Niet elke grasduinende mol is een hacker

Waarom de Hoge Raad het begrip computervredebreuk te ver heeft opgerekt

Mr. M. (Michael) Berndsen en mr. C.J.J. (Christian) Visser*

De 'politiemol' Mark M. had als politieambtenaar toegang tot meerdere systemen met vertrouwelijke informatie. Hij zocht informatie op en deelde die met personen buiten de politieorganisatie. Nadat dit aan het licht kwam, werd het opzoeken van deze informatie ten laste gelegd als computervredebreuk. Met goedkeuring van de Hoge Raad heeft het hof deze feiten als computervredebreuk bewezen en gekwalificeerd. De rechtmatige toegang die de agent had, werd een valse sleutel zodra hij informatie opzocht die buiten zijn lopende onderzoeken viel. Wij menen op basis van de wet en de totstandkoming daarvan dat het hof en de Hoge Raad daarmee een onjuiste – want te extensieve – interpretatie van het begrip computervredebreuk hebben gehanteerd.[1]

Ongewenst grasduinen

Het opzoeken van informatie door medewerkers van organisaties terwijl dit voor de taakuitoefening niet nodig is, komt ten minste met enige regelmaat voor. In 2005 constateerde de politie dat meer dan 200 agenten hadden geprobeerd om het verkrachtingsdossier van voetballer Robin van Persie in te zien. Geen van hen maakte deel uit van het onderzoeksteam.[2] Een ander voorbeeld dat de media haalde, betrof de kwestie rond realityster 'Barbie', die in 2018 als gevolg van een overdosis drugs in een Haags ziekenhuis was opgenomen. Tientallen medewerkers van het ziekenhuis bleken zonder noodzaak daartoe Barbies medisch dossier te hebben geraadpleegd.[3] Een recenter voorbeeld ten slotte is de GGD-datadiefstal. In 2021 bleek dat GGD-medewerkers persoonsgegevens van bekende Nederlanders in het CoronIT-systeem hadden opgezocht en verspreid.[4]

De zaak van de politiemol was ernstiger. Niet alleen door de hoeveelheid bevragingen die hij in de politiesystemen deed, maar ook omdat hij de geheime politiegegevens doorgaf aan criminelen. Over de ernst en onwenselijkheid hiervan zal weinig discussie bestaan. Wel bestaat verschil van inzicht over de vraag of zijn handelen computervredebreuk oplevert.

Rechtbanken en hoven zien zich steeds vaker geconfronteerd met een tenlastelegging waarin ongeoorloofde zoekslagen ten laste worden gelegd als computervredebreuk (art. 138ab Sr). Alleen al in de gepubliceerde rechtspraak van 2021 is bijna maandelijks[5] een geval van ongeoorloofde raadpleging van systemen door medewerkers te vinden, waarbij dit telkens is bewezenver-

* Michael Berndsen is strafrechtadvocaat bij Meijers Canatan Advocaten te Amsterdam, gespecialiseerd in cybercrime. Christian Visser is strafrechtadvocaat bij Meijers Canatan Advocaten te Amsterdam, gespecialiseerd in cybercrime.

1 Voor de goede orde wordt opgemerkt dat de auteurs niet betrokken zijn geweest bij deze strafzaak.

2 www.bitsoffreedom.nl/2005/10/12/agenten-gluren-in-dossier-van-persie/, laatst geraadpleegd op 6 februari 2022.

3 https://eenvandaag.avrotros.nl/item/tientallen-snuffelden-ongeoorloofd-in-medisch-dossier-barbie/, laatst geraadpleegd op 6 februari 2022.

4 Zie o.a. Rb. Midden-Nederland 14 september 2021, ECLI:NL:RBMNE:2021:4419 en ECLI:NL:RBMNE:2021:4434.

5 Zeven keer een politiemedewerker, twee keer een GGD-medewerker, eenmaal een gemeenteambtenaar en eenmaal een militair. Overigens blijkt uit een Wob-verzoek bij de politie dat in 2019 t/m 2021 in respectievelijk 63, 65 en 64 gevallen sprake was van het onbevoegd raadplegen van systemen.

doi: 10.5553/BSb/266669012022003004008

klaard als computervredebreuk. Kort gezegd: zodra een medewerker zonder legitiem doel het systeem bevraagt, *hackt* hij het systeem. Ligt die uitleg voor de hand wanneer men eigen inloggegevens gebruikt en op zichzelf rechtmatig toegang heeft tot de betreffende systemen?

Van computervredebreuk is volgens artikel 138ab Sr sprake als iemand opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of een deel daarvan. Van binnendringen is in elk geval sprake als gebruik wordt gemaakt van een valse sleutel. De bedoeling van de wetgever zoals blijkt uit de parlementaire geschiedenis komt later in deze bijdrage aan de orde.

Hof en Hoge Raad over de politiemol

Terug naar de zaak van de politiemol. Van belang is dat de veroordeelde destijds een politiemedewerker was met toegang tot diverse systemen, waaronder het metazoeksysteem BlueView. Naar eigen zeggen doorzocht hij de systemen ook bij wijze van hobby, uit nieuwsgierigheid. Onder meer door een WOD-traject met undercoveragenten staat echter vast dat hij (ook) bevragingen van de politiesystemen deed op verzoek van derden. Een belangrijke rechtsvraag in zijn strafzaak was of zulke ongewenste raadplegingen van de systemen nu computervredebreuk opleveren.

Het hof is tot een veroordeling voor computervredebreuk gekomen. Daarbij heeft het hof overwogen dat de politiemol wist dat het systeem beveiligd was, dat hij doelbewust de beveiliging heeft doorbroken en dus is 'binnengedrongen'.[6] Daarbij heeft hij – aldus het hof – gebruikgemaakt van een valse sleutel, te weten zijn dienstnummer en zijn wachtwoord.[7] Hij was weliswaar *geautoriseerd* (hij beschikte immers over inloggegevens van de systemen), maar voor die gegevens *onbevoegd* (omdat hij de bevragingen niet deed in het kader van zijn werk).

In cassatie werd namens de verdachte stelling genomen tegen deze uitleg. Het hof zou een onjuiste uitleg hebben gegeven aan de begrippen 'binnendringen' en 'valse sleutel'.[8] De politiemol beschikte immers rechtmatig over een accreditatie voor de systemen.

Advocaat-generaal Spronken overwoog in haar conclusie dat de wetsgeschiedenis geen eenduidig antwoord geeft op de vraag of deze situatie nu onder computervredebreuk kan worden geschaard. De wetgever lijkt volgens Spronken bij de totstandkoming van de strafbaarstelling van hacken niet aan deze situatie te hebben gedacht. Omdat bij elke bevraging een waarschuwing in beeld komt dat misbruik en verstrekking van gegevens aan derden verboden is, waarna op 'OK' moet worden geklikt, concludeert de advocaat-generaal dat vaststaat dat Mark M. zijn autorisatie heeft overschreden.[9] Daarom zou sprake zijn van binnendringen met behulp van een valse sleutel. Daarbij overweegt Spronken nog dat dit potentieel leidt tot een 'erg groot' bereik van de strafbaarstelling van computervredebreuk, maar dat in casu geen sprake is van een grijs gebied.[10]

De Hoge Raad geeft in zijn arrest een weergave van de wetsgeschiedenis inzake computervredebreuk. Vervolgens benoemt het arrest dat de verdachte toegang had tot BlueView, dat die autorisatie diende voor zijn werk als opsporingsambtenaar, maar dat hij de systemen gebruikte zonder dat daartoe vanuit zijn politietaak aanleiding bestond. De Hoge Raad volstaat met de conclusie dat het oordeel van het hof niet onjuist en niet onbegrijpelijk is, en laat de veroordeling wegens computervredebreuk in stand.[11]

Kritiek

Met het arrest van de Hoge Raad inzake de politiemol is de heersende leer bevestigd. Het raadplegen van systemen zonder professionele noodzaak daartoe kan volgens diverse rechterlijke instanties computervredebreuk opleveren. Er is, aldus deze rechtspraak, sprake van binnendringen met behulp van een valse sleutel (art. 138ab lid 1 aanhef en sub c Sr).

Die uitleg komt ongetwijfeld tegemoet aan behoeften in de rechtspraktijk, nu langs deze weg kan worden opgetreden tegen nieuwsgierige blikken van medewerkers. Het is begrijpelijk dat hiertegen moet worden opgetreden, zeker in die gevallen waar geheime informatie bovendien met derden wordt gedeeld. Deze argumenten maken echter de heersende leer omtrent computervredebreuk nog niet juist.

Zo heeft advocaat-generaal Spronken overwogen dat de wetsgeschiedenis geen eenduidig antwoord geeft op de vraag of – in onze woorden – 'grasduinen' met eigen inloggegevens onder computervredebreuk valt. We zetten hieronder uiteen dat de wetsgeschiedenis daarover volgens ons wel degelijk helder is. De wetgever heeft er uitdrukkelijk voor gekozen om computersystemen en onderdelen daarvan te beschermen, en niet bepaalde informatie op die systemen.

Wij menen dat niet alleen de advocaat-generaal, maar ook de Hoge Raad een onjuiste – want te extensieve – interpretatie van de strafbepaling heeft gehanteerd. Wettekst noch wetsgeschiedenis bevat aanwijzingen dat deze situatie kan gelden als computervredebreuk. Wel

6 Hof 's-Hertogenbosch 4 mei 2020, ECLI:NL:GHSHE:2020:1514.
7 Het hof nam ook het gebruik van een *valse hoedanigheid* aan. De klacht over dit oordeel slaagde bij de Hoge Raad, maar leidde niet tot cassatie. Deze kwestie valt buiten het bestek van deze bijdrage.
8 Aldus samengevat in de conclusie van advocaat-generaal Spronken d.d. 31 augustus 2021, ECLI:NL:PHR:2021:777, randnummer 5.1 e.v.
9 Ibid., randnummer 5.27 e.v.
10 Ibid., randnummer 5.30.
11 HR 30 november 2021, ECLI:NL:HR:2021:1691, r.o. 2.4.2.

doi: 10.5553/BSb/266669012022003004008

zijn in de totstandkomingsgeschiedenis van artikel 138ab Sr aanwijzingen te vinden voor het tegendeel. Zoals hierna zal blijken, gaat ook de analogie met een fysieke valse sleutel (denk aan diefstal met een valse sleutel) mank. Ten slotte achten wij de uitleg van de Hoge Raad in strijd met het beginsel van rechtszekerheid (*lex certa*). Wij zullen deze stellingen toelichten.

Wettekst

Allereerst de wettekst. Wie artikel 138ab Sr zorgvuldig leest, ziet dat de tekst evident ziet op het verwerven van toegang tot een *systeem*. De strafbepaling is in andere woorden gericht op het binnenkomen, niet op het beschermen van informatie die men – eenmaal binnen – al dan niet kan raadplegen.

In artikel 90 Sr is gedefinieerd wat in elk geval onder een valse sleutel kan worden verstaan, namelijk *'alle tot opening van het slot niet bestemde werktuigen'*. In de jurisprudentie is dit uitgebreid tot o.a. sleutels, wachtwoorden en pinpassen tot het gebruik waarvan men niet gemachtigd is, zoals andermans sleutel, pas of wachtwoord. Uit de nu door de Hoge Raad aanvaarde uitleg volgt dat ook een eigen sleutel of wachtwoord kan worden gezien als valse sleutel als men daarmee de gegeven autorisatie overschrijdt. Die uitleg staat op gespannen voet met het tot nu toe gangbare bereik van het begrip 'valse sleutel'.

Wetsgeschiedenis

Ook de wetsgeschiedenis van de strafbaarstelling van hacken geeft blijk van een binair begrip van het binnenkomen in een systeem. Men is bevoegd om in te loggen, of men is het niet. Wij hebben geen indicatie kunnen vinden dat de wetgever bij computervredebreuk een onderscheid heeft willen maken tussen de ingelogde werknemer die bepaalde gegevens in het kader van zijn werk opzoekt en de werknemer die iets opzoekt met minder nobele intenties.

Zo heeft de minister in de memorie van antwoord meermalen benadrukt dat de strafbaarstelling van computervredebreuk gericht is op bescherming van het *systeem* als zodanig. De minister noemt bij wijze van analogie een kast die de daarin opgeborgen gegevens beschermt, waarbij het openbreken van die kast strafbaar is.[12] De minister duidt het geautomatiseerde werk aan als een 'huls' en schrijft: *'De huls [is] het object van bescherming, en niet de gegevens.'*[13]

Van die ratio wordt afstand genomen als op het niveau van gegevens wordt gekeken of een medewerker een werkgerelateerde noodzaak had om deze gegevens op te zoeken. Stel dat de politiemol rechtmatig is ingelogd in het systeem, een aantal bevragingen in lopende onderzoeken doet, en tussendoor een zoekslag maakt ten behoeve van een derde. Volgens de huidige lijn van de Hoge Raad kan dan sprake zijn van computervredebreuk terwijl hij zich al rechtmatig in het systeem, de 'huls', bevond.

Verderop in de memorie van antwoord stelt de minister het nog scherper:

> *'Gemeenschappelijk is dat de onbelemmerde kennisneming van gegevens, ook al zijn deze niet voor de betrokkene bestemd, niet strafbaar is. Evenmin is van belang of de kennisneming per ongeluk plaatsvindt dan wel opzettelijk de situatie is opgezocht om van de betrokken gegevens kennis te nemen. Strafbaarheid ontstaat eerst daar waar doelbewust getroffen voorzieningen met het oog op geheimhouding worden omzeild, om aldus de kennelijk door de rechthebbende niet gewenste kennisneming door derden, toch te bewerkstelligen.'*[14]

Kortom, de minister stelde expliciet dat zelfs opzettelijke kennisneming van gegevens die niet voor een betrokkene zijn bestemd, *niet* strafbaar is gesteld.

Dat de wetgever ten tijde van de totstandkoming van de Wet computercriminaliteit III nog steeds dit standpunt was toegedaan, kan worden afgeleid uit de toelichting op het toen ingevoerde verbod op heling van gegevens (art. 138c Sr). De minister schrijft over dit verbod:

> *'Hiermee wordt tegemoet gekomen aan situaties waarin personen gegevens van een computer waartoe zij rechtmatige toegang hebben, bijvoorbeeld vanwege hun functie bij een overheidsinstelling, zonder daartoe gerechtigd te zijn voor zichzelf of voor een ander overnemen.'*[15]

Ook in de recente wetsgeschiedenis wordt dus uitgegaan van rechtmatige toegang tot het systeem, zelfs als men die gebruikt om ongewenst gegevens over te nemen.

Kortom, wij menen dat het oordeel van de Hoge Raad in strijd is met zowel de wettekst als de kennelijke bedoeling van de wetgever.

Rechtszekerheid

Daartegen bestaat een belangrijk bezwaar, namelijk de rechtsonzekerheid die uit deze rechtspraak voortvloeit. Als computervredebreuk wordt uitgelegd op de manier zoals het is bedoeld, valt het bereik van de strafbepaling vrij duidelijk af te bakenen. Het gaat dan immers om al dan niet rechtmatige toegang tot een systeem. Die duidelijkheid verdampt bij aanvaarding van de nu heersende leer.

Als de rechtmatigheid van de toegang tot een systeem wordt beoordeeld aan de hand van de gegevens die men daarin opzoekt, wordt moeilijker voorspelbaar waar de grenzen liggen. Een politieagent die in opdracht van de leider van het opsporingsteam een bevraging doet, zit

12 *Kamerstukken II* 1990/91, 21 551, nr. 6 (MvA), p. 12.

13 Zo ook Koops en Oerlemans: *'Daarbij heeft de wetgever gekozen voor het beginsel dat gegevens als zodanig niet strafrechtelijk worden beschermd tegen (onrechtmatige) toegang of kennisneming: slechts strafbaar is de wijze waarop men zich die gegevens toe-eigent, door in te breken in computers of (tele)communicatie af te luisteren.'* in: B.J. Koops en J.J. Oerlemans (red.), *Strafrecht & ICT*, Den Haag: Sdu 2019, p. 29.

14 *Kamerstukken II* 1990/91, 21 551, nr. 6 (MvA), p. 28-29.

15 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 64.

doi: 10.5553/BSb/266669012022003004008

uiteraard goed. Maar hoe zit het met de agent die in zijn vrije tijd een merkwaardige situatie ziet op straat, en direct in zijn diensttelefoon een bevraging doet? Of de werknemer die uit beroepsmatige interesse een document van zijn collega opent en doorneemt? En stel dat deze collega dat doet uit *persoonlijke* interesse? Welke factoren bepalen of iemand de gegevens redelijkerwijs nodig had voor de uitoefening van zijn functie? Moet hiervoor binnen een organisatie beleid zijn, en leidt dat er dan toe dat hetzelfde gedrag binnen de ene organisatie strafbaar is en binnen de andere organisatie niet? Of kan de onbevoegde raadpleging van gegevens worden ingevuld aan de hand van feiten van algemene bekendheid en bewijsvermoedens? Op sommige van deze vragen lijkt nog geen algemeen antwoord te bestaan, en dat is bezwaarlijk te noemen.

Om deze lijn in de rechtspraak beter te kunnen beschouwen in het licht van het legaliteitsbeginsel is het nuttig om eerst kort stil te staan bij de regelconceptie en rechtenconceptie van legaliteit.[16]
De *regelconceptie* gaat uit van een legaliteitsconcept waarin strenge eisen worden gesteld aan de duidelijkheid van de wettekst, en waarbij de bedoeling van de wetgever een belangrijk hulpmiddel is bij de interpretatie van wettelijke bepalingen.[17] De rechtszekerheid van de potentiële verdachte – of liever: de burger die zijn gedrag wil afstemmen op de wet – staat daarbij centraal. De *rechtenconceptie* is een wat complexer begrip, waarin het verwezenlijken van 'rechtvaardigheid' centraal staat. De betekenis van rechtvaardigheid wordt onder meer afgeleid uit fundamentele rechten van burgers. Dit kan betekenen dat verandering van inzicht over algemene rechten leidt tot verandering van het bereik van strafbepalingen, terwijl in de wettekst geen letter is gewijzigd.[18] De huidige uitleg van artikel 138ab Sr lijkt dus vooral te kunnen worden verklaard vanuit de rechtenconceptie van legaliteit, waarbij kennelijk een maatschappelijke behoefte heeft geleid tot een ruimer bereik van de strafbepaling.

Wij menen dat de huidige lijn van de Hoge Raad leidt tot een grijs gebied waarbinnen op voorhand moeilijk aan te geven is of gedrag wel of niet strafbaar is.[19] De bepaling die feitelijk slechts verbiedt om zonder toestemming andermans computer binnen te dringen, verwordt zo tot een algemeen verbod op het kennisnemen van *bepaalde informatie*. Daarmee is het toepassingsbereik van artikel 138ab Sr en de voorzienbaarheid daarvan evident ruimer en bovendien minder duidelijk dan blijkens wettekst en parlementaire geschiedenis de bedoeling was.

Het door ons gesignaleerde probleem van onvoldoende rechtszekerheid is gecreëerd door beslissend te achten of er een beroepsmatige noodzaak van het raadplegen van gegevens bestaat, in plaats van de vraag of wederrechtelijk in een *systeem* wordt binnengedrongen.

Ontbrekende noodzaak

Als we deze bezwaren onder ogen zien, resteert de vraag waarom deze extensieve uitleg van computervredebreuk nodig wordt geacht. Weliswaar zijn vage normen soms onvermijdelijk[20] en kan de rechtspraak duidelijkheid verschaffen over het bereik van een norm,[21] maar dat laat onverlet dat er een noodzaak behoort te bestaan alvorens men een relatief duidelijke norm vervangt door een vage norm. Wij zien een dergelijke noodzaak niet.

De excessen waren tenslotte al vervolgbaar – denk aan de zaken waarin geheime informatie uit systemen wordt gedeeld met criminele groeperingen. Dan is immers sprake van schending van het ambtsgeheim (art. 272 Sr). In gevallen waar dat niet aan de orde is maar informatie wel wordt overgenomen, kan inmiddels worden vervolgd voor heling van gegevens (art. 138c Sr).[22] En in de minder ernstige gevallen, waar iemand zijn eigen nieuwsgierigheid bevredigt door te grasduinen in het systeem, kunnen rechtspositionele maatregelen worden getroffen.

Ook zonder deze ruime uitleg van computervredebreuk kan dus passend worden opgetreden tegen integriteitsschendingen van uiteenlopende aard en ernst. Een noodzaak voor de extensieve uitleg zien wij dan ook niet. Ook daarom ligt een interpretatie van de strafbepaling met de nadruk op een regelconceptie van legaliteit hier voor de hand.

Conclusie

Met instemming van de Hoge Raad heeft de strafbaarstelling van computervredebreuk een zeer ruim bereik gekregen. Dit ruime bereik leidt tot de onwenselijke situatie dat interne bedrijfsvoorschriften thans mede bepalen of een gedraging strafbaar is. Immers, het rechtmatig inloggen in een IT-systeem op het werk maar vervolgens zonder professionele noodzaak raadplegen van informatie, geldt inmiddels als hacken. Wij hebben betoogd dat deze uitleg in strijd is met de wettekst, haaks staat op de wetsgeschiedenis en bezwaren oproept vanuit het perspectief van rechtszekerheid. Het wezenskenmerk van computervredebreuk is niet langer het binnendringen in een systeem, maar wordt nu bepaald door de informatie die vervolgens wordt opgezocht. Voor deze extensieve uitleg – volgens ons *contra*

16 Ontleend aan R.M. Dworkin, *A Matter of Principle*, Oxford: Oxford University Press 1985, p. 9-32.
17 N. Rozemond, 'Legaliteit in het materiële strafrecht,' *RM Themis* 1999/4, p. 118.
18 Zie ook B. Jansen, 'Dworkin's Rights Conception of the Rule of Law in Criminal Law: Should Criminal Law be extensively Interpreted in Order to Protect Victims' Rights', *Neth. J. Legal Phil.* 2017/46, p. 166.
19 Volgens de dissertatie van Joost Nan is in ieder geval tot 2011 nooit een cassatieklacht over *lex certa* gegrond verklaard: J.S. Nan, *Het lex certa-beginsel* (diss. Tilburg), Den Haag: Sdu 2011, p. 232-233.
20 Nan 2011, p. 236-241.
21 EHRM 25 mei 1993, appl.no. 14307/88 *(Kokkinakis t. Greece)*, par. 52.
22 *Stb.* 2018, 322 (i.w.tr. op 1 maart 2019).

doi: 10.5553/BSb/266669012022003004008

legem – bestaat geen noodzaak. Niet elke vorm van grasduinen is hacken. De heersende leer overtuigt niet en vraagt om een koerswijziging van de Hoge Raad.

doi: 10.5553/BSb/266669012022003004008