelen de internetgebruikers niet nodeloos de mogelijkheid ontzeggen om zich rechtmatig toegang te verschaffen tot de beschikbare informatie. Bovendien moeten die maatregelen tot gevolg hebben dat niet-toegestane oproepingen van de beschermde werken worden verhinderd of minstens bemoeilijkt, en moeten zij internetgebruikers ontraden om zich toegang te verschaffen tot de ontoegankelijk gemaakte werken. De maatregelen moeten m.a.w. doeltreffend zijn. Het komt echter aan de nationale autoriteiten en rechterlijke instanties toe om hierover te waken.[22]

Ook wie moet worden beschouwd als de "verantwoordelijke van het informaticasysteem" is niet in de wet bepaald. De wetgever koos er hier voor om enige flexibiliteit te bewaren, aangezien het niet altijd duidelijk is wie de reële of juridische controle over een informaticasysteem heeft.[23] Volgens sommigen is het overigens mogelijk dat de informatieverplichting ten aanzien van de verantwoordelijke van het informaticasysteem pas wordt voldaan nadat er reeds beslag is gelegd. Er wordt in dat verband gewaarschuwd voor het gevaar van een beslag op afstand zonder dat de verantwoordelijke van het systeem hiervan op de hoogte is. Hierbij kan evenwel worden opgemerkt dat hacking door de overheid als nieuwe, geheime bewakingsmaatregel in elk geval verboden is.[24]

1.3.2. Netwerkzoeking

ICT komt in het opsporingsonderzoek ook aan bod bij de netwerkzoeking of de "zoeking in een informaticasysteem", zoals de officiële benaming ervan in artikel 88*ter* Sv. (ingevoegd bij de wet van 28 november 2000) luidt. Dit artikel voorziet in de mogelijkheid voor de onderzoeksrechter,

---

[19] Cass. 22 oktober 2013, nr. AR.P.2013.0551.N.

[20] M. TAEYMANS, "Onderzoeksrechter mag toegang tot websites laten blokkeren", *De Juristenkrant* 4 december 2013, 2.

[21] HvJ 27 maart 2014, nr. C-314/12, UPC Telekabel. Een dergelijk bevel lijkt de vrijheid van ondernemerschap van de internettoegangsleverancier niet te raken. Zie: T. SCHOEFS, "Strijd tegen The Pirate Bay over andere boeg gegooid: databeslag toegestaan", *T.Strafr.* 2014, 140-141.

[22] T. SCHOEFS, "Strijd tegen The Pirate Bay over andere boeg gegooid: databeslag toegestaan", *T.Strafr.* 2014, 140-141.

[23] *Parl.St.* Kamer 1999-2000, nr. 50 0213/001, 22; G. NERINCKX, "Computercriminaliteit" in DE CORTE, R. (ed.), *Praktijkboek Recht en Internet*, Titel II, Hoofdstuk 10, Brugge, Vanden Broele, 2006, 36; D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context", in VERSTRAETEN, R. en VERBRUGGEN, F. (eds.), *Straf- en strafprocesrecht*, Brugge, die Keure, 2010, voetnoot 62.

[24] F. MOLS, J. KEUSTERMANS en T. DE MAERE, "Informaticacriminaliteit" in VANDEPLAS, A., ARNOU, P. en VAN OVERBEKE, S. (red.), *Strafrecht en strafvordering. Artikelsgewijze commentaar met overzicht van rechtspraak en rechtsleer*, Kluwer, Mechelen, 2010, 32.

wanneer hij een zoeking beveelt in een informaticasysteem of een deel daarvan, om deze zoeking, onder bepaalde voorwaarden, uit te breiden naar een informaticasysteem of een deel daarvan dat zich op een andere plaats bevindt dan waar de zoeking plaatsvindt.[25] De door de wet gehanteerde term "zoeking" verwijst naar de zoeking in een informaticasysteem onder welke technische en procedurele vorm dan ook en heeft een algemene draagwijdte, zodat die zoeking kan plaatsvinden zowel binnen als buiten het kader van een klassieke huiszoeking.[26]

Als voorbeeld van een netwerkzoeking buiten de context van een klassieke huiszoeking, kan worden verwezen naar het doordringen tot andere ICT-systemen vanaf een op een openbare plaats in beslag genomen laptop of smartphone.[27] Tijdens de parlementaire voorbereidingen van artikel 88*ter* Sv. gaf de minister van Justitie overigens uitdrukkelijk te kennen dat de netwerkzoeking ook buiten de huiszoeking mogelijk moet zijn, aangezien ICT-systemen niet enkel binnen eenzelfde gebouw met elkaar verbonden kunnen zijn, maar dat er ook rekening moet worden gehouden met draagbare computers, telefoons en mobiele telecommunicatie en dataverkeer. Voor de consultatie van de op een gsm, smartphone of *personal digital assistant* (pda) opgeslagen data, bijvoorbeeld het raadplegen van de opgeslagen in- en uitgaande sms- of e-mailberichten, is geen afzonderlijk bevel nodig. De bevoegdheid tot het leggen van beslag op de materiële drager omvat immers ook de bevoegdheid tot consultatie van de toestellen. Voor het uitvoeren van een netwerkzoeking vanaf deze toestellen, bijvoorbeeld het beluisteren van de voice mail of het raadplegen van *in the cloud* opgeslagen mails (bv. op de server van Outlook of Gmail), is daarentegen een netwerkzoekingsbevel op grond van artikel 88*ter* Sv. vereist.[28]

Een beperking bij een traditionele dwangmaatregel zoals de huiszoeking is dat ze, per definitie, enkel mag worden uitgevoerd ten aanzien van de plaats waarvoor ze wordt bevolen. Kenmerkend voor informaticasystemen — of het nu gaat om grote systemen binnen bedrijven of om handige draagbare computers — is dat ze meer en meer verbonden zijn in netwerken. Wanneer de informaticasystemen waarin onderzoek noodzakelijk blijkt te zijn, zich op verschillende locaties bevinden, zijn derhalve in de klassieke context meerdere bevelen tot huiszoeking of inbeslagneming vereist. Bovendien kunnen die informaticasystemen op hun beurt met andere informaticasystemen verbonden zijn, zodat er een sneeuwbaleffect kan kan ontstaan van huiszoekingen en bijhorende mandaten.[29] Het is duidelijk dat een klassieke benadering problematisch is in het geval van zoekingen in informaticanetwerken. Niet alleen bestaat het risico dat bij niet gelijktijdig optreden bewijsmateriaal verloren gaat, maar bovendien zal in veel gevallen niet *a priori* vastgesteld kunnen worden op welke plaatsen de zoeking moet plaatsvinden, welke bestanden relevant zijn, of zelfs waar de computers geografisch gesitueerd zijn.[30]

Om hieraan te verhelpen bepaalt het betrokken artikel de voorwaarden waaronder de uitbreiding van de zoeking in een informaticasysteem naar elders gesitueerde systemen toegelaten is. Hierbij

---

[25] F. MOLS, J. KEUSTERMANS en T. DE MAERE, "Informaticacriminaliteit" in VANDEPLAS, A., ARNOU, P. en VAN OVERBEKE, S. (red.), *Strafrecht en strafvordering. Artikelsgewijze commentaar met overzicht van rechtspraak en rechtsleer*, Kluwer, Mechelen, 2010, 33.

[26] G. NERINCKX, "Computercriminaliteit" in DE CORTE, R. (ed.), *Praktijkboek Recht en Internet*, Titel II, Hoofdstuk 10, Brugge, Vanden Broele, 2006, 37; D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context", in VERSTRAETEN, R. en VERBRUGGEN, F. (eds.), *Straf- en strafprocesrecht*, Brugge, die Keure, 2010, 144.

[27] D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context", in VERSTRAETEN, R. en VERBRUGGEN, F. (eds.), *Straf- en strafprocesrecht*, Brugge, die Keure, 2010, 144.

[28] D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context", in VERSTRAETEN, R. en VERBRUGGEN, F. (eds.), *Straf- en strafprocesrecht*, Brugge, die Keure, 2010, 144.

[29] PH. VAN LINTHOUT en J. KERKHOFS, "Inleiding tot het materieel en strafprocedureel cyberstrafrecht: uitdagingen voor de advocatuur", in DE MEULENAERE, B., *Internet &/@ Recht*, Gent, Larcier, 2013, 38.

[30] *Parl.St.* Kamer 1999-2000, nr. 50 0213/001, 22; G. NERINCKX, "Computercriminaliteit" in DE CORTE, R. (ed.), *Praktijkboek Recht en Internet*, Titel II, Hoofdstuk 10, Brugge, Vanden Broele, 2006, 36.

moet het gaan om onderling verbonden systemen.[31] Daarnaast moet aan nog twee cumulatieve voorwaarden voldaan zijn. In de eerste plaats moet de uitbreiding noodzakelijk zijn om de waarheid aan het licht te brengen ten aanzien van het misdrijf dat het voorwerp van de zoeking uitmaakt. Ten tweede moeten andere maatregelen, zoals bv. het verlenen van meerdere huiszoekingsbevelen,[32] disproportioneel zijn, of moet er een risico bestaan dat zonder de uitbreiding bewijselementen verloren gaan.[33] Het valt op dat de tweede cumulatieve voorwaarde, meer nog dan de eerste, quasi automatisch vervuld zal zijn in de mate door de eigenheid van de ICT-omgeving en de beweeglijkheid en de vluchtigheid van de bewaarde gegevens, er steeds een risico zal bestaan dat bewijsmateriaal verloren gaat. Bovendien is het zo dat doordat de netwerkzoeking een alternatief is voor meerdere huiszoekingen op plaatsen die men nooit op voorhand kent, ook steeds de alternatieve maatregel van een cascade van huiszoekingen disproportioneel zal zijn, zowel naar de inzet van mensen als naar de aantasting van het beschermde goed, met name de privacy van alle geviseerde adressen.[34]

De grens voor het uitoefenen van deze opsporingsbevoegdheid wordt gevormd door de toegangsbevoegdheid van de personen die bevoegd zijn voor het gebruik van het informaticasysteem dat het voorwerp uitmaakt van de zoeking. De maatregel gaat inderdaad niet zo ver dat de overheid gerechtigd zou worden om onbeperkt alle systemen die mogelijk met het onderzochte computersysteem in verbinding staan of kunnen gebracht worden, te doorzoeken. De technische verbinding via de netwerken moet een element van permanentie en stabiliteit inhouden, en niet louter occasioneel zijn.[35] Het is bijgevolg onmogelijk dat een welbepaalde zoeking wordt uitgebreid tot een willekeurig aantal informaticasystemen dat, bijvoorbeeld via het internet, met het onderzochte informaticasysteem kan worden verbonden.[36] In de praktijk zal dit meestal opgelost worden doordat gebruik wordt gemaakt van een login en een paswoord. Zij zullen de garantie vormen voor tegelijk de toegangsbevoegdheid als voor de begrenzing ervan: iemand heeft toegang, want hij beschikt over een login. Door gebruik te maken van deze login en paswoord komt men in het 'vreemde' systeem nooit verder dan waar de betrokken persoon toegang zou hebben gehad.[37]

Een kenmerk van computercriminaliteit is dat ze niet door staatsgrenzen beperkt is. De bestanddelen van een strafbaar feit en de verzwarende omstandigheden waarin het gepleegd wordt, kunnen dus gemakkelijk tegelijkertijd op het grondgebied van verschillende staten gelokaliseerd zijn. Er mag dan ook van uitgegaan worden dat de klassieke territoriale aanknopingspunten niet steeds adequaat zijn om de specifieke handelingen in de computercriminaliteit doeltreffend op te sporen.[38]

Een van de fundamentele regels van het internationaal recht bepaalt dat een staat staatsgezag uitoefent op zijn eigen grondgebied, en dat alleen doet, zonder inmenging van enige andere staat. Hieruit volgt dat een staat in vredestijd absoluut geen dwangmiddelen mag gebruiken op het grondgebied van een andere staat. Een staat mag dus buiten zijn grondgebied geen arrestatie

[31] *Parl.St.* Kamer 1999-2000, DOC 50 0213-0214/001, 22.
[32] *Parl.St.* Kamer 1999-2000, DOC 50 0213-0214/001, 23.
[33] Artikel 88*ter* Sv.
[34] PH. VAN LINTHOUT en J. KERKHOFS, "Inleiding tot het materieel en strafprocedureel cyberstrafrecht: uitdagingen voor de advocatuur", in DE MEULENAERE, B., *Internet &/@ Recht*, Gent, Larcier, 2013, 39.
[35] *Parl.St.* Kamer 1999-2000, DOC 50 0213-0214/001, 23.
[36] G. NERINCKX, "Computercriminaliteit" in DE CORTE, R. (ed.), *Praktijkboek Recht en Internet*, Titel II, Hoofdstuk 10, Brugge, Vanden Broele, 2006, 39.
[37] PH. VAN LINTHOUT en J. KERKHOFS, "Inleiding tot het materieel en strafprocedureel cyberstrafrecht: uitdagingen voor de advocatuur", in DE MEULENAERE, B., *Internet &/@ Recht*, Gent, Larcier, 2013, 39-40.
[38] RvS, afd. Wetg., advies 28.029/2 van 31 mei 1999, *Parl.St.* Kamer 1999-2000, DOC 50 0213-0214/001, 44.

verrichten, noch een proces-verbaal opmaken waarbij een strafbaar feit vastgesteld wordt, noch een onderzoek doen, enz. Dit is vaste internationale rechtspraak.[39]

Het is evenwel niet eenvoudig de precieze strekking van die regel te bepalen ten aanzien van het optreden van justitie of politie in verband met computergegevens, inzonderheid wat betreft bevelen tot opsporing en inbeslagneming van zulke gegevens. Dat probleem is niet alleen het gevolg van de blijvende onzekerheid die soms bestaat over de vraag waar computergegevens precies te vinden zijn. Het houdt ook verband met het feit dat een autoriteit, precies dankzij de informatica, gegevens in het buitenland kan navorsen zonder daarom het grondgebied van de staat waaronder ze ressorteert, in de letterlijke zin te verlaten.[40]

De internationale verwevenheid van de netwerken zal onvermijdelijk aanleiding geven tot gevallen waarbij tijdens de netwerkzoeking bestanden worden opgevraagd die zich in het buitenland bevinden.[41] De grensoverschrijdende netwerkzoeking vormt de uitzondering op de regel dat wanneer er voldoende tijd en kennis voorhanden is, de weg van de klassieke internationale rogatoire commissie moet worden gevolgd.[42] Wanneer in het kader van de netwerkzoeking blijkt dat gegevens die nuttig zijn voor dezelfde doeleinden als de inbeslagneming, zich niet op het grondgebied van het Rijk bevinden, wordt een pragmatische houding aangenomen. In die gevallen wordt een specifieke procedure gevolgd: de betrokken gegevens worden enkel gekopieerd, waarna de buitenlandse autoriteiten van deze actie in kennis worden gesteld.[43] De wetgever beschouwt deze houding analoog aan de '*hot pursuit*', een traditionele rechtsinstelling in het internationale zeerecht, een visie waarmee de Belgische Raad van State het niet eens is.[44]

Deze pragmatische houding kan worden aangenomen in drie gevallen. In de eerste plaats wordt zij aanvaard voor situaties waarin onderzoekers per toeval of onopzettelijk data uit het buitenland bekomen. Ten tweede geldt deze aanpak ook in de gevallen waarin onderzoekers tijdens de zoeking wel kennis hebben van het feit dat de gezochte bestanden in het buitenland zijn gesitueerd, maar er – op dat ogenblik – redelijkerwijze niet in slagen die staat te identificeren. Ten derde wordt deze procedure ook aanvaard wanneer tijdens de zoeking wordt vastgesteld dat de relevante bestanden zich op een welbepaalde plaats in een geïdentificeerde vreemde staat bevinden, maar de dringendheid het stopzetten van de netwerkzoeking alsook het beroep doen op een internationale rogatoire commissie waarbij de betrokkenen inmiddels de data zouden kunnen doen verdwijnen, in de weg staat.[45]

Die pragmatische aanpak is voor kritiek vatbaar. Een netwerkzoeking is immers een onderzoeksmaatregel die een inbreuk uitmaakt op het recht op eerbiediging van het privé-leven. In dat opzicht kan slechts een inbreuk op dit recht plaatsvinden in die gevallen die de wet bepaalt

---

[39] RvS, afd. Wetg., advies 28.029/2 van 31 mei 1999, *Parl.St.* Kamer 1999-2000, DOC 50 0231-0214/001, 45.

[40] RvS, afd. Wetg., advies 28.029/2 van 31 mei 1999 over een ontwerp van wet "inzake informaticacriminaliteit", *Parl.St.* Kamer 1999-2000, DOC 50-0213/001 en 50-0214/001, 45.

[41] F. MOLS, J. KEUSTERMANS en T. DE MAERE, "Informaticacriminaliteit" in VANDEPLAS, A., ARNOU, P. en VAN OVERBEKE, S. (red.), *Strafrecht en strafvordering. Artikelsgewijze commentaar met overzicht van rechtspraak en rechtsleer*, Kluwer, Mechelen, 2010, 34.

[42] D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context", in VERSTRAETEN, R. en VERBRUGGEN, F. (eds.), *Straf- en strafprocesrecht*, Brugge, die Keure, 2010, 149.

[43] G. NERINCKX, "Computercriminaliteit" in DE CORTE, R. (ed.), *Praktijkboek Recht en Internet*, Titel II, Hoofdstuk 10, Brugge, Vanden Broele, 2006, 40; D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context", in VERSTRAETEN, R. en VERBRUGGEN, F. (eds.), *Straf- en strafprocesrecht*, Brugge, die Keure, 2010, 149.

[44] RvS, afd. Wetg., advies 28.029/2 van 31 mei 1999, *Parl.St.* Kamer 1999-2000, DOC 50 0231-0214/001, 46.

[45] D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context", in VERSTRAETEN, R. en VERBRUGGEN, F. (eds.), *Straf- en strafprocesrecht*, Brugge, die Keure, 2010, 150.

en in de vorm die zij voorschrijft. Men kan bij de invulling van de manier waarop een netwerkzoeking gevoerd moet worden geen ruimte laten voor 'toevallige' schendingen van internationale regelgeving, van toepassing in België en/of in de landen waar er bewijsmateriaal wordt verzameld.[46]

Een uitbreiding van de netwerkzoeking tot buiten de landsgrenzen is evenwel enkel mogelijk wanneer "blijkt" dat de betrokken gegevens zich niet op het grondgebied van het Rijk bevinden. Het is derhalve uitgesloten dat bewust onderzoek wordt gedaan naar gegevens die zich in het buitenland bevinden, indien deze factor vooraf is gekend: in dat geval dient steeds een beroep te worden gedaan op de verdragen inzake internationale rechtsbijstand in strafzaken.[47]

Of het verzamelen van gegevens die zich in het buitenland bevinden al dan niet onwettig is vanuit het oogpunt van het internationale recht, moet vanzelfsprekend ook bezien worden ten aanzien van de eventuele weerslag van die mogelijke onwettigheid op de bewijskracht die de strafrechtbanken aan dat materiaal kunnen toekennen of ontzeggen. In dit opzicht kan de, recent wettelijk verankerde,[48] Antigoon-rechtspraak van het Belgische Hof van Cassatie worden toegepast. Eens de vaststelling van onrechtmatige bewijsgaring is gemaakt, mogen de onderzoeks- of vonnisgerechten volgens deze rechtspraak het bewijselement in kwestie in de regel toch aanwenden. Ze moeten het slechts uitsluiten indien ofwel:

- de naleving van de geschonden vormvoorwaarden op straffe van nietigheid wordt voorgeschreven;

- de begane onrechtmatigheid de betrouwbaarheid van het bewijs heeft aangetast;

- het gebruik van het onrechtmatig verkregen bewijs in strijd is met het recht op een eerlijk proces. De schending van het recht op een eerlijk proces moet worden beoordeeld rekening houdend met de elementen van de zaak in haar geheel genomen, inbegrepen de wijze waarop het bewijs verkregen werd en de omstandigheden waarin de onrechtmatigheid werd begaan. De bedoelde omstandigheden die de rechter in overweging kan nemen zijn bijvoorbeeld: (i) het feit dat de overheid de onrechtmatigheid al dan niet opzettelijk heeft begaan, (ii) de vraag of de ernst van het misdrijf de begane onrechtmatigheid veruit overstijgt, (iii) de vaststelling dat het onrechtmatig bewijs alleen een materieel element van het misdrijf betreft, (iv) de weerslag van de onrechtmatigheid op het beschermde grondrecht en (v) het puur formele karakter van de onrechtmatigheid.[49]

1.3.3. Meewerkverplichtingen

In verband met de meewerkverplichtingen is er in de eerste plaats een informatie- en meewerkplicht in hoofde van de *geïnformeerde derde*.[50] Deze bepaling laat de overheid toe om personen van wie wordt vermoed dat ze een bijzondere kennis hebben van het informaticasysteem dat het voorwerp uitmaakt van de zoeking of van diensten om gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, te

[46] F. MOLS, J. KEUSTERMANS en T. DE MAERE, "Informaticacriminaliteit" in VANDEPLAS, A., ARNOU, P. en VAN OVERBEKE, S. (red.), *Strafrecht en strafvordering. Artikelsgewijze commentaar met overzicht van rechtspraak en rechtsleer*, Kluwer, Mechelen, 2010, 35.

[47] G. NERINCKX, "Computercriminaliteit" in DE CORTE, R. (ed.), *Praktijkboek Recht en Internet*, Titel II, Hoofdstuk 10, Brugge, Vanden Broele, 2006, 41.

[48] De wet van 24 oktober 2013 'tot wijziging van de voorafgaande titel van het Wetboek van strafvordering wat betreft de nietigheden' voegt een nieuw artikel 32 toe aan de Voorafgaande Titel van het Wetboek van Strafvordering.

[49] http://www.eubelius.be/nl/spotlight/wettelijke-verankering-van-de-antigoon-rechtspraak (op 15 september 2014 laatst geraadpleegd).

[50] Art. 88*quater*, §§ 1-5 Sv.; ingevoegd bij de wet van 28 november 2000.

beveiligen of te versleutelen, bevelen inlichtingen te verstrekken over de werking ervan en over de wijze om er toegang toe te verkrijgen, of in een verstaanbare vorm toegang te verkrijgen tot de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen. De overheid kan in het licht van deze bepaling ook iedere geschikte persoon bevelen om zelf het informaticasysteem te bedienen of de ter zake dienende gegevens, die door middel daarvan worden opgeslagen, verwerkt of overgedragen, naargelang het geval, te zoeken, toegankelijk te maken, te kopiëren, ontoegankelijk te maken of te verwijderen, in de gevraagde vorm.

Verder bestaat er een meewerkplicht in hoofde van de *operatoren van telecommunicatienetwerken* en de *verstrekkers van telecommunicatiediensten*.[51] Onder bepaalde omstandigheden kan de overheid:

- telecommunicatie doen opsporen of de oorsprong of de bestemming van telecommunicatie laten lokaliseren;

- door middel van toegang tot de klantenbestanden van de operator of van de dienstenverstrekker overgaan tot de identificatie van de abonnee of de gewoonlijke gebruiker van een elektronische communicatiedienst of van het gebruikte elektronische communicatiemiddel;

- door middel van toegang tot de klantenbestanden van de operator of van de dienstenverstrekker overgaan tot de identificatie van de elektronische communicatiediensten waarop een bepaald persoon geabonneerd is of die door een bepaald persoon gewoonlijk gebruikt worden.

1.3.4. Informaticatap

Ook wordt nog in de mogelijkheid voorzien om met betrekking tot de misdrijven van valsheid in informatica, informaticabedrog, hacking en datasabotage gebruik te maken van enkele uitzonderlijke onderzoeksmaatregelen, met name het afluisteren, kennis nemen en opnemen van privécommunicatie of privételecommunicatie tijdens de overbrenging ervan, de zogeheten informaticatap.[52]

2. Administratieve rechtshandhaving: illustratie aan de hand van enkele voorbeelden

Zoals bij de strafrechtelijke rechtshandhaving rijzen vergelijkbare problemen bij rechtshandhaving via administratieve weg. Ook hier is het voor de overheid niet gemakkelijk om greep te krijgen op ICT-fenomenen en die te lokaliseren. Wat de administratieve rechtshandhaving betreft is er een veelheid aan toepassingen, vermits het om een veelheid aan materies gaat. Ter illustratie geven we twee materies als voorbeeld: de online kansspelen en omroep via het internet.

2.1. De kanalisatie van online kansspelen

2.1.1. Rechtshandhaving via vergunningsplicht

In België zijn kansspelen geregeld bij de wet van 7 mei 1999 'op de kansspelen, de weddenschappen, de kansspelinrichtingen en de bescherming van de spelers' (hierna: de Kansspelwet). Het uitgangspunt is een verbod op kansspelen, met uitzondering van een beperkt

[51] Art. 46*bis* en 88*bis* Sv.; ingevoegd bij de wet van 10 juni 1998.
[52] Art. 90*ter* § 1, Sv.; ingevoegd bij de wet van 30 juni 1994. Zie over de informaticatap o.m. J. KERKHOFS en PH. VAN LINTHOUT, "Inleiding tot het materieel en strafprocedureel cyberstrafrecht: uitdagingen voor de advocatuur", in DE MEULENAERE, B., *Internet &/@ Recht*, Gent, Larcier, 2013, 30-38.

aantal kansspelen.[53] De wet gaat uit van de "kanalisatiegedachte": om te voldoen aan de klaarblijkelijke speelbehoefte van de mens, wordt het illegale aanbod bestreden door het toelaten van een beperkt, door de overheid gecontroleerd "legaal" spelaanbod.[54] De regels daarvoor zijn bepaald in de Kansspelwet, die ook de Kansspelcommissie heeft ingesteld, die voor de exploitatie van kansspelen verschillende types vergunningen toekent. Het gaat om een gesloten vergunningensysteem, wat inhoudt dat voor de meeste kansspelen het aantal vergunningen wettelijk gelimiteerd is.

Tot 2010 regelde de Kansspelwet enkel de exploitatie van kansspelen in drie kansspelinrichtingen, nl. de casino's, de speelautomatenhallen en de cafés. Aangezien kansspelen via het internet niet waren geregeld, vielen ze onder het principiële verbod.

In de praktijk was er echter een wildgroei aan illegale online kansspelen, zodat de wetgever gedwongen werd om in te grijpen. Bij wet van 10 januari 2010 'tot wijziging van de wetgeving inzake kansspelen' werd deze vorm van kansspelen geregulariseerd en gekanaliseerd.

Sedert de wijziging ervan bij de wet van 10 januari 2010 bepaalt de Kansspelwet dat enkel houders van bepaalde vergunningen voor kansspelinrichtingen een *aanvullende* vergunning kunnen krijgen die noodzakelijk is voor het uitbaten van online kansspelen. Die aanvullende vergunning voor het online aanbieden van kansspelen kan bovendien enkel betrekking hebben op de uitbating van kansspelen van dezelfde aard als die welke zij in hun "*bricks and mortar*"-kansspelinrichtingen mogen aanbieden. Wie geen licentie heeft om in de reële wereld (offline) kansspelen aan te bieden, kan dergelijke spelen ook niet (zelfs niet eenmalig) via het internet aanbieden.

En alweer duikt een nieuwe uitdaging op: gok-apps die de mogelijkheid bieden om met een smartphone en mobiel internet altijd en overal te spelen, blijken erg succesvol vooral bij jongeren. Ze ontsnappen momenteel in de praktijk aan elke controle.[55]

2.1.2. Fiscale aspecten: belasting op de spelen en weddenschappen

De opmars van de digitalisering heeft ook effecten op fiscaal vlak. Nemen we het voorbeeld van de belasting op de spelen en weddenschappen die in België wordt geheven.[56] Het gaat om een zgn. gewestelijke belasting, d.i. een door de federale overheid ingestelde en bij bijzondere meerderheidswet geregelde belasting, maar waarvan de opbrengst aan de gewesten ten goede komt, die de aanslagvoet, heffingsgrondslag en vrijstellingen vrij kunnen bepalen.[57] De federale overheid staat kosteloos in voor de "dienst van de belasting"[58] en bepaalt de van toepassing zijnde procedureregels, tenzij een gewest beslist om voortaan die taken over te nemen.[59] Het

[53] Art. 4, § 1, van de Kansspelwet: "Het is eenieder verboden om, zonder voorafgaande vergunning van de Kansspelcommissie overeenkomstig deze wet toegestaan en behoudens de uitzondering door de wet bepaald, een kansspel of kansspelinrichting te exploiteren, onder welke vorm, op welke plaats en op welke rechtstreekse of onrechtstreekse manier ook."

[54] *Parl.St.* Kamer 2008-2009, DOC 52 1992/001, 4.

[55] *De Standaard* 29 september 2014, 4: "Kansspelcommissie waarschuwt voor populaire gokspelletjes: 'Generatie verslaafden door gratis gok-apps'".

[56] Titel III van het Wetboek van de met Inkomstenbelasting Gelijkgestelde Belastingen (hierna: WIGB).

[57] Artikelen 3, eerste lid, 1°, en 4, § 1, van de bijzondere wet van 16 januari 1989 'betreffende de financiering van de gemeenschappen en de gewesten' (hierna: bijzondere financieringswet).

[58] De "dienst van de belasting" heeft betrekking op de feitelijke vaststelling van de belastinggrondslag, de berekening van de belasting, de controle van de belastinggrondslag en van de belasting, de daarop betrekking hebben betwistingen (zowel administratief als gerechtelijk), en de inning en de invordering van de belastingen (met inbegrip van de kosten en de interesten) (Grondwettelijk Hof 19 september 2014, nr. 130/2014, B.8.1).

[59] Artikel 5, § 3, van de bijzondere financieringswet.

Waalse Gewest heeft in die zin beslist en staat sedert 1 januari 2010 zelf in voor de inning van de belasting op de spelen en weddenschappen. Het Vlaamse Gewest en het Brusselse Hoofdstedelijke Gewest laten de inning ervan nog steeds over aan de federale belastingdiensten.

Vermits elk gewest eigen regels kan bepalen, is het van belang te weten waar de belaste activiteit te situeren is. De lokalisatie is ook van belang om te bepalen aan welk gewest de opbrengst moet worden toegewezen en welke instantie instaat voor het innen van de belasting.

De belasting op de spelen en weddenschappen wordt geacht te zijn gelokaliseerd "op de plaats waar de spelen plaatsvinden en de weddenschappen worden aangegaan".[60] Indien die spelen en weddenschappen offline gebeuren is het bepalen van de plaats niet zo heel moeilijk, maar indien het om online activiteiten gaat, is dat een veel complexere aangelegenheid.

N. HOEKX neemt, althans voor het lokaliseren van misdrijven, aan dat het aanbod een voldoende constitutief element is, of het nu gaat om een aanbod met reële formulieren dan wel om een aanbod via het internet.[61] Ze verwijst daarbij naar een arrest van het Franse Hof van Cassatie.[62]

Dat criterium is echter niet bruikbaar voor de lokalisering van de spelen en de weddenschappen binnen België met het oog op de toepassing van de fiscale wetgeving, omdat het aanbod normaal voor geheel België geldt (de Kansspelwet is nog steeds federale materie) en het zeer moeilijk is om de plaats in België te bepalen van waar het spel wordt gespeeld of de weddenschap wordt aangegaan. Om problemen te vermijden hebben de drie gewesten (het Vlaamse Gewest, het Waalse Gewest en het Brusselse Hoofdstedelijke Gewest) hun wettelijke regelingen op elkaar afgestemd: indien het gaat om sommen of inleggelden ingezet via informatiemaatschappij-instrumenten wordt een belasting van 11 procent geheven op de werkelijke brutomarge die ter gelegenheid van de spelen of weddenschappen wordt bereikt.[63] De sommen of inleggelden worden geacht ingezet te zijn in een bepaald gewest indien de spelen of weddenschappen worden ontvangen via een server die in het betrokken gewest gevestigd is of uitgebaat wordt.[64]

2.2. Omroep via het internet

In 2005 startte de partij het Vlaams Belang met een eigen zender, nl. "Digitale Radio VB6015", gericht op Vlaanderen en Nederland, die uitzond via de korte golf vanuit Rusland en via het internet.[65] Omdat het – wat de uitzendingen via de ether betreft – om een landelijke radio-omroep in de zin van het toenmalige artikel 31, § 2, 1°, van het Vlaamse Mediadecreet ging, waarvoor een vergunning vereist was, en – wat de uitzendingen via het internet betreft – om een radiodienst waarvoor op grond van de toenmalige artikelen 31, § 4, en 54, § 2, van het Vlaamse Mediadecreet een voorafgaande melding vereist was, en het Mediadecreet bepaalde dat omroepen onafhankelijk van politieke partijen moeten zijn, startte de mediatoezichthouder van de Vlaamse Gemeenschap een ambtshalve onderzoek.

Het Vlaamse Mediadecreet bevat nog slechts één artikel dat voorziet in straffen via de strafrechter, in verband met illegale uitrusting en programmatuur voor het ontvangen van

[60] Artikel 5, § 2, 1°, van de bijzondere financieringswet.
[61] N. HOEKX, *Kansspelen op het internet*, Gent, Larcier, 2011, 91.
[62] Cass. fr. 22 mei 1997, *Bull. crim.* 1997, n° 198.
[63] Art. 43*bis*, § 1 WIGB (versie Vlaamse Gewest); art. 44*bis*, § 1 WIGB (versie Waalse Gewest); art. 44*bis* WIGB (versie Brusselse Hoofdstedelijke Gewest).
[64] Art. 43*ter* WIGB (versie Vlaamse Gewest); art. 44*bis*, § 3 WIGB (versie Waalse Gewest); art. 44*bis* WIGB (versie Brusselse Hoofdstedelijke Gewest).
[65] http://nl.wikipedia.org/wiki/Digitale_Radio_VB6015.

omroepprogramma's. Het gros van de bepalingen van dat decreet wordt dus via administratieve weg gehandhaafd.[66]

In de loop van de procedure werd aangevoerd dat de technische apparatuur die voor de uitzendingen gebruikt werd (zowel de zendapparatuur voor de korte golf als de servers voor de verspreiding via het internet) in het buitenland gelegen was, en dat ook het zwaartepunt van de omroepactiviteiten buiten België lag.

De mediatoezichthouder zag dat anders en oordeelde dat de betrokken omroepactiviteiten wel degelijk aan de regels van de Vlaamse Gemeenschap onderworpen waren, op basis van de volgende vaststellingen:

- de omroepdienst is hoofdzakelijk op de Vlaamse Gemeenschap gericht;

- de omroep kan zich niet beroepen op het vrij verkeer van diensten binnen de Europese Unie, vermits hij niet in een andere EU-lidstaat, maar in Vlaanderen is gevestigd;

- het zwaartepunt van de omroepactiviteiten ligt in Vlaanderen, waar o.a. de redactionele keuzes over de inhoud van de programma's worden gemaakt.

De initiatiefnemers werden veroordeeld tot een administratieve geldboete van 12.500 euro en aangemaand om zich te conformeren aan de bepalingen van het Mediadecreet.[67]

De in verband met de beslissingen van de mediatoezichthouder ingestelde juridictionele beroepen werden alle verworpen.[68]

3. Nadere bespreking aan de hand van concrete toepassingsgevallen

3.1. De strijd tegen niet-vergunde online kansspelen[69]

3.1.1. Spelen van niet-vergunde online kansspelen is strafbaar

Niet enkel het exploiteren van een kansspel of kansspelinrichting, maar onder meer ook het deelnemen aan onvergunde kansspelen is strafbaar in België, alhans indien de speler "weet" dat het gaat om de exploitatie van een kansspel dat of een kansspelinrichting die niet is vergund in toepassing van de Kansspelwet.[70] De Kansspelcommissie maakt daarom op haar website een *white list* en een *black list* bekend met de vergunde, respectievelijk niet-vergunde sites.

---

[66] J. BAERT, "Regels voor omroepreclame in Vlaanderen en de handhaving ervan", *Auteurs & Media* 2008, (279) 286-292.

[67] http://www.vlaamseregulatormedia.be/media/4985/2005-113.pdf (basisbeslissing van 16 december 2005); http://www.vlaamseregulatormedia.be/media/6580/2006-002.pdf (beslissing van 21 april 2006 na bezwaar).

[68] GwH 17 januari 2007, nr. 14/2007; RvS 23 oktober 2008, nr. 187.279, Verstrepen en BVBA Business Concepts, Creations and Visualisations.

[69] Voor het uitwerken van dit onderdeel is in ruime mate gebruik gemaakt van volgende werken: N. HOEKX, Kansspelen op het internet, Gent, Larcier, 2011; A. DIERICK, "Online kansspelen – Wedden dat u ermee in aanraking komt" in B. DE MEULENAERE (ed.), Internet &/@ Recht, Gent, Larcier, 2013, 151-181.

[70] Art. 4, § 2, van de Kansspelwet: "Het is eenieder verboden deel te nemen aan een kansspel, de exploitatie van een kansspel of kansspelinrichting te vergemakkelijken, reclame te maken voor een kansspel of kansspelinrichting of spelers te werven voor een kansspel of kansspelinrichting wanneer de betrokkene weet dat het gaat om de exploitatie van een kansspel of kansspelinrichting die niet is vergund in toepassing van deze wet."

De Kansspelcommissie streeft er bovendien naar om, in samenwerking met de internettoegangleveranciers (IAP's of *internet access providers*), in België de toegang tot niet-vergunde sites te blokkeren. In de praktijk komt dit erop neer dat een computer met een Belgisch IP-adres, de site normaal niet kan betreden. Er zijn echter verschillende mogelijkheden om een dergelijke blokkering te omzeilen. Zo kan men de fictie creëren over een buitenlands IP-adres te beschikken, om op die manier toch toegang te krijgen tot de geblokkeerde site.[71] Zie bijvoorbeeld de mogelijkheden die te vinden zijn op http://www.mijn-ip.net/ip_adres_verbergen.asp (software om het IP-adres te maskeren of werken via een proxy server die zich in het buitenland bevindt) of het TOR(*The Onion Router*)-project (http://nl.wikipedia.org/wiki/Tor_(netwerk)).

In dat geval kan het algemeen opzet worden aangetoond waardoor de speler zich schuldig maakt aan het wetens en willens deelnemen aan een niet-vergund online kansspel en zal hij geen onoverwinnelijke dwaling kunnen inroepen. Hetzelfde geldt ingeval een (buitenlandse) casinosite een bewijs van woonst vraagt om de getrouwheid van de opgegeven nationaliteit na te gaan en de speler een onjuist bewijs levert.[72]

3.1.2. Exploiteren van niet-vergunde online kansspelen: bepaling van de plaats van het misdrijf

De normen die voor de exploitatie van het online spelen het belangrijkste zijn, zijn de specifieke kansspelwetgevingen van de nationale staten. Die wetgeving is meestal een mix van administratief recht en strafrecht. Het administratieve luik omvat de toekenning van vergunningen en de (administratieve) sancties verbonden aan de niet-naleving van de vergunningsvoorwaarden. Het niet beschikken over de vereiste vergunning wordt in alle landen streng bestraft, net omdat ze een belangrijke waarborgfunctie heeft. Maar ook andere overtredingen van de kansspelwetgeving worden bestraft met, soms zeer zware, strafsancties.[73]

In België wordt ervoor gekozen, in de eerste plaats door de Kansspelcommissie, om op actieve wijze buitenlandse aanbieders van online kansspelen zonder vergunning te vervolgen. Aangezien de Belgische Kansspelwet niet zelf haar territoriale toepassingsgebied bepaalt, moet daarbij gebruik worden gemaakt van de algemene regels inzake territoriale toepassing van de strafwet. Het uitgangspunt is dat de Belgische strafwet normaal slechts van toepassing is op misdrijven gepleegd op het eigen grondgebied, ongeacht de nationaliteit van de dader of van het slachtoffer. De stelregel daarbij is dat het misdrijf te situeren is op alle plaatsen waar zich een gedraging voordoet die een constitutief element van het misdrijf vormt (= *ubiquiteitsleer*). Daarnaast wordt de leer van de ondeelbaarheid gevolgd. Dit houdt in dat de Belgische rechter kennis mag nemen van alle elementen van het misdrijf die een ondeelbaar geheel vormen met het misdrijf dat op Belgisch grondgebied werd gepleegd.[74]

De combinatie door de Belgische rechtspraak van de objectieve ubiquiteitstheorie met de leer van de ondeelbaarheid kan tot de feitelijke toepassing van de effectenleer leiden.[75] In 2008 paste een

---

[71] A. DIERICK, "Online kansspelen – Wedden dat u ermee in aanraking komt" in DE MEULENAERE, B. (ed.), *Internet &/@ Recht*, Gent, Larcier, 2013, 167.

[72] A. DIERICK, "Online kansspelen – Wedden dat u ermee in aanraking komt" in DE MEULENAERE, B. (ed.), *Internet &/@ Recht*, Gent, Larcier, 2013, 167.

[73] N. HOEKX, *Kansspelen op het internet*, Gent, Larcier, 2011, 89.

[74] N. HOEKX, *Kansspelen op het internet*, Gent, Larcier, 2011, 90-91. Op die manier kan bv. deelneming in het buitenland aan misdrijven gepleegd in België ook worden bestraft onder de Belgische strafwet (N. HOEKX, *l.c.*, voetnoot 379).

[75] K. DE SCHEPPER en F. VERBRUGGEN, "Ontsnappen *space invaders* aan onze *pacmannen*? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverleners", *T. Strafr.* 2013, 150.

correctionele rechtbank[76] deze effectenleer toe in een cyberstrafzaak. De dader werd vervolgd voor o.m. hacking. De rechter achtte zich bevoegd op basis van de leer van de ondeelbaarheid: hij vond dat de plaats waar het slachtoffer had gemerkt dat het niet meer kon inloggen en dat enkele profielen waren gewijzigd, bevoegdheidsverlenende aspecten waren die één ondeelbaar geheel vormden met het misdrijf.[77]

Dit geval toont aan dat een *de facto*-toepassing van de effectenleer in cyberstrafzaken de strafrechter een erg ruime bevoegdheid kan verlenen. De vraag rijst of deze evolutie wel zo wenselijk is. Een te ruime toepassing van de effectenleer kan namelijk dezelfde nefaste gevolgen hebben als extraterritoriale jurisdictie, zoals rechtsonzekerheid en wetsconflicten. Bovendien hangt de plaats waar dit effect optreedt vaak af van louter toevallige omstandigheden, bijvoorbeeld de plaats waar iemand zijn mails checkt. Overigens vereist ook de effectenleer dat het effect onder de wettelijke misdrijfomschrijving kan worden gebracht. Merken dat je e-mailaccount werd gehackt, voldoet bezwaarlijk aan één van de constitutieve bestanddelen van het misdrijf hacking.[78]

Het misdrijf waar alles om draait, is het aanbieden van kansspelen zonder vergunning. Van belang voor het antwoord op de vraag naar de territoriale toepassing van de Belgische strafwet, is te weten wat de constitutieve elementen van dit misdrijf zijn. Volgens sommigen zijn de strafbare elementen van het misdrijf: de inzet, de uitbetaling, de spelkeuze enzovoort. Volgens anderen volstaat het louter aanbod, zodat de Belgische overheid bevoegd is zodra een aanbod op haar grondgebied plaatsvindt. Nog anderen koppelen het aanbod aan de effectieve aanvaarding van de inschrijving van de speler.[79]

Soms gebeurt de handhaving van de kansspelwetgeving niet door spontaan overheidsoptreden, maar langs indirecte weg, via *private enforcement*. Legale aanbieders vragen dan de staking van illegale offline of online activiteiten wegens schending van de Kansspelwet. Het vergunningsloze aanbod wordt dan gekwalificeerd als het profiteren van een oneerlijke en onrechtmatige voorsprong t.o.v. de optredende vergunninghouder. Ook de Belgische regering vindt een dergelijk burgerrechtelijk optreden in bepaalde gevallen efficiënter dan strafrechtelijke vervolging. In België zorgt de Nationale Loterij op die manier voor de handhaving van haar monopolie en dus van de wet op de Nationale Loterij.[80]

3.2. Blokkeren van websites met illegale content

Het internet biedt enorm veel mogelijkheden en is zeer flexibel. Een website kan snel worden opgezet en even snel weer van het net worden gehaald. De ICT-context is bovendien grensoverschrijdend: het gaat om immateriële, vluchtige data, waarvan de verwerking en opslag

---

[76] Corr. Dendermonde 29 september 2008, *T. Strafr.* 2009, 111-112, noot P. VAN LINTHOUT.

[77] K. DE SCHEPPER en F. VERBRUGGEN, "Ontsnappen *space invaders* aan onze *pacmannen*? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverleners", *T. Strafr.* 2013, 150.

[78] K. DE SCHEPPER en F. VERBRUGGEN, "Ontsnappen *space invaders* aan onze *pacmannen*? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverleners", *T. Strafr.* 2013, 150.

[79] N. HOEKX, *Kansspelen op het internet*, Gent, Larcier, 2011, 91.

[80] N. HOEKX, *Kansspelen op het internet*, Gent, Larcier, 2011, p. 93 en voetnoten 391 en 392, met verwijzingen naar Antwerpen 8 november 2007, *Jaarboek Handelspraktijken & Mededinging* 2007, 560, noot V. WELLENS; *NjW* 2008, 221, noot R. STEENNOT; *TBH* 2008, 436, noot C. DE PRETER en T. DE MEESE; Voorz. Kh. Brussel 11 september 2002, *Jaarboek Handelspraktijken & Mededinging* 2002, 605 en Gent, KI 31 maart 2009, *Telebet NV ea / Nationale Loterij*, KI2008/KI/215, *niet gepubl.* en Rb. Dendermonde 30 juni 2008, nr. DE.58.L6.104912/05/26, *niet gepubl*.

over de nationale grenzen heen kan gebeuren. Daartegenover staat de klassieke traagheid en omslachtigheid van het rechterlijk ingrijpen, laat staan van de traditionele internationale rechtshulp. Daarom wordt gezocht naar mogelijkheden om efficiënter te kunnen optreden. Het blokkeren van websites is een van die mogelijkheden.

3.2.1. Langs burgerrechtelijke en strafrechtelijke weg

De blokkering van websites kan zowel langs burgerrechtelijke als langs strafrechtelijke weg gebeuren.

De mogelijkheid om langs burgerrechtelijke weg de toegang tot bepaalde websites te laten blokkeren, komt voor in de Belgische Auteurswet[81]. In aangelegenheden die tot de respectieve bevoegdheid van die rechtbanken behoren, kunnen de voorzitter van de rechtbank van eerste aanleg of de voorzitter van de rechtbank van koophandel een bevel tot staking uitvaardigen ten aanzien van tussenpersonen wier diensten door derden worden gebruikt om inbreuk op het auteursrecht of op een naburig recht te plegen en dit op verzoek van elke betrokkene, van een gemachtigde vennootschap voor het beheer van de rechten (vb. SABAM, SOFAM) of van een beroepsvereniging of interprofessionele vereniging met rechtspersoonlijkheid.

Op basis daarvan heeft men in België "*The Pirate Bay*" initieel proberen aan te pakken. Het Antwerpse hof van beroep[82] willigde bij arrest van 26 september 2011 de eis van de Belgische antipiraterijvereniging B.A.F. in. Aan Telenet en Belgacom, de belangrijkste Belgische internetproviders, werd toen het bevel gegeven om een lijst van elf limitatief opgesomde domeinnamen die toegang verschaften tot de *Pirate Bay*-website, te blokkeren door middel van DNS-blocking.[83] Dat arrest bracht echter weinig zoden aan de dijk. Kort na de uitspraak van het arrest moest immers vastgesteld worden dat de *Pirate Bay*-website opnieuw toegankelijk was via nieuwe domeinnamen. De antipiraterijvereniging B.A.F. heeft enkele maanden na dat arrest haar strijd tegen *The Pirate Bay* over een andere boeg gegooid, het burgerrechtelijke pad verlaten, en een klacht met burgerlijkepartijstelling ingediend in handen van de onderzoeksrechter.[84]

De strafrechtelijke blokkering van websites is nl. de tweede piste die men kan bewandelen. Daartoe kan men bijvoorbeeld een klacht met burgerlijke partijstelling indienen bij de onderzoeksrechter. Een andere mogelijkheid om een website strafrechtelijk te laten blokkeren, is via het online platform "*e-cops*". *E-cops* is een Belgisch overheidsmeldpunt voor internetmisbruik dat tot stand kwam op gezamenlijk initiatief van de *Federal Computer Crime Unit* van de Federale Gerechtelijke Politie (FCCU) en de Federale Overheidsdienst Economie, KMO, Middenstand en Energie. Op de website kan je een online formulier invullen vb. wanneer je terecht bent gekomen

[81] Wet van 30 juni 1994 'betreffende het auteursrecht en de naburige rechten' (hierna: Auteurswet), hoofdstuk VIII ("Algemene bepalingen"), afdeling 3 ("Burgerlijke rechtsvordering ter zake van auteursrecht"). De auteurswet wordt opgeheven met ingang van 1 januari 2015 en vanaf die datum geldt de overeenstemmende regeling opgenomen in boek XI ("Intellectuele eigendom"), titel 9 ("Burgerrechtelijke aspecten van de bescherming van intellectuele eigendomsrechten") van het Wetboek van Economisch Recht van 28 februari 2013.

[82] Antwerpen 26 september 2011, *RABG* 2011, 1269-1287, noot P. VAN EECKE en A. FIERENS, "Pirate Bay: schip voor anker in de Antwerpse haven".

[83] Bij DNS-blocking (wat staat voor "Domain Name System blocking") wordt aan de internettoegangsleverancier gevraagd om in diens databank de desbetreffende domeinnaam te schrappen waardoor het bijhorende IP-adres niet langer wordt herkend. Daartegenover staat de meer ingrijpende techniek van IP-blocking (waarin "IP" staat voor Internet Protocol) waarbij de internettoegangsleverancier wordt gevraagd om het IP-adres van een website te blokkeren. In dat geval kan noch via een domeinnaam noch via een IP-adres toegang tot de website worden verschaft. Die tweede techniek werd door het Antwerpse hof niet weerhouden.

[84] T.SCHOEFS, "Strijd tegen The Pirate Bay over andere boeg gegooid: databeslag toegestaan", *T.Strafr.* 2014, 134, noot bij Cass. 22 oktober 2013, P.13.0550.N en P.13.0551.N, *T.Strafr.* 2014, 126-131.

op een verwarrende site met misleidende informatie, wanneer je via e-mail ongewenste reclame of een frauduleus voorstel ontving of nog wanneer je kinderporno zag op een site. Die melding kan de aanleiding zijn voor een verdere actie door de FOD Economie, Politie of Justitie.

Of men kiest voor een burgerlijke partijstelling, dan wel voor een melding via het online platform *e-cops* maakt geen verschil uit voor het verdere verloop van de procedure: in beide gevallen wordt de informatie aan het parket bezorgd.[85] Daarop neemt het parket een beslissing, zonder de zaak eerst voor te leggen aan de grondrechter. De blokkering van een website langs strafrechtelijke weg gebeurt evenwel steevast in het kader van een opsporingsonderzoek of een gerechtelijk onderzoek en verloopt volgens de voorwaarden, opgesomd in artikel 39*bis* Sv. (zie hierna).[86] Die bepaling voorziet ook in een procedure om tegen de blokkeringsmaatregel op te komen, het zogenaamde strafrechtelijk kortgeding, met verzoekschrift bij de procureur des Konings en een beroepsmogelijkheid bij de kamer van inbeschuldigingstelling.[87]

De vraag van de bevoegde magistraat wordt aan alle betrokken operatoren via een centraal meldpunt meegedeeld, nl. de *Federal Computer Crime Unit* van de Federale Gerechtelijke Politie. De duur van de blokkering hangt af van de magistraat, maar is in principe onbeperkt. In het algemeen duurt de blokkering zo lang het misdrijf aanhoudt.[88]

3.2.2. Hoe verloopt het blokkeren van websites in België in de praktijk?[89]

De eerste stap bij het ontdekken van een internetsite met als illegaal beschouwde inhoud, is de bepaling van de geografische ligging van de servers waar de gegevens zijn opgeslagen.

Indien de server zich in België bevindt, dan zal onmiddellijk tot een feitelijke inbeslagname van de server of het wissen van de gegevens op basis van artikel 39*bis* van het Wetboek van Strafvordering (= databeslag) worden overgegaan. In dat geval is er geen blokkeringsprocedure op basis van de domeinnaam meer nodig.

Wanneer de server in het buitenland is gelegen of nog niet werd gelokaliseerd, dan zal de toegang tot deze gegevens worden verhinderd of zullen de gegevens ontoegankelijk worden gemaakt. In dat geval zal de procedure van artikel 39*bis*, § 3, van het Wetboek van Strafvordering worden toegepast die de magistraat, wanneer er geen inbeslagneming mogelijk is, in staat stelt om alle passende technische middelen aan te wenden om gegevens die het voorwerp van het misdrijf vormen of voortgekomen zijn uit het misdrijf ontoegankelijk te maken wanneer deze:

- strijdig zijn met de openbare orde (vb. dreigen met een aanslag, verspreiden van gevoelige informatie);
- strijdig zijn met de goede zeden (vb. kinderpornografie);

[85] Wat *e*-cops betreft geldt dit enkel voor nieuwe misdrijven die onder de Belgische rechtsmacht vallen. Wanneer via *e-cops* een melding wordt gedaan van een misdrijf dat onder een buitenlandse rechtsmacht valt, wordt geen pv opgesteld maar wordt de bevoegde buitenlandse (politie)dienst ingelicht via Interpol. Betreft de melding een bepaald fenomeen (vb. drugs) of heeft de melding betrekking op een fenomeen dat al het voorwerp van een strafdossier uitmaakt, dan wordt de bevoegde politiedienst ingelicht. Heeft de melding betrekking op een administratieve inbreuk naar Belgisch recht, dan wordt de bevoegde overheid in kennis gesteld.

[86] D. DECKMYN en N. VANHECKE, "Geen juridische basis om websites te blokkeren", *De Standaard*, 23 mei 2013, http://www.standaard.be/cnt/dmf20130522_090 (laatst geraadpleegd op 22 september 2014).

[87] *Vr. en Antw.* Senaat 2012-2013, Vr. 5-9486 (B. ANCIAUX).

[88] *Vr. en Antw.* Senaat 2011-2012, Vr. 5-4661 (B. ANCIAUX).

[89] Zie *Vr. en Antw.* Senaat 2011-2012, Vr. 5-4661 (B. ANCIAUX).

- een gevaar opleveren voor de integriteit van informaticasystemen of gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen (vb. verspreiding van virussen, *phishing*).

Technisch gezien gebeurt de blokkering door de domeinnaam van de website niet langer door te verwijzen naar het IP-adres van de website, maar om te leiden naar het IP-adres van de "STOP-pagina" van de Belgische overheid, gehost door Fedict, de federale overheidsdienst voor informatie- en communicatietechnologie. Hiervoor maakt de *Federal Computer Crime Unit* of de Kansspelcommissie de opgestelde vorderingen over aan de internettoegangleveranciers, die het originele IP-adres wijzigen in het IP-adres van de "STOP-pagina".[90] Deze pagina vermeldt: "U wordt naar deze stoppagina doorverwezen omdat de website die u tracht te bezoeken inhoud aanbiedt die door de Belgische wetgeving als illegaal wordt aanzien. Indien u beheerder of eigenaar van deze website bent en u meent dat deze maatregel ten onrechte is genomen, kan u een fax sturen op het nummer +32(0)2/733.56.16". Er bestaat m.a.w. een mogelijkheid om de blokkering aan te vechten, die uitdrukkelijk wordt vermeld op de stoppagina van de overheid.

3.2.3. Het blokkeren van kansspelwebsites

Laten we het fenomeen van de blokkering van websites verduidelijken aan de hand van het voorbeeld van de Kansspelcommissie en het blokkeren van illegale gokwebsites.

De Kansspelcommissie is opgericht als advies-, beslissings- en controleorgaan van de Federale Overheidsdienst Justitie.[91] De commissie beschikt over een secretariaat, waarvan de leden kunnen worden belast met het uitvoeren van onderzoeken ter plaatse. Deze leden van het secretariaat zijn rijksambtenaren met de hoedanigheid van officier van gerechtelijke politie, hulpofficier van de Procureur des Konings.[92] Inbreuken op de Kansspelwet (alsook op haar uitvoeringsbesluiten) kunnen zowel door politieambtenaren als door deze leden van het secretariaat van de Kansspelcommissie worden vastgesteld. In het kader van de uitoefening van hun functie kunnen de leden van het secretariaat alle voorwerpen, inzonderheid documenten, stukken, boeken en kansspelen, in beslag nemen die kunnen dienen als overtuigingsstuk betreffende een inbreuk op deze wet en haar uitvoeringsbesluiten of die nodig zijn om mededaders of medeplichtigen op te sporen.[93] In het kader van online kansspelen is, kan het beslag worden gelegd onder de vorm van databeslag of m.a.w. het blokkeren van de website waarop het illegaal online kansspel wordt aangeboden.

In het geval waarin een inbreuk wordt vastgesteld, wordt een proces-verbaal opgemaakt dat aan het bevoegde parket wordt overgezonden. Een afschrift van dat proces-verbaal wordt overgezonden aan de Kansspelcommissie evenals aan de persoon die de inbreuk heeft gepleegd.[94]

De procureur des Konings moet binnen een termijn van zes maanden aan de Commissie mededelen welk gevolg hij aan het proces-verbaal zal geven.

Wanneer de procureur des Konings aan de Kansspelcommissie ter kennis brengt dat een vervolging zal worden ingesteld of dat hij van oordeel is dat geen toereikende bezwaren voorhanden zijn, kan de Kansspelcommissie niet langer optreden: in het geval waarin de

[90] Mondelinge vraag van de heer RIK DAEMS aan de minister van Justitie over "het blokkeren van de toegang tot websites" (nr. 5-1003), *Hand.* Senaat 2012-2013, 23 mei 2013, nr. 5-104, 27.
[91] Artikel 9 van de Kansspelwet.
[92] Artikel 15, § 1, tweede lid Kansspelwet.
[93] Artikel 15, § 1, vierde lid, 4 Kansspelwet.
[94] Artikel 15, § 2 Kansspelwet.

procureur des Konings zelf vervolgt, is er immers een strafrechtelijk onderzoek lopende; in het geval waarin de procureur des Konings oordeelt dat er geen toereikende bezwaren voorhanden zijn, dient de Kansspelcommissie zich aan deze vaststelling van de feiten te conformeren.

De mogelijkheid bestaat echter dat de procureur des Konings, binnen een termijn van zes maanden te rekenen van de dag van ontvangst van het origineel van het proces-verbaal, geen mededeling doet aan de commissie of haar laat weten dat, zonder het bestaan van de inbreuk in twijfel te trekken, geen gevolg zal worden gegeven aan de feiten. In beide gevallen staat dan voor de Kansspelcommissie de mogelijkheid open om een administratieve geldboete op te leggen aan de betrokken daders.[95]

3.2.4. Blokkeren van buitenlandse websites

Er rijzen een aantal problemen bij de toepassing van artikel 39*bis* Sv., voornamelijk inzake de blokkering van in het buitenland gevestigde internetsites. Andere acties zouden kunnen worden overwogen, maar ook die veroorzaken een aantal problemen.[96] Er zou bijvoorbeeld een partnerschap kunnen worden overwogen met de bedrijven die domeinnamen beheren (eurid.eu/dns.be) voor de gevallen waarin de betrokken domeinnaam eindigt op ".eu" of ".be". Een dergelijke actie treedt echter buiten het wettelijk kader en de regels die de bedoelde maatschappijen uitwerken in de relaties met hun cliënten. Deze optie zou een eenvoudiger technischer alternatief zijn dan werken via het stelsel bij de operatoren, maar die techniek zou het toepassingsgebied van de maatregel niet beperken tot het grondgebied van België. Dat zou eventueel problemen kunnen veroorzaken ingeval de ten laste gelegde feiten niet strafbaar zijn in het buitenland.[97]

Er zou bijvoorbeeld ook gebruik kunnen worden gemaakt van artikel XII.5 van het Wetboek Economisch Recht, over de elektronische economie, en het koninklijk besluit van 7 mei 2003 'tot vaststelling van de modaliteiten volgens dewelke het vrije verkeer van een dienst van de informatiemaatschappij beperkt kan worden'. Deze wettelijke bepaling en haar uitvoeringsbesluit betreffen de gedeeltelijke omzetting van de richtlijn "Elektronische Handel"[98] en voorzien in de bestuurlijke procedure die moet worden gevolgd, onverminderd de gerechtelijke procedure, wanneer de openbare orde, de bescherming van de volksgezondheid, de openbare veiligheid of de bescherming van de consument in het gedrang komt. Conform artikel XII.5, § 1 van het Wetboek Economisch Recht kunnen de overheden maatregelen nemen tot beperking van het vrije verkeer van een dienst van de informatiemaatschappij geleverd door een in een andere lidstaat gevestigde dienstverlener. Die procedure is evenwel log en wordt bijgevolg zelden of zo goed als nooit toegepast.[99]

3.3. De Yahoo-saga: in hoeverre kunnen internationale internetbedrijven tot medewerking worden gedwongen?

Artikel 46*bis*, § 1 Sv. geeft de procureur des Konings de bevoegdheid om "zo nodig" de medewerking te vorderen van de "operator van een elektronisch communicatienetwerk" of van de "verstrekker van een elektronische communicatiedienst" om, door middel van een toegang tot

[95] Artikel 15/1 en 15/3 Kansspelwet. Uiteraard gelden hier nog bijzondere procedureregels, maar de bespreking hiervan zou ons te ver afleiden van het eigenlijke onderwerp van dit colloquium.
[96] *Vr. en Antw.* Senaat 2013-2014, Vr. 5-10040 (B. ANCIAUX).
[97] *Vr. en Antw.* Senaat 2013-2014, Vr. 5-10040 (B. ANCIAUX).
[98] Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt, *PB L* 178, 17 juli 2000, 1–16.
[99] *Vr. en Antw.* Senaat 2013-2014, Vr. 5-10040 (B. ANCIAUX).

de klantenbestanden van de operator of van de dienstenverstrekker, de abonnee of de gewoonlijke gebruiker van een elektronische communicatiedienst of van het gebruikte elektronische communicatiemiddel te identificeren. De operator van een elektronisch communicatienetwerk en de verstrekker van een elektronische communicatiedienst die weigert de gevraagde gegevens mee te delen kan krachtens artikel 46*bis*, § 2 Sv. een geldboete krijgen van minimum 26 euro tot maximum 10.000 euro, te verhogen met 50 opdecimes (wat neerkomt op een vermenigvuldiging van het boetebedrag met 6).[100]

Artikel 46*bis* Sv. is voorwerp van een aanslepende betwisting tussen het Belgische openbaar ministerie en het Amerikaanse Yahoo, die de Belgische rechtswereld al enkele jaren in de ban houdt. De uitkomst van die zaak zal immers "bepalend zijn voor de effectiviteit van de dagelijkse strijd op het terrein tegen criminaliteit via het internet, waarbij zeer frequent beroep moet worden gedaan op de medewerking van veelal in het [buitenland] gevestigde aanbieders van wereldwijde elektronische diensten".[101]

Naar aanleiding van een geval van oplichting vastgesteld door de politie van Aalst en gepleegd met gebruikmaking van een aantal e-mailadressen gratis ter beschikking gesteld – wellicht aan personen die zich op dat ogenblik niet in België bevonden – door Yahoo, vorderde de procureur des Konings te Dendermonde van Yahoo Inc., met zetel in de Verenigde Staten van Amerika en zonder vestiging in België, de mededeling van een reeks gegevens aangaande de met de mailadressen verbonden mailaccounts (o.a. de identificatie- en registratiegegevens van degene die de account creëerde). Hij maakte daarbij gebruik van de meewerkverplichting bedoeld in artikel 46*bis* Sv. voor de operator van een elektronische communicatienetwerk en voor de verstrekker van een elektronisch communicatiedienst.

Yahoo weigerde echter die gegeven mede te delen met het argument dat het om in de Verenigde Staten geregistreerde accounts gaat, zodat een dergelijke vraag moet verlopen via het Departement of Justice van de Verenigde Staten. Naast de territoriale onbevoegdheid van de Belgische overheid, voerde Yahoo ook de materiële onbevoegdheid aan, omdat het niet als "operator van een elektronisch communicatienetwerk" of "verstrekker van een elektronische communicatiedienst" in de zin van artikel 46*bis* Sv. te beschouwen zou zijn.

Op 2 maart 2009 veroordeelde de correctionale rechtbank van Dendermonde Yahoo echter tot een geldboete van 55.000 euro, op dat moment de maximumstraf. Volgens de rechtbank richt de wettelijke verplichting zich zonder onderscheid tot elke ISP die in België diensten ontplooit en aanwezig is. De betrokken e-mailaccounts zijn in België aangewend, terwijl ook Yahoo zowel commercieel (via een digitaal loket voor derden) als dienstenverstrekkend (voor de gebruikers) op het Belgisch territorium aanwezig is, zij het "virtueel", via het internet.[102]

Yahoo gaat in beroep en krijgt op 30 juni 2010 gelijk van het hof van beroep te Gent. Dat redeneert dat het webmail-systeem van Yahoo niet gekwalificeerd kan worden als een elektronische communicatiedienst in de zin van de Belgische wet. Volgens het Gentse hof van beroep is het de leverancier van de internettoegang (IAP) die integraal instaat voor het effectieve transport of de effectieve overbrenging van signalen over het internet. Het webmail-systeem zoals door Yahoo uitgewerkt en ter beschikking gesteld van de gebruikers van het internet, kan volgens het hof niet worden gekwalificeerd als een elektronische communicatiedienst in de zin van de Belgische wet. Het Yahoo-systeem verschaft webmail via een portaalsite en maakt zelf

[100] Art. 1, eerste lid, van de wet van 5 maart 1952 'betreffende de opdecimes op de strafrechtelijke geldboeten'.
[101] G.S., noot bij Antwerpen 20 november 2013, *T.Strafr.* 2014, 75.
[102] Corr. Dendermonde 2 maart 2009, *T.Strafr.* 2009, 116-124.

enkel gebruik van het internet, uitgebouwd en beheerd door – van Yahoo te onderscheiden – operatoren van netwerken en verstrekkers van elektronische communicatiediensten. De conclusie van het hof is dan ook dat "onvoldoende (is) komen vast te staan dat de materiële toepassingsvoorwaarden van artikel 46*bis* van het wetboek van strafvordering vervuld zouden zijn". Yahoo gaat derhalve vrijuit.[103]

Het openbaar ministerie gaat in cassatie en krijgt van het Belgische Hof van Cassatie op 18 januari 2011 gelijk, nota bene op andersluidend advies van de eerste advocaat-generaal. Het Hof van Cassatie oordeelt in het arrest dat als "verstrekker van een elektronische communicatiedienst" in de zin van art. 46*bis* Sv. te beschouwen is "niet alleen de Belgische operator in de zin van de wet van 13 juni 2005 betreffende de elektronische communicatie, maar iedereen die diensten van elektronische communicatie verstrekt, zoals onder meer de transmissie van communicatiegegevens".[104] Het arrest van het Gentse hof van beroep wordt vernietigd en de zaak wordt verwezen naar het hof van beroep van Brussel.[105]

Het hof van beroep te Brussel spreekt op 12 oktober 2011 Yahoo vrij. Het hof stelt dat het openbaar ministerie geen daden van opsporing kan verrichten of gelasten buiten het Belgisch grondgebied, terwijl geen bewijs voorligt van een geldig door de procureur des Konings binnen het Belgisch grondgebied aan beklaagde gerichte vordering tot mededeling van gegevens in de zin van art. 46*bis*, § 2 Sv. Volgens het hof volstaat daartoe niet het loutere gegeven dat het technisch mogelijk is om beklaagde vanop Belgisch grondgebied te bereiken bij wege van elektronische of andere communicatiemiddelen.[106]

Weer gaat het openbaar ministerie in cassatie. In een arrest van 4 september 2012 oordeelt het Hof van Cassatie kort maar krachtig dat de "omstandigheid dat de procureur des Konings zijn (…) schriftelijke vordering, waarbij de medewerking wordt gevorderd van een buiten het Belgisch grondgebied gevestigde operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst, verstuurt vanuit België aan een in het buitenland gelegen adres", die vordering niet ongeldig maakt, en verwijst het de zaak naar het hof van beroep te Antwerpen.[107]

---

[103] Gent 30 juni 2010, *T.Strafr.* 2011, 132-136, noot P.V.L.; PH. VAN LINTHOUT, "Yahoo is geen verstrekker van elektronische communicatiedienst", *De Juristenkrant* 27 oktober 2010, 4-5.

[104] Art. 46*bis* Sv. is ingevoerd bij de wet van 10 juni 1998 'tot wijziging van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privécommunicatie en -telecommunicatie'. In het wetsontwerp van de regering dat er aan de basis van ligt, werd oorspronkelijk slechts melding gemaakt van "de operator van een telecommunicatienetwerk" (*Parl.St.* Kamer 1996-1997, nr. 1075/1, 21). De regering diende echter amendementen in omdat de term "operator van een telecommunicatienetwerk" te beperkt geworden was en de regeling ook toegepast moest kunnen worden op "een dienstenaanbieder die niet noodzakelijk een operator van een netwerk is (bijvoorbeeld een Internet-toegangsleverancier of de zogenaamde '*access providers*'" (*Parl.St.* Kamer 1996-97, nr. 1075/2, 2-4; zie ook *Parl.St.* Kamer 1996-97, nr. 1075/9, 13 en 22). Bij de wet van 23 januari 2007 'tot wijziging van artikel 46bis van het Wetboek van strafvordering' is de notie 'telecommunicatie' vervangen door de notie 'elektronische communicatie'.

[105] Cass. 18 januari 2011, *T.Strafr.* 2011, 120-122, noot P.V.L.; *Nullem Crimen* 2011, 76-85, concl. eerste advocaat-generaal DE SWAEF; *Auteurs & Media* 2011, 218-223, noot N. VANDEZANDE ("Yahoo! als operator of verstrekker"); L. KERZMANN, "L'affaire *Yahoo!* ou à qui s'adresse l'obligation de collaboration instaurée par l'article 46*bis* du Code d'instruction criminelle?", *Revue du Droit des Technologies de l'Information* 2011, 116-123.

[106] Brussel 12 oktober 2011, *T.Strafr.* 2012, 472-474, noot PH. VAN LINTHOUT; *Auteurs & Media* 2012, 238-243, noot K. DE SCHEPPER ("Medewerking in een virtuele context? Ya! Hoo echter afdwingen?").

[107] Cass. 4 september 2012, *T.Strafr.* 2012, 464-465, noot PH. VAN LINTHOUT; P. DE HERT en G. BOULET, "Yahoo! moet meewerken met Belgische procureur", *De Juristenkrant* 12 september 2012, 8; O. LEROUX, "Arnaques,

Het arrest van het hof van beroep van Antwerpen dateert van 20 november 2013. Het hof veroordeelt Yahoo tot een geldboete van 48.000 euro (8000 euro x 6). Volgens het hof biedt de aanbieder van een (web)maildienst die instaat voor de verzending en transmissie van deze elektronische communicatie, diensten aan die geheel of hoofdzakelijk bestaan in het overbrengen van signalen via elektronische communicatienetwerken, zodat die aanbieder te beschouwen is als een verstrekker van een elektronische communicatiedienst in de zin van art. 46*bis* Sv. Een verstrekker van een elektronische communicatiedienst die zijn diensten ook in België aanbiedt, zoals gratis e-maildiensten, is in België territoriaal aanwezig en dus verplicht tot medewerking overeenkomstig art. 46*bis* Sv. Volgens het hof zijn de door de procureur des Konings gevorderde gegevens "draagbaar": de verstrekker heeft de actieve verplichting om deze te bezorgen waar ze gevraagd worden en dus in België te bezorgen. Het misdrijf van strafbare weigering tot mededeling bedoeld in artikel 46*bis*, § 2 Sv. voltrekt zich derhalve in België. Het hof merkt ten slotte nog op dat indien Yahoo zich niet wil onderworpen zien aan de verplichtingen van art. 46*bis*, § 2 Sv. het haar vrij staat het IP-bereik van België uit te sluiten.[108]

Na de veroordeling door het hof van beroep van Antwerpen, heeft ook Yahoo cassatieberoep ingesteld. Er wordt nu met spanning afgewacht hoe het Belgische Hof van Cassatie de zaak verder zal beoordelen.

4. Besluit

Rechtshandhaving in de virtuele wereld is allerminst evident. Het internet en de ermee verbonden technologie kent immers geen grenzen en evolueert erg snel. Nog meer dan bij het bestrijden van de internationale misdaad botst ons traditioneel rechtssysteem daarbij op zijn grenzen. Nieuwe wegen moeten dus worden gezocht, vermits de klassieke middelen niet meer volstaan. Het vraagt een grote alertheid en flexibiliteit van de overheid.

G.S. verwoordt het in het Tijdschrift voor Strafrecht als volgt:

"*Uiteindelijk zal de nieuwe (virtuele) realiteit van 'cyberspace' (moeten) leiden tot een herdenken, een heruitvinden van de traditionele basisconcepten uit het internationaal strafrecht als daar zijn: strafrechtsmacht, lokalisatie van een misdrijf, territorialiteit, soevereiniteit, internationale rechtshulp in strafzaken enz.*"[109]

Hetzelfde geldt overigens voor de administratieve rechtshandhaving.

Dat herdenken is volop bezig: met vallen en opstaan worden nieuwe mogelijkheden geconcipieerd, in de praktijk uitgetest en onderworpen aan rechterlijke toetsing. Het is opvallend dat de nieuwe regels regelmatig dienen te worden bijgesteld, om ze te verduidelijken, performanter te maken of in overeenstemming te brengen met het recht van de Europese Unie.

Daarbij wordt gezocht naar een bredere invulling van de rechtsmacht, bijvoorbeeld door te pogen om informaticamisdrijven in eigen land te lokaliseren en zo overtreders efficiënter te kunnen aanpakken. Terwijl in de reële wereld gepoogd wordt om de nationale grenzen te doen vervagen, proberen de staten grenzen in te stellen in de virtuele wereld en niet-getolereerde content "buiten de grenzen te houden" door de toegang ertoe af te sluiten of te bemoeilijken.

---

fraudes et escroqueries sur internet: moyens concrets d'investigation – Point sur l'affaire dite Yahoo! à la suite du second arrêt de la Cour de cassation", *JT* 2012, 839-843.

[108] Antwerpen 20 november 2013, *T.Strafr.* 2014, 73-76, noot G.S.; M. TAEYMANS, "Yahoo moet e-mailgegevens aan procureur overmaken", *De Juristenkrant* 29 januari 2014, 6.

[109] *T.Strafr.* 2014, 75.

Maar op termijn zullen de nationale staten tot het besef komen dat zij geïsoleerd vrij zwak staan. Een nauwere Europese en internationale samenwerking dringt zich onvermijdelijk op. Daarbij dreigt echter een conflict tussen zij die het internet als vrijstaat zien en de overheden die meer greep willen krijgen op het wereldwijde web.

Het zijn boeiende tijden.

BRONNENMATERIAAL

Rechtsleer

BAERT, J., "Regels voor omroepreclame in Vlaanderen en de handhaving ervan", Auteurs & Media 2008, 279-293.

DE HERT, P. en BOULET, G., "Yahoo! moet meewerken met Belgische procureur", De Juristenkrant 12 september 2012, 8.

DE SCHEPPER, K., "Medewerking in een virtuele context? Ya! Hoo echter afdwingen?", Auteurs & Media 2012, 239-243 [noot onder Brussel 12 oktober 2011].

DE SCHEPPER, K. en VERBRUGGEN, F., "Ontsnappen space invaders aan onze pacmannen? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverleners", *T.Strafr.* 2013, afl. 3, 143-166.

DEWANDELEER, D., "Misdrijven en strafonderzoek in de IT-context" in VERSTRAETEN, R. en VERBRUGGEN, F. (eds.), *Themis: Straf- en strafprocesrecht*, Brugge, die Keure, 2010, 125-163.

DIERICK, A., "Online kansspelen – Wedden dat u ermee in aanraking komt" in DE MEULENAERE, B., Internet &/@ Recht, Gent, Larcier, 2013, 151-181 (181).

G.S., noot onder Antwerpen 20 november 2013, T.Strafr. 2014, 75-76.

HOEKX, N., Kansspelen op het internet, Gent, Larcier, 2011, 606.

KERKHOFS, J. en VAN LINTHOUT, PH., "Inleiding tot het materieel en strafprocedureel cyberstrafrecht: uitdagingen voor de advocatuur" in DE MEULENAERE, B., *Internet &/@ Recht*, Gent, Larcier, 2013, 1-44 (181).

KERZMANN, L., "L'affaire Yahoo! ou à qui s'adresse l'obligation de collaboration instaurée par l'article 46bis du Code d'instruction criminelle?", Revue du Droit des Technologies de l'Information 2011, 116-123.

LEROUX, O., "Arnaques, fraudes et escroqueries sur internet: moyens concrets d'investigation – Points sur l'affaire dite Yahoo! à la suite du second arrêt de la Cour de cassation", JT 2012, 839-843.

MOLS, F., KEUSTERMANS, J. en DE MAERE, T., "Informaticacriminaliteit" in VANDEPLAS, A., ARNOU, P. en VAN OVERBEKE, S. (red.), Strafrecht en strafvordering. Artikelsgewijze commentaar met overzicht van rechtspraak en rechtsleer, Mechelen, Kluwer, 2010, 1-39.

NERINCKX, G., Computercriminaliteit in DE CORTE, R. (ed.), *Praktijkboek Recht en Internet*, Titel II, Hoofdstuk 10, Brugge, Vanden Broele, 2006, 46.

SCHOEFS, T., "Strijd tegen The Pirate Bay over andere boeg gegooid: databeslag toegestaan", T.Strafr. 2014, 131-142 [noot onder Cass. 22 oktober 2013, nr. P.13.0550.N en P.13.0551.N].

TAEYMANS, M., "Yahoo moet e-mailgegevens aan procureur overmaken", De Juristenkrant 29 november 2014, 6.

TAEYMANS, M., "Onderzoeksrechter mag toegang tot websites laten blokkeren", De Juristenkrant 4 december 2013, 2.

VAN DEN WYNGAERT, C., Strafrecht en strafprocesrecht. In hoofdlijnen, Antwerpen, Maklu, 2011, 1330.

VANDEZANDE, N., "Yahoo! als operator of verstrekker", Auteurs & Media 2011, 220-223 [noot onder Cass. 18 januari 2011].

VAN EECKE, P., en FIERENS, A., "Pirate Bay: schip voor anker in de Antwerpse haven", RABG 2011, 1278-1287 [noot onder Antwerpen 26 september 2011].

VAN LINTHOUT, Ph. "Yahoo is geen verstrekker van elektronische communicatiedienst", De Juristenkrant 27 oktober 2010, 4-5.

VAN LINTHOUT, Ph., "Territoriale bevoegdheid in cyberspace", T.Strafr. 2009, 113-114 [noot onder Corr. Dendermonde 29 september 2008].

Rechtspraak

HvJ 27 maart 2014, nr. C-314/12, UPC Telekabel.

Grondwettelijk Hof 19 september 2014, nr. 130/2014.

Grondwettelijk Hof 17 januari 2007, nr. 14/2007.

Cass.fr. 22 mei 1997, Bull.crim. 1997, n° 198.

Cass. 22 oktober 2013, nr. AR.P.2013.0551.N.

Cass. 4 september 2012, T.Strafr. 2012, 464, noot Ph. VAN LINTHOUT.

Cass. 18 januari 2011, T.Strafr. 2011, 120, noot P.V.L.; Nullum Crimen 2011, 76, concl. eerste advocaat-generaal DE SWAEF; Auteurs & Media 2011, 218, noot N. VANDEZANDE.

Cass. 24 februari 2004, Arr.Cass. 2004, 314.

Cass. 21 juni 1989, Arr.Cass. 1988-89, 620.

Cass. 4 februari 1986, Arr.Cass. 1985-86, 355.

Cass. 29 januari 1979, Arr.Cass. 1979, 575.

RvS 23 oktober 2008, nr. 187.279, Verstrepen en BVBA Business Concepts, Creations and Visualisations.

RvS, afd. Wetg., advies 28.029/2 van 31 mei 1999, Parl.St. Kamer 1999 – 2000, DOC 50 0213-0214/001.

Antwerpen 20 november 2013, T.Strafr. 2014, 73, noot G.S.

Brussel 12 oktober 2011, T.Strafr. 2012, 472, noot Ph. VAN LINTHOUT; Auteurs & Media 2012, 238, noot K. DE SCHEPPER.

Antwerpen 26 september 2011, RABG 2011, 1269, noot VAN EECKE, P., en FIERENS, A.

Gent 30 juni 2010, T.Strafr. 2011, 132, noot P.V.L.

Antwerpen 8 november 2007, Jaarboek Handelspraktijken & Mededinging 2007, 560, noot V. WELLENS; NjW 2008, 221, noot R. STEENNOT; TBH 2008, 436, noot C. DE PRETER en T. DE MEESE.

Gent, KI 31 maart 2009, Telebet NV e.a. / Nationale Loterij, KI2008/KI/215, niet gepubl.

Voorz.Kh. Brussel 11 september 2002, Jaarboek Handelspraktijken & Mededinging 2002, 605.

CA Versailles 4 maart 2009, Ministère Public / Patrick P., www.legalis.net, Revue Lamy droit de l'immatériel 2009, nr. 1554, noot M. TRÉZÉGUET.

Corr. Dendermonde 2 maart 2009, T.Strafr. 2009, 116.

Corr. Dendermonde 29 september 2008, T.Strafr. 2009, 111, noot Ph. VAN LINTHOUT.

Corr. Brussel 22 december 1999, Auteurs & Media 2000, 134, noot D. VOORHOOF.

Rb. Dendermonde 30 juni 2008, nr. DE.58.L6.104912/05/26, niet gepubl.

Wetgeving

Parl.St. Kamer 2010 – 2011, DOC 53 1639/001.

Parl.St. Kamer 2008 – 2009, DOC 52 1992/001.

Parl.St. Kamer 1999 – 2000, DOC 50 0213-0214/001.

Parl.St. Kamer 1996 – 1997, nr. 1075/1.

Vr. en Antw. Senaat 2013 – 2014, Vr. 5-10040 (B. ANCIAUX).

Vr. en Antw. Senaat 2012 – 2013, Vr. 5-9486 (B. ANCIAUX).

Vr. en Antw. Senaat 2011 – 2012, Vr. 5-4661 (B. ANCIAUX).

Hand. Senaat 2012 – 2013, 23 mei 2013, nr. 5-104 (mondelinge vraag van de heer R. DAEMS aan de minister van Justitie over "het blokkeren van de toegang tot websites" [nr. 5-1003]).

Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt, Pb.L 178, 17 juli 2000, 1-16.

Wet 24 oktober 2013 'tot wijziging van de voorafgaande titel van het Wetboek van strafvordering wat betreft de nietigheden', BS 12 november 2013.

Wetboek Economisch Recht (28 februari 2013), BS 29 maart 2013.

Wet 10 januari 2010 'tot wijziging van de wetgeving inzake kansspelen', BS 1 februari 2010.

Wet 23 januari 2007 'tot wijziging van artikel 46bis van het Wetboek van strafvordering', BS 14 maart 2007.

Wet 7 mei 1999 op de kansspelen, de weddenschappen, de kansspelinrichtingen en de bescherming van de spelers, BS 30 december 1999 ("Kansspelwet").

Wet 10 juni 1998 'tot wijziging van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privécommunicatie en -telecommunicatie', BS 22 september 1998.

Wet 30 juni 1994 'betreffende het auteursrecht en de naburige rechten', BS 27 juli 1994 ("Auteurswet").

Bijzondere wet 16 januari 1989 betreffende de financiering van de gemeenschappen en de gewesten ("bijzondere financieringswet"), BS 17 januari 1989.

Wetboek van de met inkomsten gelijkgestelde belastingen (23 november 1965), BS 18 januari 1966.

Wet 5 maart 1952 'betreffende de opdecimes en de strafrechtelijke geldboeten', BS 3 april 1952.

Strafwetboek (8 juni 1867), BS 9 juni 1867.

Wetboek van strafvordering (17 november 1808), BS 27 november 1808.

Overige

DECKMYN, D. en VANHECKE, N., "Geen juridische basis om websites te blokkeren", De Standaard 23 mei 2013, http://www.standaard.be/cnt/dmf20130522_90.

VANHECKE, N., "Kansspelcommissie waarschuwt voor populaire gokspelletjes: 'Generatie verslaafden door gratis gok-apps'", De Standaard 29 september 2014, 4.

http://www.eubelius.be/nl/spotlight/wettelijke-verankering-van-de-antigoon-rechtspraak

http://nl.wikipedia.org/wiki/Digitale_Radio_VB6015

http://www.vlaamseregulatormedia.be/media/4985/2005-113.pdf

http://www.vlaamseregulatormedia.be/media/6580/2006-002.pdf