Rolnummer 2697
Arrest nr. 51/2004 van 24 maart 2004

A R R E S T

_____

In zake : de prejudiciële vraag betreffende artikel 550*bis* van het Strafwetboek, gesteld door de Correctionele Rechtbank te Gent.

Het Arbitragehof,

samengesteld uit de voorzitters A. Arts en M. Melchior, en de rechters L. François, M. Bossuyt, A. Alen, J.-P. Moerman en E. Derycke, bijgestaan door de griffier P.-Y. Dutilleux, onder voorzitterschap van voorzitter A. Arts,

wijst na beraad het volgende arrest :

*

* *

I. *Onderwerp van de prejudiciële vraag en rechtspleging*

Bij vonnis van 22 april 2003 in zake het openbaar ministerie tegen D. Goossens en anderen, waarvan de expeditie ter griffie van het Arbitragehof is ingekomen op 7 mei 2003, heeft de Rechtbank van eerste aanleg te Gent de volgende prejudiciële vraag gesteld :

« Schendt artikel 550*bis* van het Strafwetboek (ingevoerd bij wet van 28 november 2000, *Belgisch Staatsblad* van 3 februari 2001) de artikelen 10 en 11 van de Grondwet door de interne hacker slechts strafbaar te stellen wanneer een bijzonder opzet (nl. een bedrieglijk opzet of het oogmerk om te schaden) aanwezig is (artikel 550*bis*, § 2), terwijl de externe hacker reeds strafbaar is zodra een algemeen opzet aanwezig is (artikel 550*bis*, § 1) ? »

Memories zijn ingediend door :

- C. Muylaert, wonende te 9150 Bazel, Blauwe Gaanweg 50;

- B.V.;

- de Ministerraad.

De Ministerraad heeft een memorie van antwoord ingediend.

Op de openbare terechtzitting van 4 februari 2004 :

- zijn verschenen :

. Mr. A. Vermote, advocaat bij de balie te Brussel, *loco* Mr. J. Leysen, advocaat bij de balie te Kortrijk, voor B.V.;

. Mr. O. Vanhulst *loco* Mr. P. Hofströssler en Mr. K. Lemmens, advocaten bij de balie te Brussel, voor de Ministerraad;

- hebben de rechters-verslaggevers M. Bossuyt en L. François verslag uitgebracht;

- zijn de voornoemde advocaten gehoord;

- is de zaak in beraad genomen.

De bepalingen van de bijzondere wet van 6 januari 1989 op het Arbitragehof met betrekking tot de rechtspleging en het gebruik van de talen werden toegepast.

II. *De feiten en de rechtspleging in het bodemgeschil*

Naar aanleiding van een klacht met burgerlijke partijstelling, worden Dirk Goossens, Kris Muylaert en B.V. vervolgd op basis van artikel 550*bis*, § 1, van het Strafwetboek. Ze zouden zich toegang hebben verschaft tot het informaticasysteem van de n.v. Marke Research & Creation, of zich daarin hebben gehandhaafd, terwijl ze wisten dat ze daartoe niet gerechtigd waren.

De verwijzende rechter stelt vast dat artikel 550*bis* van het Strafwetboek een onderscheid maakt tussen externe en interne hacking. Alle beklaagden worden vervolgd als externe hackers.

De beklaagde B.V. werpt op dat de wetgever in artikel 550*bis* een ongeoorloofde ongelijkheid heeft ingevoerd tussen interne en externe hacking. Ten gevolge daarvan heeft de verwijzende rechter de hierboven geformuleerde vraag aan het Hof gesteld.

III. *In rechte*

- *A* -

A.1.1. De Ministerraad oordeelt dat het door de wetgever gecreëerde onderscheid bestaanbaar is met de artikelen 10 en 11 van de Grondwet om de volgende redenen.

Het onderscheid is gebaseerd op de toegangsbevoegdheid tot een informaticasysteem (externe versus interne hacking), wat als een objectief criterium moet worden beschouwd.

Met artikel 550*bis* werd door de wetgever een wettig doel nagestreefd, namelijk het beschermen van de vertrouwelijkheid, de integriteit en de beschikbaarheid van informaticasystemen en data. In het licht van dat uitgangspunt was het aangewezen om de bescherming van het netwerk te koppelen aan de hoedanigheid - insider of buitenstaander - van diegene die de inbreuk pleegt. De transgressie van buitenstaanders brengt het gehele netwerk in het gevaar. De insider daarentegen kan legaal kennis nemen van alle informatie die binnen zijn bevoegdheid valt. Hij is slechts strafbaar indien hij gehandeld heeft met bedrieglijk opzet of met het oogmerk om te schaden. Voor een bevoegdheidsoverschrijding die geïnspireerd is door een louter algemeen opzet, gaat de wetgever ervan uit dat er, gelet op de juridische band tussen de interne hacker en de eigenaar van het netwerk, interne mechanismen zijn die dergelijke gedragingen beter en efficiënter kunnen beteugelen. De wetgever heeft hier het strafrecht opgevat als « *ultima ratio* ».

Het onderscheid is pertinent doordat het bijdraagt tot het bereiken van het doel. De wetgever streeft immers ernaar de vertrouwelijkheid van data te waarborgen door, enerzijds, onbevoegden te bestraffen voor de inbreuk in het systeem en, anderzijds, bevoegden te bestraffen voor de bedrieglijke of schadelijke overschrijding van de toegangsbevoegdheid.

Met betrekking tot de evenredigheid oordeelt de Ministerraad dat de sancties in verhouding staan tot het beoogde doel. Aangezien het bij externe hacking niet mogelijk is om een beroep te doen op andere – interne - sanctiemechanismen, wat bij interne hacking wel het geval is, vermocht de wetgever het algemeen opzet van de externe hacker als uitgangspunt te nemen en voor de interne hacker een bijzonder opzet te vereisen. Bovendien worden beide categorieën hackers, wanneer er sprake is van bijzonder opzet, op een gelijke manier behandeld, wat verantwoord is, aangezien interne mechanismen in dit geval niet volstaan en aangezien het onderscheid tussen externe en interne hackers, indien de intentie om te schaden aanwezig is, van ondergeschikt belang is. Het onderscheid wordt bijgevolg slechts gehandhaafd voor zover het strikt noodzakelijk is.

A.1.2. De Ministerraad oordeelt ten slotte dat de vraag of de wetgever, in plaats van de strafbaarheidsdrempel voor de interne hacker hoger te leggen, niet veeleer had moeten kiezen voor verzwarende omstandigheden, niet aan de orde is, aangezien die keuze tot de appreciatiebevoegdheid van de wetgever behoort.

A.2. B.V., de vierde beklaagde voor de verwijzende rechter, oordeelt, onder meer met verwijzing naar het door de Raad van State over het in het geding zijnde artikel verleende advies, dat het door de wetgever gehanteerde onderscheidingscriterium niet pertinent is en dat voor het onderscheid geen redelijke en objectieve verantwoording voorhanden is. Hij is van mening dat de wetgever, bij zijn op het bestaan van interne sanctiemiddelen gebaseerde argumentatie, enkel aan de relatie tussen werkgever en werknemer heeft gedacht en niet aan andere relaties waarop de regel van de interne hacking ook van toepassing zou zijn (tussen klant en financiële instelling, tussen leerling en school, enz.). In dergelijke relaties volstaan interne sanctiemiddelen immers niet.

De stelling dat externe hacking op zichzelf de veiligheid van het netwerk in gevaar zou brengen, wordt bovendien als niet correct beschouwd, aangezien hackers vaak de onveiligheid van het bestaande netwerk willen illustreren en aanklagen.

Ten slotte is hij van oordeel dat de omstandigheid dat men reeds toegang heeft tot een informaticasysteem juist een strafverzwaring zou verantwoorden voor de hackers die handelen met een bedrieglijk opzet of een oogmerk tot schaden. Het strafrecht straft personen die misbruik maken van het vertrouwen dat zij genieten immers veelal zwaarder.

A.3. Kris Muylaert, tweede beklaagde voor de verwijzende rechter, herinnert aan de feiten van het geschil en beargumenteert zijn stelling dat de in het geding zijnde bepaling in strijd is met de artikelen 10 en 11 van de Grondwet uitsluitend met verwijzingen naar het door de Raad van State verleende advies, de parlementaire voorbereiding en rechtsleer.

A.4. In zijn memorie van antwoord oordeelt de Ministerraad dat niet blijkt dat de wetgever, wanneer hij verwijst naar het bestaan van interne sanctiemechanismen om het verschil in behandeling tussen de interne en de externe hacker te rechtvaardigen, enkel aan de relatie werkgever-werknemer zou hebben gedacht. Artikel 550*bis*, § 2, is ook toepasselijk op andere gevallen van interne hacking, precies omdat er ook in die gevallen sprake is van een bestaande juridische band tussen de eigenaar van het netwerk en de hacker.

De argumentatie van B.V., gebaseerd op het gegeven dat externe hackers vaak goede bedoelingen hebben, wordt door de Ministerraad betwist. Het feit dat iemand met goede bedoelingen, maar toch ook met algemeen opzet, in een netwerk binnendringt, belet geenszins dat afbreuk wordt gedaan aan de vertrouwelijkheid en de integriteit van het netwerk.

- *B* -

B.1.1. De prejudiciële vraag heeft betrekking op artikel 550*bis*, §§ 1 en 2, van het Strafwetboek, luidend als volgt :

« § 1. Hij die, terwijl hij weet dat hij daar toe niet gerechtigd is, zich toegang verschaft tot een informaticasysteem of zich daarin handhaaft, wordt gestraft met gevangenisstraf van drie maanden tot een jaar en met geldboete van zesentwintig frank tot vijfentwintig duizend frank of met een van die straffen alleen.

Wanneer het misdrijf, bedoeld in het eerste lid, gepleegd wordt met bedrieglijk opzet, bedraagt de gevangenisstraf zes maanden tot twee jaar.

§ 2. Hij die, met bedrieglijk opzet of met het oogmerk om te schaden, zijn toegangsbevoegdheid tot een informaticasysteem overschrijdt, wordt gestraft met gevangenisstraf van zes maanden tot twee jaar en met geldboete van zesentwintig frank tot vijfentwintigduizend frank of met een van die straffen alleen. »

B.1.2. De in het geding zijnde bepaling creëert een onderscheid gebaseerd op het al dan niet bezitten van toegangsbevoegdheid tot een informaticasysteem.

Personen die zich toegang verschaffen tot een informaticasysteem of zich daarin handhaven, terwijl zij weten dat zij niet daartoe gerechtigd zijn (hierna « externe hackers » genoemd), zijn strafbaar op basis van het enkele feit dat zij zich toegang verschaffen tot het systeem. Personen die toegangsbevoegdheid hebben tot een informaticasysteem (hierna « interne hackers » genoemd) zijn slechts strafbaar indien zij, met bedrieglijk opzet of met het oogmerk om te schaden, hun toegangsbevoegdheid overschrijden.

Bij interne hacking vormt bijzonder opzet (bedrieglijk opzet of het oogmerk om te schaden) een constitutief element van het misdrijf, wat niet het geval is bij externe hacking. Bij externe hacking volstaat een algemeen opzet en vormt het bijzonder opzet een verzwarende omstandigheid.

De verwijzende rechter vraagt of het aldus gecreëerde onderscheid bestaanbaar is met de artikelen 10 en 11 van de Grondwet.

B.2. Het staat aan de wetgever de voorwaarden vast te stellen waaronder handelingen of onthoudingen als strafbare feiten kunnen worden beschouwd. Het behoort tot de vrijheid van de wetgever om zich, bij het vaststellen van die voorwaarden, streng op te stellen. Hij mag zich daarbij evenwel niet onttrekken aan de eerbiediging van het grondwettelijk beginsel van gelijkheid en niet-discriminatie.

B.3.1. Met de uitvaardiging van de wet van 28 november 2000, waarvan artikel 6 de in het geding zijnde bepaling heeft ingevoerd, heeft de wetgever « de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en data » als een te beschermen rechtsbelang opgevat (*Parl. St.*, Kamer, 1999-2000, DOC 50-0213/001 en 0214/001, p. 10).

De idee die ten grondslag ligt aan de wet houdt, luidens de parlementaire voorbereiding, in « dat, wanneer bepaalde inlichtingen omwille van hun aard zelf een bijzondere bescherming rechtvaardigen, dit het voorwerp moet uitmaken van een apart beschermingsregime » (*ibid.*, p. 17). Daaraan werd toegevoegd : « het feit of deze inlichtingen vastgelegd zijn op papier of op een geïnformatiseerde drager, is ter zake irrelevant […]. Het door de nieuwe bepalingen beschermde rechtsbelang is op de eerste plaats de integriteit van het systeem » (*ibid.)*.

B.3.2. De wetgever heeft de integriteit van informaticasystemen bijgevolg opgevat als een te beschermen rechtsbelang, dat dient te worden onderscheiden van de integriteit van gegevens, die het voorwerp uitmaken van aparte beschermingsstelsels, zoals dat van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

Dit brengt met zich mee dat, wanneer door de hacking andere rechtsbelangen dan de integriteit van een informaticasysteem worden aangetast, de handeling een misdrijf kan uitmaken, niet enkel op basis van artikel 550*bis* van het Strafwetboek, maar eveneens op basis van andere door de wetgever omschreven strafbaarstellingen.

B.3.3. In het licht van de in B.3.1 omschreven algemene doelstelling heeft de wetgever het nodig geacht een onderscheid te maken tussen interne en externe hacking. Met betrekking tot dat onderscheid vermeldt de parlementaire voorbereiding het volgende :

« De logica van het voorontwerp houdt rekening met de realiteit dat het binnen een organisatie frequenter zal voorkomen dat er een ongeoorloofde toegang is tot bepaalde delen van het netwerk omwille van allerhande factoren (persoonlijke contacten, structuur van het netwerk, werkomgeving). Deze inbreuken kunnen weliswaar intentioneel zijn, maar worden slechts strafwaardig geacht als er een bijzondere negatieve bedoeling achterzit (strafrecht als *ultima ratio*) : interne controlemechanismen moeten voor de minder ingrijpende gevallen volstaan. Deze situatie is verschillend ten aanzien van derden die buiten het netwerk zitten : hun transgressie brengt op zichzelf de veiligheid van het interne netwerk in gevaar. » (*ibid.*, p. 16)

B.4.1. Het onderscheid tussen de in de prejudiciële vraag bedoelde categorieën van hackers berust op een objectief criterium, namelijk het al dan niet bezitten van een in het kader van een juridische verhouding verleende toegangsbevoegdheid tot een informaticasysteem.

B.4.2. De loutere omstandigheid dat bepaalde gedragingen aanleiding kunnen geven tot uit interne controlemechanismen voortvloeiende vormen van « sanctie » - privaatrechtelijke dan wel publiekrechtelijke die niet strafrechtelijk van aard zijn - kan geen verantwoording bieden voor het creëren van verschillen bij het bepalen van de voorwaarden waaronder een gedraging als misdrijf moet worden beschouwd.

Het strafrecht heeft tot doel inbreuken op de maatschappelijke orde te doen bestraffen. De strafvordering wordt uitgeoefend in het belang van de maatschappij en behoort tot de bevoegdheid van de strafgerechten. Zij kan enkel betrekking hebben op feiten die door de wet als misdrijf zijn omschreven en zij geeft, in geval van veroordeling, aanleiding tot de door of krachtens de wet voorgeschreven straffen.

De uit interne controlemechanismen voortvloeiende vormen van « sanctie » hebben een fundamenteel andere aard. Zij hebben niet noodzakelijk betrekking op feiten die door de wet als misdrijf zijn omschreven; zij hebben niet noodzakelijk tot doel inbreuken op de maatschappelijke orde te doen bestraffen; het initiatief en de bevoegdheid tot het nemen van sancties komen niet toe aan organen die, in het belang van de maatschappelijke orde, daartoe zijn aangewezen door de Grondwetgever en de wetgever.

B.4.3. Te dezen dient er evenwel rekening mee te worden gehouden dat de wetgever, in de in artikel 550*bis*, § 2, van het Strafwetboek vervatte strafbaarstelling, de toegangsbevoegdheid tot een informaticasysteem als criterium heeft gehanteerd.

De aard en de omvang van de toegangsbevoegdheid tot een informaticasysteem wordt in beginsel niet bepaald door de wetgever, maar overgelaten aan de beoordelingsbevoegdheid van de eigenaar van het systeem. De wetgever vermocht ervan uit te gaan dat de eigenaar van een informaticasysteem het best geplaatst is om te bepalen wie toegangsbevoegdheid verkrijgt en binnen welke grenzen.

De wetgever heeft daarbij bovendien rekening willen houden met het feit dat het loutere overschrijden van de verleende toegangsbevoegdheid, vanwege allerhande factoren, eigen aan de organisatie waarbinnen een informaticasysteem functioneert, niet steeds de integriteit van het informaticasysteem in het gedrang brengt en bijgevolg niet strafwaardig moet worden geacht. Aangezien dergelijke factoren de strafwaardigheid van externe hacking niet kunnen beïnvloeden, is de wetgever ervan uitgegaan dat die vorm van hacking steeds als strafbaar moet worden beschouwd.

B.4.4. In die omstandigheden is het niet kennelijk onredelijk dat de wetgever het overschrijden, zonder bijzonder opzet, van de door de eigenaar van het informaticasysteem verleende toegangsbevoegdheid, niet strafbaar stelt, onder verwijzing naar controlemechanismen waarover de eigenaar van het informaticasysteem beschikt.

Het gehanteerde onderscheidingscriterium is in dit licht pertinent om de vertrouwelijkheid, de integriteit en de beschikbaarheid van informaticasystemen en data te beschermen. Artikel 550*bis* van het Strafwetboek is in dit licht evenmin onevenredig. De wetgever vermocht immers van oordeel te zijn dat de externe hacker moet worden gestraft, ook al heeft hij niet gehandeld met bedrieglijk opzet of met het oogmerk om te schaden. Wanneer de hacking gebeurt met bedrieglijk opzet of met het oogmerk om te schaden heeft de wetgever bovendien voor de interne en de externe hacker dezelfde minimum- en maximumstraffen bepaald.

Om die redenen,

het Hof

zegt voor recht :

Artikel 550*bis* van het Strafwetboek, ingevoerd bij de wet van 28 november 2000, schendt de artikelen 10 en 11 van de Grondwet niet.

Aldus uitgesproken in het Nederlands en het Frans, overeenkomstig artikel 65 van de bijzondere wet van 6 januari 1989 op het Arbitragehof, op de openbare terechtzitting van 24 maart 2004.

De griffier, De voorzitter,

P.-Y. Dutilleux A. Arts