

Vrijspraak voor hacker: een website is geen geautomatiseerd werk

Annotatie bij Gerechtshof Den Haag

23 augustus 2022, ECLI:NL:GHDHA:2022:1551

*mr. M. Berndsen*¹

Onlangs sprak de cyberkamer van het Haagse gerechtshof een verdachte vrij van computervredesbreuk. Hij werd verdacht van het hacken van de website van een onderneming, waarbij ook gevoelige informatie zou zijn buitgemaakt. De crux was dat het OM ten laste had gelegd dat hij "een geautomatiseerd werk, te weten de website" zou hebben gehackt. Het hof oordeelde dat een website geen geautomatiseerd werk is en sprak de verdachte dus vrij. Het arrest leverde op social media verbazing op. Betekent dit nu dat het inbreken op een website niet strafbaar is? Of is het een semantische kwestie? Draait immers niet elke website op een geautomatiseerd werk?

1. De uitspraak

De beschuldiging in de zaak luidde dat de verdachte met het programma SQLmap een website en de bijbehorende SQL-database zou hebben gehackt. Op die manier zouden o.a. wachtwoorden, adressen, bankrekeningsnummers en BIG-nummers van huisartsen zijn buitgemaakt. De rechtbank Den Haag kwam in 2020 tot een bewezenverklaring en legde een gevangenisstraf op van twee maanden, waarvan één maand voorwaardelijk, met een proeftijd van twee jaar.² De verdachte heeft hoger beroep ingesteld en kwam zo bij de cyberkamer van het Haagse gerechtshof terecht.

Het hof overwoog in het arrest dat een website een verzameling gegevens is, die als onderdeel van het World Wide Web via het internet toegankelijk is. De strafbepaling van computervredesbreuk verbiedt het opzettelijk en wederrechtelijk binnendringen in een *geautomatiseerd werk* (artikel 138ab Sr). Het hof moest zich dan ook buigen over de vraag of een website kan gelden als een geautomatiseerd werk.

In zijn beoordeling wijst het hof op de (destijds geldende) tekst van artikel 80sexies Sr, waarin een geautomatiseerd werk werd gedefinieerd als "een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen".³ Uit de parlementaire geschiedenis blijkt dat de wetgever bij een geautomatiseerd werk steeds uitsluitend het oog heeft gehad op fysieke apparaten. Daarbij benadrukte de wetgever dat het gaat om de bescherming van het voorwerp waarin de gegevens zich bevinden, en niet om de gegevens zelf. Het hof overweegt dat een website slechts een samenstel van gegevens is, zonder fysieke vorm, en dus niet kan gelden als 'inrichting'. Daarmee is niet voldaan aan de vereisten die worden gesteld aan een geautomatiseerd werk. Het gevolg is vrijspraak van computervredesbreuk.

2. Beschouwing

2.1. Betekenis van de uitspraak

Is het hacken van een website dus niet strafbaar, zoals sommige Twitteraars uit de uitspraak begrepen? Dat is een misverstand. Computervredesbreuk

1. Michael Berndsen is strafrechtadvocaat gespecialiseerd in cybercrime bij Meijers Canatan Advocaten te Amsterdam.
2. Rb. Den Haag 1 juni 2020, 09/767016-18 (niet gepubliceerd).

3. Het huidige artikel 80sexies Sr verstaat sinds 1 maart 2019 onder een geautomatiseerd werk "een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken." (Stb. 2018, 322).

kan namelijk wel degelijk worden gepleegd door in te breken in een website of een gebruikersaccount, maar dan moet het OM in de tenlastelegging wel het geautomatiseerde werk benoemen waarop is binnengedrongen.

Zou in deze zaak de tenlastelegging niet "een geautomatiseerd werk, te weten de website" hebben vermeld, maar "een geautomatiseerd werk, te weten de server(s) waarop de website wordt gehost", dan zou wel op juiste wijze een geautomatiseerd werk zijn aangeduid.

2.2. Andere uitspraken

Het komt vaker voor dat bij computervrederebreuk in de tenlastelegging niet wordt verwezen naar het achterliggende geautomatiseerde werk (bijv. de server), maar slechts naar de gebruikersinterface. Zo heeft het Hof Den Haag in 2020 al geoordeeld dat een Facebookaccount geen geautomatiseerd werk is.⁴ Rechtbank Amsterdam sprak vrij van een tenlastelegging waarin een 'internetbankieren-applicatie' als geautomatiseerd werd opgevoerd.⁵ De Rotterdamse rechtbank overwoog dat 'accounts van webshops' ook geen geautomatiseerd werk opleveren, bij gebrek aan een fysieke component.⁶

Aan de andere kant worden in een artikel van Van den Hurk 15 uitspraken van voornamelijk rechtbanken opgesomd waarin een 'niet-fysiek' fenomeen wél werd aangemerkt als een geautomatiseerd werk.⁷ Zo kwam het Amsterdamse hof tot een bewezenverklaring waarin '32 websites' werden aangemerkt als een geautomatiseerd werk.⁸ Kortom, er wordt tot op heden verschillend over geoordeeld.

2.3. Wetsgeschiedenis en literatuur

Toch is m.i. duidelijk dat de Haagse cyberkamer het bij het rechte eind heeft. In de wetsgeschiedenis is glashelder dat slechts *apparaten* worden beschermd tegen computervrederebreuk, en dus niet de daarop aanwezige data.⁹ De minister benadrukte tijdens de parlementaire behandeling: "*De huls [is] het object van bescherming, en niet de gegevens.*"¹⁰ Ook Koops &

Oerlemans bespreken de fysieke connotatie van het begrip geautomatiseerd werk.¹¹

Bij wijze van analogie wijs ik nog op de uitleg van 'bezit' van digitale kinderpornografie in cloudopslag. In 2020 hekelde de Hoge Raad de bewezenverklaring van het Haagse hof, inhoudende dat de verdachte "*een gegevensdrager, (...) te weten een digitale opslagruimte (Skydrive)*" in zijn bezit heeft gehad. De HR benadrukte het onderscheid tussen de voor de gebruiker beschikbare digitale opslagruimte en de (elders aanwezige) fysieke gegevensdrager waarop die opslagruimte zich bevindt. Ook daar speelt het fysieke element een rol en luistert de formulering van de tenlastelegging nauw.

2.4. Praktische aspecten

De nadruk op een fysiek apparaat hoeft niet te betekenen dat sprake is van één duidelijk aanwijsbare server waarop is binnengedrongen. Dat zou ook buitengewoon lastig zijn. Tegenwoordig zien we immers dat gegevens verspreid over vele servers en locaties in datacenters worden bewaard. Zo kan bij cloudopslag sprake zijn van blokken of containers waarin gegevens van verschillende gebruikers op volgorde van verwerking zijn opgeslagen.¹² Het benaderen van een gebruikersaccount zal doorgaans betekenen dat gegevens worden geladen vanaf diverse (al dan niet virtuele) servers. Van een hacker die inbreekt op één fysiek apparaat zal in de praktijk dus regelmatig geen sprake zijn.

Toch is dit voor de juridische beoordeling van beperkt belang. Meerdere servers tezamen vormen ook 'een geautomatiseerd werk of een deel daarvan', volgens de hiervoor genoemde definitie. De rechtspraak eist geen nadere aanduiding van die servers. Ook de locaties waar die servers staan zijn voor de beoordeling niet zo relevant, omdat de locatie van de verdachte zich bevond doorgaans als pleegplaats ten laste wordt gelegd. Het komt er voor het OM dus vooral op aan om in ieder geval te verwijzen naar 'een of meer server(s)'.

Ook uit eigen waarneming weet ik dat die verwijzing met enige regelmaat achterwege blijft. Voor de verdediging kan dit een dilemma opleveren omtrent het wel of niet voeren van verweer. Als namens verdachte bij pleidooi wordt aangevoerd dat (bijvoorbeeld) 'de internetbankierenomgeving' geen geautomatiseerd werk is en dat dus vrijpraak moet volgen, kan (en zal) de officier van justitie vermoedelijk de ontbrekende woorden toevoegen.¹³ Het kan dus in

4. Hof Den Haag 22 september 2020, ECLI:NL:GHDHA:2020:2005. Tegen deze uitspraak is door het OM geen cassatieberoep ingesteld.

5. Rb. Amsterdam 21 oktober 2021, ECLI:RBAMS:2021:6000.

6. Rb. Rotterdam 16 september 2021, ECLI:NL:RBROT:2021:9596.

7. J.W. van den Hurk, 'Geautomatiseerde werken en gegevensdragers, tijd voor vernieuwing', AA p. 367.

8. Hof Amsterdam 8 november 2017, ECLI:NL:GHAMS:2017:4753.

9. Zie hierover ook M. Berndsen & C.J.J. Visser, 'Niet elke grasduinende mol is een hacker. Waarom de Hoge Raad het begrip computervrederebreuk te ver heeft opgerekt', *Boom Strafblad* 2022, afl. 4, p. 160-164.

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

11. B.J. Koops & J.J. Oerlemans (red.), *Strafrecht & ICT*, Den Haag: Sdu 2019, p. 32 e.v.

12. Zie over de technische werking en duiding van cloudopslag: J.W. van den Hurk & S.J. de Vries, 'Cybercrime', *Strafblad* 2019, afl. 4, p. 34-44.

13. Wijziging van de tenlastelegging is mogelijk, zie art. 313 Sv (jo. 415 Sv) en het overzichtsarrest HR 1 februari 2011, ECLI:NL:HR:2011:BM9102, NJ 2011/394 m.nt. Y. Buruma.

het belang van de verdachte zijn om dit verweer juist *niet* te voeren, in de hoop dat in hoger beroep het hof ambtshalve vrijspreekt op deze grond. Daarna is immers geen wijziging meer mogelijk. Dat veronderstelt overigens wel dat de rechters of raadsheren geen opmerking maken over de redactie van de tenlastelegging.¹⁴ Mogelijk heeft het hof in deze zaak dergelijke hints niet gegeven, of heeft de advocaat-generaal geen aanleiding gezien om de tenlastelegging te wijzigen.

2.5. Kan het anders?

Intussen rijst de vraag of het anders kan. Als een website, account of bankomgeving zich per definitie bevindt op een (deel van een) geautomatiseerd werk, waarom wordt dan zo zwaar getild aan de vermelding van een fysiek apparaat in de tenlastelegging? Van den Hurk heeft er al op gewezen dat de wet enkel het apparaat beschermt, terwijl het een hackslachtoffer toch vooral om de bekeken of buitgemaakte gegevens zal gaan.¹⁵ Bovendien zal de aangever er niet altijd in slagen op de juiste manier het geautomatiseerde werk aan te duiden. We zagen hiervoor immers dat de serversstructuur voor de eindgebruiker doorgaans niet inzichtelijk is.

Kan de Hoge Raad dan niet gewoon uitgaan van de denkstap dat bij het inbreken in een website of account per definitie ook een geautomatiseerd werk is binnengedrongen?¹⁶ Het enkele noemen van 'een server' voegt immers niet veel toe. Dat zou weliswaar voor het OM en de rechtspraak een bruikbare oplossing zijn, maar verdient bepaald niet de voorkeur omdat de wettekst en wetsgeschiedenis zich hier zo duidelijk tegen verzetten. Een website of account *als zodanig* is nu eenmaal geen geautomatiseerd werk, en een dergelijk extensieve interpretatie lijkt op gespannen voet te staan met het materieel-rechtelijke legaliteitsbeginsel en het daaruit voortvloeiende beginsel van *lex certa*.¹⁷

Een fraaier alternatief lijkt mij om het door Van den Hurk voorgestelde begrip 'digitale omgeving' in de wettekst op te nemen.¹⁸ Dat begrip komt tegemoet

aan de wensen in de praktijk en neemt het huidige gebrek aan rechtseenheid weg. Bovendien is dat begrip toekomstbestendig. Tot die tijd lijkt mij de uitleg in het hier besproken arrest leidend en doet het OM er dus goed aan om telkens naar een of meer servers of een ander (deel van een) geautomatiseerd werk te verwijzen, dit op straffe van vrijspraak.

14. Zie over de toelaatbaarheid van zulke 'hints' richting het OM: L.M.G. de Weerd, 'Geen scheidsrechter maar rechter. Als de officier van justitie een lekke band heeft, mag de rechter die best plakken', *Trema* 2013, p. 156-160, en de reacties daarop in *Trema* 2013, p. 243-248.

15. Van den Hurk 2022, p. 370.

16. Zo heeft de Hoge Raad wel aanvaard dat een DDoS-attack op een website de werking van een geautomatiseerd werk belemmert, waarbij de HR overweegt dat "*de instandhouding van een actieve website vereist dat een geautomatiseerd werk (...) in werking is*" (HR 24 december 2021, ECLI:NL:HR:2021:1944, NJ 2022/124 m.nt. J.M. Reijntjes). Het hof leidt daar in het onderhavige arrest niet uit af dat de Hoge Raad een website als zodanig als een geautomatiseerd werk kwalificeert.

17. Zie voor een uitgebreide analyse van deze beginselen: J.S. Nan, *Het lex certa-beginsel* (diss. Tilburg), Den Haag: Sdu 2011.

18. Van den Hurk 2022, p. 378.