FRANSE RECHTSPRAAK OORDEELT DAT EEN COMPUTERVIRUS GEEN GEVAL VAN OVERMACHT UITMAAKT: WAT ZIJN DE GEVOLGEN VOOR BELGISCHE ONDERNEMINGEN?

COMMENTAAR OP HET ARREST VAN HET HOF VAN BEROEP VAN PARIJS VAN 7 FEBRUARI 2020

Florine De Ridder, advocaat, Affluo (f.deridder@affluo.be)

Marilyn Vandermarliere, advocaat, Affluo (m.vandermarliere@affluo.be)

Samenvatting. Het Hof van Beroep van Parijs oordeelde recent, in een geschil tussen een ICT-dienstverlener en diens cliënt, dat een computervirus niet kan beschouwd worden als geval van overmacht. Het arrest, dat aantoont dat het voor een onderneming geen sinecure is om zich van haar contractuele verplichtingen te ontdoen door zich te beroepen op overmacht, vraagt om een nieuwe beoordeling van de risico's verbonden aan commerciële relaties op dit punt. Dit zowel vanuit het perspectief van de dienstverlener als van haar cliënteel, wanneer deze laatste op haar beurt diensten levert aan een derde partij. De diensten die zij levert riskeren namelijk mee beïnvloed te worden door incidenten bij haar dienstverlener (al dan niet gekwalificeerd als overmacht). Concreet houdt dit in dat ondernemingen bijzonder waakzaam moeten zijn bij de onderhandeling van overeenkomsten en bij het opstellen van aansprakelijkheidsclausules, met name door het opnemen van een bepaling over gevallen van overmacht. Het Franse arrest illustreert daarnaast het belang voor ondernemingen om te voorzien in gepaste beveiliging van hun computersystemen, en toont het nut aan van verzekeringen die de risico's van mogelijke computeraanvallen dekken.

Heel wat situaties kunnen ertoe leiden dat de uitvoering van een contractuele verplichting in praktijk onmogelijk wordt gemaakt. Een voorbeeld daarvan zijn cyberaanvallen, die steeds vaker voorkomen en ook continu evolueren, waardoor ze steeds moeilijker te voorkomen zijn.

Het probleem van dergelijke cyberaanvallen – en de gevolgen ervan op de uitvoering van overeenkomsten – is onderwerp van een recent arrest van het Hof van Beroep te Parijs, dat zich moest uitspreken over een brandend actuele vraag: maakt een infectie door een computervirus een geval van overmacht uit?

Meer concreet lag de vraag voor of een ICT-dienstverlener ten aanzien van zijn klant kan worden ontheven van de naleving van zijn contractuele verplichtingen, bij het optreden van een cyberaanval tegen deze laatste.

De klant van de betrokken ICT-dienstverlener had deze laatste voor de rechter gedaagd om vergoeding te bekomen van de schade, die de klant geleden had ten gevolge van een *ransomware* aanval die een grote hoeveelheid van zijn computergegevens onbruikbaar had gemaakt door ze te versleutelen. De dienstverlener, die verantwoordelijk was voor de beveiliging en back-up van de computergegevens, was er niet in geslaagd om de gecompromitteerde bestanden te herstellen.

In zijn arrest van 7 februari 2020[1], oordeelde het Hof van Beroep te Parijs dat een computervirus "*niet onvoorspelbaar, noch onvermijdelijk*" is en aldus geen geval van overmacht uitmaakt.

Het Hof oordeelde dan ook dat de aanwezigheid van het virus de dienstverlener niet verhinderde zijn contractuele verplichtingen na te komen en hij derhalve niet van deze contractuele verplichtingen kon worden ontheven. De dienstverlener blijft aldus aansprakelijk ten aanzien van zijn cliënt.

Het is belangrijk erop te wijzen dat deze interpretatie van het begrip overmacht, zoals uitgelegd door het Hof van Beroep van Parijs, aanleunt bij de draagwijdte die er in het Belgische recht van oudsher aan wordt gegeven.

Hoewel er melding van wordt gemaakt in het Belgische Burgerlijk Wetboek, wordt het begrip overmacht niet uitdrukkelijk in de wet gedefinieerd. Artikel 1148 BW stelt dat: "*geen schadevergoeding is verschuldigd, wanneer de schuldenaar door overmacht of toeval verhinderd is geworden datgene te geven of te doen waartoe hij verbonden was, of datgene gedaan heeft wat hem verboden was*". De Franse *Code Civil* bevat een vergelijkbare bepaling.

Gezien het ontbreken van een echte wettelijke definitie, wordt de draagwijdte van het begrip overmacht bepaald op basis van rechtspraak en interpretaties uit de rechtsleer.

Vandaag de dag wordt overmacht in de Belgische rechtspraak en rechtsleer gedefinieerd als een onvoorzienbare en onvermijdelijke gebeurtenis die de uitvoering van de overeenkomst tijdelijk of definitief onmogelijk maakt (en ze dus niet slechts bemoeilijkt of bezwaart[2]), en dat buiten de wil om van de partij die zich op de overmachtssituatie beroept[3]. Met name worden situaties zoals natuurrampen, terrorisme en oorlogen beschouwd als typische gevallen van overmacht.

Overmacht ontheft de schuldenaar van zijn verplichtingen die door de overmachtssituatie worden verhindert. Meer concreet houdt dit in dat de schuldenaar aan zijn wederpartij geen (schade)vergoeding verschuldigd zal zijn voor het niet (tijdig) nakomen ervan.

De ontheffing kan verschillende vormen aannemen. Indien de uitvoering van bepaalde verplichtingen slechts tijdelijk wordt onmogelijk gemaakt, worden deze opgeschort zo lang de situatie van overmacht aanhoudt. Indien de naleving permanent onmogelijk wordt gemaakt, zal de schuldenaar definitief van zijn verplichtingen worden ontheven.[4]

Het is interessant om na te gaan hoe de twee traditionele voorwaarden van overmacht, namelijk enerzijds de onvoorzienbaarheid en anderzijds de onvermijdelijkheid ervan, worden toegepast in het specifieke geval waar de computersystemen van een bedrijf worden geïnfecteerd door een virus.

Wat het standpunt betreft dat het computervirus niet voldoet aan de voorwaarde van onvoorzienbaarheid, volgen we de redenering van het Hof gezien de continue toename van het aantal computeraanvallen - en in het bijzonder *ransomware* aanvallen – die wereldwijd bedrijven viseren.

---

[1] Cour d'appel de Paris, 7 février 2020, RG n° 18/03616.

[2] P. WÉRY, *Droit des obligations*, vol. 1, Bruxelles, Larcier, 2010, n°564.

[3] J.-FR. GERMAIN et Y. NINANE, « Force majeure et imprévision en matière contractuelle », *Droit des obligations,* Anthemis, 2011, pp. 82 et 83 et P. VANOMMESLAGHE, *Traité de droit civil belge. Tome II. Les obligations*, vol. 2, 2013, n° 966 et J. VAN ZULEN, « La force majeure en matière contractuelle : un concept unifié ? Réflexion à partir des droits belges, français et hollandais », *R.G.D.C.*, 2013/8, p.406.

[4] Voir notamment F. GLANSSDORF, « La force majeure », *J.T.*, n°6772, 2019, p. 358.

In het door de rechtbank onderzochte geval stellen we met name vast (hoewel de rechtbank hier niet op in gaat) dat de techniek die werd gebruikt om de bestanden van het cliënteel te infecteren bijzonder voorspelbaar was. Dit gebeurde namelijk door de verzending van een e-mail met een schadelijk bestand aan een werknemer van het bedrijf. Deze werkwijze is een van de meest door cybercriminelen toegepaste manieren om doelgericht computersystemen te infecteren.

Moeilijker is de vraag of een computervirus een situatie uitmaakt die men niet kan voorkomen. Kunnen we met name redelijkerwijze aannemen dat een leverancier van computerdiensten in staat kan zijn om elke cyberaanval tegen zijn cliënteel, die mogelijk impact heeft op de verplichtingen van de dienstverlener, te voorkomen of verhelpen en wel zodanig dat hij voortdurend in staat is om die verplichtingen – in dit geval de bewaring van de computergegevens – na te komen? Bij huidige evolutie, waar cyberaanvallen steeds veelvuldiger en professioneler worden uitgevoerd, is ons antwoord op deze vraag minstens genuanceerd.

De strikte interpretatie van het Parijse Hof heeft verstrekkende gevolgen, zowel voor de initiële dienstverlener als voor de klant die op zijn beurt diensten verleent aan een derde. Er moet immers rekening mee worden gehouden dat een cyberaanval die impact heeft op een cliënt van een ICT-dienstverlener (bijvoorbeeld een bank of advocatenkantoor) ook een - soms desastreuze – invloed kan hebben op de relaties die deze klant met haar eigen cliënteel onderhoudt.

Hoewel het Hof zich slechts moest uitspreken over de contractuele aansprakelijkheid van de ICT-dienstverlener aan zijn klant en niet verder ingaat op de vraag of deze laatste klant zich ten aanzien van de eigen klanten zou kunnen beroepen op overmacht, lijkt het logisch dat de redenering van het Hof ook in die laatste situatie zou worden toegepast.

Wat kunnen ondernemingen doen om de impact van een cyberaanval op hun contractuele relaties met hun klanten te beperken?

Ten eerste kunnen we niet genoeg benadrukken hoe belangrijk het voor elke onderneming is om haar computersystemen adequaat te beveiligen. Hoewel een dergelijke bescherming niet alle risico's van een cyberaanval uitsluit (het is moeilijk om de meest geavanceerde computeraanvallen tegen te gaan), kan men zich in elk geval beschermen tegen de meest voorkomende computervirussen.

Daarnaast raden wij alle dienstverlenende ondernemingen ten zeerste aan om bij de onderhandeling van contracten bijzondere aandacht te besteden aan de redactie van bedingen met betrekking tot hun aansprakelijkheid. Men heeft er met name alle belang bij om contractueel een clausule op te nemen die de definitie en gevolgen van overmacht regelt.

In het bijzonder raden wij dienstverleners aan om in hun contracten te stipuleren dat een virus zal worden beschouwd als geval van overmacht dat de dienstverlener kan ontslaan van zijn verplichtingen.

Het arrest van het Hof van Beroep te Parijs toont namelijk aan dat het voor een onderneming in voorkomend geval zeer moeilijk kan zijn om zich te beroepen op bevrijdende overmacht, indien daarover contractueel niets werd voorzien. De partijen hebben er dus alle belang bij om de toepassingsvoorwaarden en de gevolgen van overmacht (d.w.z. de opschorting van de verplichtingen van één of beide partijen, of zelfs de beëindiging van het contract in bepaalde gevallen) contractueel te modaliseren. Dit kan hen met name in staat stellen de interpretatie die traditioneel aan overmacht wordt gegeven te verruimen, maar vooral om de omslachtigheid van een gerechtelijke procedure te

vermijden. De toepassing van een overmachtsclausule vereist niet automatisch de tussenkomst van de rechtbanken.

Tot slot kan het nuttig zijn om te investeren in een verzekering die onder meer financiële verliezen dekt die verband houden met het optreden van een computeraanval (zoals een cyberverzekering).

Concluderend kan worden gesteld dat het becommentarieerde arrest een nuttig licht werpt op de beoordeling van de risico's van computervirussen in het kader van handelstransacties. De toekomst zal uitwijzen of de Belgische rechtbanken een vergelijkbare redenering zullen toepassen als het Parijse Hof. Gezien de gelijkenissen tussen het Franse en het Belgische recht, wat betreft het begrip overmacht, is dit op zijn minst waarschijnlijk.

In afwachting van een duidelijke en eensgezinde Belgische rechtspraak over dit onderwerp, kunnen we ondernemingen die diensten verlenen aan hun cliënteel ten stelligste aanraden om de (financiële) gevolgen van mogelijke cyberaanvallen zo veel mogelijk te voorkomen, met name door te voorzien in gepaste beveiliging van computersystemen, door zorgvuldig te onderhandelen over contractuele clausules m.b.t. aansprakelijkheid en overmacht en - idealiter - door het afsluiten van een verzekering tegen cyberrisico’s.