KRONIEK IT-RECHT 2020

DOOR / ESTHER VAN GENUCHTEN, ROBERT VAN SCHAIK & REINOUD WESTERDIJK

INLEIDING

2020 was een jaar waarin de samenleving meer dan ooit afhankelijk leek te zijn van informatietechnologie (IT). Videobellen werd voor vrijwel iedere sociale samenkomst de norm. Ook advocaten ondervonden hiervan de gevolgen: terwijl digitalisering binnen Project KEI eerder nog een (te) grote uitdaging bleek, stapten de gerechtelijke instanties in enkele weken noodgedwongen over op digitale zittingen. Tegelijkertijd installeerde een kwart van de Nederlandse bevolking CoronaMelder op de telefoon[1], ondanks het vele nepnieuws dat op sociale media verspreid werd over COVID-19.[2] Cybercriminelen speelden ondertussen genadeloos in op het virus door zorginstellingen en andere kritieke infrastructuur met ransomware[3] en DDoS-aanvallen[4] te bestoken.[5]

Ondanks deze hindernissen heeft 2020 interessante rechtspraak over IT-recht opgeleverd. In deze Kroniek benoemen we de meest opmerkelijke uitspraken, waarbij wij ons vooral richten op de verbintenisrechtelijke aspecten van het IT-recht. Dat betekent dat intellectuele eigendom en privacy niet zijn meegenomen; zeer belangrijke onderwerpen in de praktijk, maar daarom geschikt voor een eigen Kroniek. Nu over het IT-recht, vanwege de specifieke en ook gefragmenteerde aard ervan, minder wordt geprocedeerd dan in het strafrecht of het gewone vermogensrecht, besteden we naast hogerberoepuitspraken ook aandacht aan lagere rechtspraak.

ZORGPLICHT

De IT-leverancier moet bij de uitvoering van zijn werkzaamheden de zorg van een goed opdrachtnemer in acht nemen, zoals in algemene bewoordingen neergelegd in artikel 7:401 Burgerlijk Wetboek.[6] De zorgplicht in IT-contracten kan daarnaast contractueel verder worden vormgegeven. Dit maakt het zorgplichtvereiste casuïstisch van aard. Maar wat mag er redelijkerwijs van de IT-leverancier worden verwacht? Dat is een belangrijk en vaak terugkerend thema. Er is zelfs een toename aan rechtspraak zichtbaar waardoor dit – toch wat vage – begrip 'zorgplicht' steeds verder wordt ingekleurd en afgebakend.

Zorgplicht bij 'totaalpakket' versus simpele opdracht

De Amsterdamse rechtbank oordeelde op 14 november 2018 (ECLI:NL:RBAMS:2018:10124, publicatie 7 juni 2020) dat er bij de levering van een 'totaalpakket' van IT-diensten een vergaande zorgplicht bestond.[7] Het administratiekantoor O'Cliance was slachtoffer geworden van een ransomware-aanval, waarbij hackers tot in haar netwerk waren doorgedrongen en alle bestanden (inclusief alle back-upbestanden) op de server hadden versleuteld. Uit onderzoek dat O'Cliance naar de aanval had laten doen, kwam naar voren dat de aanval voorkomen had kunnen worden door een combinatie van (i) eenvoudige maatregelen (zoals sterkere wachtwoorden), (ii) technische maatregelen (zoals een VPN-toegang) en (iii) het verbeteren van de back-upvoorziening van O'Cliance. Daarop stelde O'Cliance haar IT-leverancier, die in opdracht een volledige IT-infrastructuur had aangelegd en op afroep het beheer en onderhoud verzorgde, aansprakelijk voor de geleden schade. Partijen waren het eens dat de IT--leverancier een 'totaalpakket' had geleverd, maar twistten over de vraag of de beveiliging van het netwerk hiervan deel uitmaakte. Partijen hadden geen afspraken op papier gezet en daarom was van belang wat partijen redelijkerwijs over de omvang van de opdracht konden begrijpen en wat zij over en weer van elkaar mochten verwachten.

De rechtbank vond het daarentegen moeilijk voorstelbaar hoe onder de opdracht 'een totaalpakket te leveren' niet ook de aanleg van de daarbij behorende beveiliging kon zijn inbegrepen. Door het netwerk aan te leggen zonder firewall en zonder externe back-ups, had de IT-leverancier de opdracht niet naar behoren uitgevoerd. Dat O'Cliance de voorgestelde beveiligingsmaatregelen van de hand zou hebben gewezen, maakt dit niet anders. Het had op de weg van de

De auteurs zijn allen advocaat bij Kennedy Van der Laan in Amsterdam. Collega Astrid Sixma las kritisch mee en zij danken student-stagiaires Ge'ez Engidashet, Eline Hangelbroek en Julia Siskina voor hun bijdrage aan het jurisprudentieonderzoek.

IT-leverancier gelegen de opdracht te weigeren vanwege de onuitvoerbaarheid, alternatieven aan te dragen of op zijn minst indringend en herhaaldelijk te waarschuwen voor de risico's die het achterwege laten van deze maatregelen met zich brachten. Dat werknemers van O'Cliance zelf kennis van zaken hadden op het gebied van IT, ontsloeg de IT-leverancier volgens de rechtbank niet van deze verantwoordelijkheid. De rechtbank concludeerde dat, gelet op de afspraak dat hij een totaalpakket inclusief beveiliging zou leveren, in combinatie met zijn professionele deskundigheid, de IT-leverancier niet kon volstaan met een enkele waarschuwing en berusting in de keuzes van O'Cliance.

Een soortgelijke zaak (vonnis 38, gepubliceerd via IT&R 1306 op 16 april 2020) voor de Stichting Geschillenoplossing Automatisering (SGOA) werd in de sleutel van de onrechtmatige daad beoordeeld. In casu werd een ondernemer slachtoffer van een ransomware-aanval, waarbij een inbreker toegang verkreeg tot het netwerk, vervolgens het toegangsniveau uitbreidde en bestanden (inclusief back-up) versleutelde.

Als gevolg van deze inbraak had de ondernemer geen toegang tot zijn IT-omgeving die noodzakelijk was bij de uitvoering van dagelijkse operationele activiteiten. Uit onderzoek van een cybersecuritybedrijf bleek dat het 'zeer aannemelijk' was dat de inbreker zich middels een 'brute-force aanval' toegang had verschaft tot het back-upsysteem dat door de IT-leverancier van de ondernemer werd beheerd. De ondernemer stelde de IT-leverancier vervolgens in gebreke omdat die niet zou hebben voldaan aan, kort samengevat, (i) zijn verplichting dat systeem adequaat te beveiligen en (ii) zijn verplichting zorg te dragen dat de gegevens steeds beschikbaar waren. Daarnaast had de ondernemer de IT-leverancier verzocht mee te werken aan de transitie naar een andere leverancier en de inloggegevens van het ICT-systeem te overhandigen, waaronder de inloggegevens die nodig zijn om zelfstandig nieuwe accounts aan te maken, versleutelde accounts vrij te geven, wachtwoorden te resetten, SAP dashboards uit te lezen en de firewallconfiguratie te beheren.

De IT-leverancier schortte in reactie daarop al zijn verplichtingen op, totdat de ondernemer alle openstaande facturen zou hebben betaald.

Partijen twistten over de vraag of de IT-leverancier onrechtmatig had gehandeld door te weigeren de inloggegevens te verschaffen.[8] Het scheidsgerecht oordeelde dat het belang van de ondernemer bij afgifte om een ongestoorde en zelfstandige bedrijfsvoering te waarborgen zwaarder woog dan het belang van de leverancier bij niet-afgifte als 'pressiemiddel' om betaling van de openstaande facturen te verkrijgen. Voor de ondernemer was immers geen alternatief voorhanden. Door de afgifte van toegangsgegevens en medewerking aan de transitie afhankelijk te maken van volledige betaling van openstaande facturen gebruikte de IT-leverancier naar het oordeel van het scheidsgerecht zijn feitelijke machtspositie als houder van de toegangsgegevens zonder zich de gerechtvaardigde belangen van de ondernemer aan te trekken.

Een verzwaarde zorgplicht rust zeker niet op elke IT-leverancier en hangt sterk af van de omvang van de opdracht: een simpele opdracht versus het algehele IT-beheer. Het eerste was het geval in een zaak voor het gerechtshof Amsterdam (ECLI:NL:GHAMS2020:1987), waarbij het hof op 7 juli 2020 oordeelde dat de IT-leverancier geen vergaande verplichting had om de verhuizing van een advocatenkantoor op IT-gebied in algehele zin voor te bereiden en daarin te begeleiden of te adviseren.[9] Partijen sloten een overeenkomst van opdracht die inhield dat de IT-leverancier de VoIP-telefoonverbinding en ADSL-internetverbinding van het advocatenkantoor zou opzeggen, een computer op een thuis- en kantooradres zou installeren en een VPN-verbinding zou opzetten van de woning naar het kantoor. Het advocatenkantoor gaf daarbij volgens het hof specifieke en duidelijke instructies, maar geen opdracht de verhuizing op ICT-gebied in algehele zin voor te bereiden en daarin (vergaand) te begeleiden of adviseren. Dit vloeide ook niet voort uit de zorgplicht van de IT-leverancier

in de uitvoering van de opdracht, aldus het hof. Dat de IT-leverancier de 'ICT-beheerder' van het advocatenkantoor was, of zelfs dat de relatie tussen partijen meer inhield dan dat de IT-leverancier incidenteel diensten leverde, werd dan ook niet aangenomen. Het enkele feit dat het advocatenkantoor na de uitvoering van de opdracht problemen ondervond, is volgens het hof onvoldoende om te concluderen dat deze problemen werden veroorzaakt door een tekortkoming van de IT-leverancier.

Redelijke verwachtingen deskundige ICT-dienstverlener

Naast de omvang van de opdracht kunnen ook de markt, en de deskundigheid van partijen van invloed zijn op de gerechtvaardigde redelijke verwachtingen, zoals in een zaak voor de rechtbank Amsterdam (ECLI:NL:RBAMS:2019:9635) over een door Smart Connections gebouwd CRM-systeem dat niet aan de verwachtingen van afnemer ALLSAFE voldeed.[10] Onderzoek naar de kwaliteit van het softwaresysteem liet 'goed gedocumenteerde aanhoudende problemen' zien en toonde aan dat het systeem 'zeer slecht bruikbaar is' en 'ernstig tekortschiet'. Dit terwijl de markt voor CRM-systemen[11] als vrij volwassen moest worden beschouwd, wat zich onder meer liet zien in het hoge niveau van bruikbaarheid van de aangeboden systemen. De rechtbank oordeelde op 18 december 2019 (publicatie 4 februari 2020) dat Smart Connections als professionele IT-dienstverlener een CRM-systeem diende op te leveren dat voldeed aan 'de verwachtingen die een gemiddelde klant daaraan mag ontlenen'. Aangezien partijen naast een presentatie geen verdere afspraken op papier hadden gezet, rees de vraag wat ALLSAFE onder de gegeven omstandigheden had mogen verwachten. Volgens de rechtbank mag een klant, zelfs als dit niet met zoveel woorden in de overeenkomst is opgenomen, van een deskundige IT-dienstverlener die daarvoor marktconforme prijzen in rekening brengt, verwachten dat deze een systeem levert waarmee door de gemiddelde werknemer kan worden gewerkt. Daar voegt de rechtbank de (naar onze mening opmerkelijke) kanttekening aan toe dat 'ook als een ISO-norm niet met zoveel woorden is overeengekomen, de klant mag verwachten dat zijn professionele dienstverlener werkt met inachtneming van de normen die binnen de branche gebruikelijk zijn'.[12] Ook achtte de rechtbank het onbegrijpelijk dat de verwachtingen die ALLSAFE had uitgesproken over de 'look and feel' van de interfaces, door Smart Connections werden beschouwd als 'out of scope'. De rechtbank oordeelde dat de overeenkomst rechtmatig was ontbonden.

Uit een uitspraak van het gerechtshof Arnhem-Leeuwarden van 7 april 2020 (gepubliceerd via IT&R 3138 op 15 mei 2020) blijkt dat niet in alle gevallen de verwachtingen van de (meest) deskundige partij/IT-dienstverlener redelijke verwachtingen zijn.[13] In deze zaak stond centraal dat de opdrachtgever (tevens IT-dienstverlener) Ordina de overeenkomst voor de aanschaf van recruitmentsoftware zonder ingebrekestelling had ontbonden, omdat de kwaliteit van de programmatuur naar de mening van Ordina dermate slecht was dat zij er van uit mocht gaan dat de leverancier OTYS zijn verplichtingen onder de overeenkomst niet meer kon nakomen. Dat de software van zodanig slechte kwaliteit was dat deze ook na aanpassing niet aan de overeengekomen garanties zou kunnen voldoen en Ordina daarom redelijkerwijs kon voorzien dat niet kon worden nagekomen, achtte het hof onvoldoende onderbouwd. Ordina stelde dat OTYS als 'meest deskundige partij' haar zorgplicht had geschonden door Ordina niet tijdig te waarschuwen dat het eindproduct niet slechts uit standaardsoftware zou bestaan die zonder veel aanpassingen als het ware 'plug and play' in gebruik genomen kon worden. Het hof oordeelde echter dat Ordina als IT-dienstverlener niet de redelijke verwachting had mogen hebben dat de software grotendeels standaard zou zijn en wees daarmee het beroep op de zorgplicht af.

Verantwoordelijkheid afnemer op basis van eigen deskundigheid

In een geschil tussen Blue Ocean en een IT-dienstverlener ter ontwikkeling en exploitatie van een *human resource management*-applicatie was de hamvraag of de IT-dienstverlener zich voldoende had ingespannen. De IT-dienstverlener verzorgde het design, de architectuur en de ontwikkeling van de applicatie. Blue Ocean was verantwoordelijk voor verkoop, marketing, testen en implementeren van de applicatie. Na verscheidene mislukte implementaties bij verschillende klanten was voor Blue Ocean de maat vol. Zij stelde de IT-dienstverlener in gebreke en stelde daarbij dat de IT-dienstverlener niet aan zijn informatie- of waarschuwingsplicht had voldaan. Het gerechtshof Amsterdam oordeelde op 14 juli 2020 (ECLI:NL:GHAMS:2020:2016) dat uit de enkele omstandigheid dat de IT-dienstverlener verantwoordelijk is voor het design, niet kan worden afgeleid dat hij is tekortgeschoten in de nakoming van zijn inspanningsverbintenis, als blijkt dat er verschillen zijn tussen het design en het gebruik door de eindgebruikers. Dit gold te meer nu Blue Ocean geen deugdelijke acceptatietests had laten uitvoeren alvorens de applicatie aan eindgebruikers te presenteren; dit was tenslotte de verantwoordelijkheid van Blue Ocean. Het feit dat Blue Ocean een Excel-bestand had verstrekt met punten waarop de module niet overeenkomstig de specificaties functioneerde, ontsloeg Blue Ocean niet van haar contractuele verantwoordelijkheid de applicatie te testen alvorens bij eindgebruikers in gebruik te geven.[14]

Verder oordeelde het hof dat de IT-dienstverlener ervan uit mocht gaan dat Blue Ocean de deskundigheid en

capaciteit bezat om acceptatietesten van voldoende diepgang en omvang uit te voeren. Hierbij speelde mee dat in het handelsregister de activiteiten van Blue Ocean stonden omschreven als (onder meer) het ontwikkelen van diverse soorten software.

Rol van afhankelijkheid bij zorgplicht

In een zaak voor de rechtbank Amsterdam (ECLI:NL:RBAMS:2020:4059, 18 augustus 2020) stond de zorgplicht bij opzegging van de overeenkomst ter discussie.[15] PRLG exploiteerde onder een licentieovereenkomst softwareproducten ten behoeve van lokale overheden, waarvoor zij aan leverancier Uniface een licentievergoeding per inwoner betaalde. Nadat Uniface op haar mededeling dat zij de tarieven wilde herijken geen bevredigende reactie ontving, besloot Uniface de overeenkomst conform de opzegregeling te beëindigen. Volgens PRLG waren de gevolgen van de opzegging voor PRLG en tenminste honderd gemeenten echter onevenredig groot en maakte Uniface misbruik van het feit dat er technische afhankelijkheid bestond van hun software. De rechtbank meende dat de opzegging geen verband hield met een (beweerde) gebrekkige uitvoering van de overeenkomst, en in plaats daarvan geen ander doel diende dan 'het louter over de brug laten komen van PRLG met een hogere vergoeding'. De rechtbank oordeelde daarom dat, ondanks het bestaan van een opzegregeling, de eisen van redelijkheid en billijkheid in de weg stonden aan de opzegging. De bijzondere zorgplicht die Uniface als IT-leverancier had jegens PRLG en de betrokken derden – die een groot maatschappelijk belang hebben om hun wettelijke taken op een correcte en efficiënte wijze uit te (kunnen blijven) voeren – bracht mee dat Uniface niet zonder meer een beroep mocht doen op de opzegregeling. De zorgvuldigheidsverplichting van Uniface reikte naar het oordeel van de rechtbank verder dan de door Uniface aangedragen omstandigheden dat schermen niet 'op zwart springen' of dat gemeenten een rechtstreekse licentie (tegen het door Uniface te bepalen tarief) konden afnemen.
Een sterke afhankelijkheid kan verzwarend wegen als het op de zorgplicht aankomt, zo blijkt ook uit een uitspraak van de rechtbank Den Haag van 3 juni 2020 (ECLI:NL:RBDHA:2020:4735).[16] Centraal hierin stond een misgelopen automatiseringsproject bij de gemeente Leeuwarden. In de kern was in geschil of dit mislopen het gevolg was van tekortschietende prestaties van de kant van softwareontwikkelaar en adviseur Split˜Vision, met betrekking tot de tijdigheid, de volledigheid en de kwaliteit van de door haar geleverde inspanningen en resultaten, en of de gemeente Leeuwarden daarom gerechtigd was de betaling van gebruiksvergoedingen aan Split˜Vision te staken en de overeenkomst te ontbinden. Naar het oordeel van de rechtbank had de gemeente Leeuwarden voldoende onderbouwd dat gebreken in de software van Split˜Vision een aanwijsbare oorzaak vormden voor de te trage performance. Maar ook voor de stelling van Split˜Vision dat ontoereikende IT-infrastructuur aan de zijde van de gemeente Leeuwarden in de weg stond aan het verbeteren van de performance, vond de rechtbank aanknopingspunten. Desondanks oordeelde de rechtbank dat Split˜Vision tekort was geschoten. Dat de IT-infrastructuur mede de oorzaak was voor de te trage performance van het PDW-platform liet onverlet dat sprake was van tekortschietende kwaliteit van de software van Split˜Vision.
De op Split˜Vision rustende zorgplicht bracht mee dat Split˜Vision in haar rol als IT-leverancier gedurende het project ook de belangen van gemeente Leeuwarden voor ogen had moeten houden en haar adequaat en inzichtelijk had moeten informeren over de risico's voor het succes van het project.

SOFTWAREONTWIKKELING/ UITLEG/DESKUNDIGEN

Dealerafhankelijkheid voor afnemers

In een geschil tussen SW Solutions en De Vries Trappen (DVT) oordeelde het gerechtshof Arnhem-Leeuwarden op 12 mei 2020 (ECLI:NL:GHARL:2020:3683) over wat partijen hadden bedoeld met 'dealerafhankelijkheid'.[17] SW Solutions leverde en implementeerde op grond van een overeenkomst een softwarepakket bij DVT. Essentieel voor DVT was dat afwijkingen van de standaard zodanig geconfigureerd zouden zijn dat updates zonder complicatie konden plaatsvinden en dat afhankelijkheid ten opzichte van individuele SAP-dealers werd verminderd door juiste configuratie en documentatie van wisselwerkingen. Na de levering van het softwarepakket ontbond DVT de overeenkomst omdat sprake zou zijn van veel maatwerk door SW Solutions, terwijl partijen juist hadden afgesproken dat standaardapplicaties gebruikt zouden worden om een afhankelijkheidsrelatie met de leverancier te voorkomen.
Het hof volgde de uitleg van de rechtbank dat SW Solutions de opdracht had aangenomen om voor DVT een softwaresysteem te ontwikkelen en implementeren waarmee DVT 'niet (te veel) afhankelijk is van een individuele SAP-dealer' en dus relatief gemakkelijk kon overstappen naar een andere SAP-dealer. Deze afspraak bracht volgens het hof niet mee dat SW Solutions alleen een standaardpakket mocht leveren en geen maatwerk had mogen toepassen.
Voorts kwam uit verklaringen van verschillende SAP-dealers naar voren dat zij het door SW Solutions ontwikkelde softwaresysteem konden overnemen en dat er geen systeemtechnische beperking was om naar een andere SAP-dealer over te gaan voor het in werking houden van het systeem. Potentieel hoge kosten die andere SAP-dealers in rekening konden brengen voor updates van het maatwerk van SW Solutions, creëer-

den ook niet de gevreesde afhankelijkheid, zo concludeerde het hof.

Blijvende onmogelijkheid tot herstel software

Het gerechtshof Amsterdam boog zich over een geschil tussen de exploitant Equihold en ontwikkelaar Capgemini over de kwaliteit van de door Capgemini ontwikkelde softwareapplicatie (ECLI:NL:GHAMS:2020:2749, vonnis gepubliceerd op 20 oktober 2020).[18] In het kader van de te ontwikkelen sportapplicatie '1-2 Focus' zou de eindverantwoordelijkheid voor de functionaliteit van het softwarepakket bij Equihold liggen en was Capgemini verantwoordelijk voor de kwaliteit van de te ontwikkelen software. In de aanvullende overeenkomst werd afgesproken dat 'high quality software' zou worden geleverd, die uit verschillende lagen moest bestaan, en gemakkelijk te onderhouden, aan te passen en uit te breiden naar andere sporten moest zijn.
Uit de door en namens Equihold uitgevoerde onderzoeken bleek dat de aanvullende afspraken door Capgemini niet waren waargemaakt en dat de kwaliteit van de software ver beneden peil was en zelfs volledig herschreven zou moeten worden. Capgemini stelde echter dat Equihold al jaren bekend was met de door haar gestelde fundamentele gebreken in de broncode, maar niet tijdig geklaagd had. Equihold beschikte over de broncode, voerde codereviews uit en had ook de expertise daartoe in huis, aldus Capgemini. Het hof gaat niet mee in dit verweer. Equihold had wel degelijk tijdig geklaagd, en een eerder onderzoek naar de kwaliteit door Equihold had ook niet van hem verlangd mogen worden terwijl Capgemini zelf ook in de gelegenheid was onderzoek te verrichten, en daar ook aanleiding toe had op grond van het tijdige klagen van Equihold.
Op basis van de gebrekkige kwaliteit had Equihold de overeenkomst zonder ingebrekestelling ontbonden en gesteld dat als de software na jaren pas in de overeengekomen vorm werd geleverd, de software door verloop van jaren technisch en functioneel verouderd was en nakoming daarmee zinloos zou zijn. Het hof benoemde een onafhankelijke deskundige om te onderzoeken of dit inderdaad zou leiden tot blijvende onmogelijkheid tot nakoming, waarmee de verzuimregels buiten toepassing bleven.

Onrechtmatig buiten bereik plaatsen van software

Het kopiëren van software en deze buiten de macht brengen van de leverancier was onrechtmatig, maar had desalniettemin niet tot schade geleden, zo oordeelde de rechtbank Gelderland op 28 februari 2020 (ECLI:NL:RBGEL:2020:1345).[19] Haerst, een onderneming die zich richt op videotechnologie en diagnostiek, was een samenwerking aangegaan met het jonge IT-bedrijf Lizard Apps voor de ontwikkeling van een diagnostische camera voor toepassing in de psychiatrie. De software voor de camera werd door Lizard Apps ontwikkeld en opgeleverd en de camera werd door verschillende gebruikers ingezet. Voor de ontwikkeling van de 2.0-versie van de camera werd door Lizard Apps in opdracht van Haerst de oude software werkend gemaakt voor de nieuwe hardware met gezichtsherkenning. Tijdens deze fase ontstonden

samenwerkingsproblemen waarna Haerst de samenwerking had opgezegd. Haerst kopieerde vervolgens de software voor de camera, die haar via een server van Lizard Apps ter beschikking was gesteld, naar een andere server en bracht deze buiten het bereik van Lizard Apps.[20]
De rechtbank toonde begrip voor het verweer van Haerst dat zij ervoor wilde zorgen dat zij de diagnostische camera – die alleen kon draaien op de software van Lizard Apps – kon blijven gebruiken, terwijl zij intussen een andere leverancier zocht. Dat nam niet weg dat Haerst onrechtmatig had gehandeld door Lizard Apps de toegang tot haar eigen software te ontzeggen, aldus de rechtbank. Dat Lizard Apps als gevolg van het buiten haar macht brengen van de software door Haerst meer of andere schade heeft geleden dan de niet-betaalde licentievergoeding over het voortgezette gebruik, achtte de rechtbank echter niet aannemelijk.

Agile versus Prince2 projectmethodiek

In een zaak voor het gerechtshof Amsterdam (ECLI:NL:GHAMS:2020:46, 14 januari 2020) werd duidelijk hoe belangrijk overeenstemming over de te hanteren projectmethodiek kan zijn. De samenwerking tussen leverancier Vancis en afnemer Horizon College voor implementatie en beheer van een IT-infrastructuur was al in een vroeg stadium vastgelopen, omdat partijen twistten over de vraag of Vancis tijdig een gedetailleerd genoeg project- en testplan had opgeleverd. Vancis stelde dat zij voor het sluiten van de overeenkomst meermaals had aangegeven dat zij een agile werkwijze[21] hanteerde, en dat Horizon College deze werkwijze na het sluiten van de overeenkomst ook had geaccepteerd. Als gevolg hiervan, aldus Vancis, dienden de eisen in de overeenkomst over de mate van detaillering van het project- en testplan in overeenstemming met die werkwijze te worden uitgelegd, en was Vancis niet tekortgeschoten door een plan op te leveren dat slechts de strikt noodzakelijke informatie bevatte.[22]
De stelling van Vancis dat een gedetailleerd projectplan niet mogelijk is bij toepassing van agile methodiek is begrijpelijk. Bij toepassing van een agile werkwijze passen partijen hun project na de afronding van *sprints* gaandeweg aan. Toch oordeelde het hof dat Vancis geen plan had ingediend dat voldeed aan de eisen die de overeenkomst stelde. Horizon College had immers tijdens de aanbestedingsprocedure ondubbelzinnig afwijzend gereageerd op de vraag of het projectplan op een andere werkwijze dan Prince2[23] mocht worden uitgevoerd. Ook na sluiting van de overeenkomst mocht Vancis er niet van uitgaan dat Horizon College had ingestemd met afwijking van de daarin genoemde eisen over een gedetailleerd projectplan. Door onterecht uit te gaan van toepassing van een agile werkwijze was Vancis wel degelijk tekortgeschoten.[24]

TOEPASSING FRAANJE/ALUKON-ARREST

Ingebrekestelling na lange vertraging

In de vorige Kroniek deden we uitgebreid verslag over het (niet IT-specifieke) Hoge Raad arrest-Fraanje/Alukon.[25] Ook in 2020 bleek dit arrest van belang voor de IT-rechtspraktijk. In een zaak voor het gerechtshof Den Haag (ECLI:NL:GHDHA:2020:1273, 14 juli 2020) hadden partijen tweemaal de 'go live'-datum verschoven zonder dat de afnemer zich op het standpunt had gesteld dat de leverancier in verzuim was, althans zonder op dit punt zijn rechten voor te behouden. Nadat de leverancier vervolgens had toegezegd de cruciale kwesties binnen veertien dagen op te lossen, schreef de afnemer niet lang daarna: 'Als aangegeven wordt de tijd inmiddels heel krap. Vanaf augustus hebben we toezeggingen gekregen dat alle rapporten klaar zouden zijn en elke keer worden deadlines niet gehaald en verschoven. Ik ga ervanuit dat bovenstaande zaken deze week eindelijk opgelost worden zodat we kunnen focussen op andere openstaande punten.' Het hof oordeelde in lijn met het arrest-Fraanje/Alukon dat deze mededeling als voldoende ingebrekestelling kwalificeerde, althans dat van de leverancier verwacht had mogen worden dat deze binnen de genoemde week zou reageren, wat zij niet deed.[26]

EXIT/TRANSITIE

Het belang van transitieafspraken

Hoe snel een geschil tussen partijen over de transitie van IT-beheer naar een nieuwe leverancier kan escaleren, bleek in een zaak voor de rechtbank Midden-Nederland van 29 juli 2020 (ECLI:NL:RBMNE:2020:3239).[27]
Na opzegging door de afnemer van een beheersovereenkomst met haar leverancier, weigerde de leverancier de configuratiegegevens van een firewall, die zij op de router in het bedrijfspand van de afnemer had geïnstalleerd, aan de afnemer over te dragen omdat zij een gedeelte van de gegevens als vertrouwelijk beschouwde. Vervolgens merkte de leverancier in de week voor de beëindiging van de dienstverlening dat iemand zich toegang had verschaft tot de firewall en de router. Later bleek dat de systeembeheerder van de afnemer de router had uitgezet om de configuratiegegevens van de firewall te kopiëren. Hiervan was de leverancier niet op de hoogte gebracht. Hij vermoedde een 'hack' en startte daarom zoals verplicht onder de overeenkomst een onderzoek. De afnemer spande hierna een zaak aan tegen de leverancier, omdat de leverancier tijdens dit onderzoek de volledige inhoud van de mailbox van de systeembeheerder zou hebben gekopieerd. Volgens de afnemer kwalificeerde dit als een schending van de overeengekomen vertrouwe-

lijkheidsbepaling, met als gevolg dat leverancier een contractuele boete van EUR 100.000 en een schadevergoeding zou moeten betalen. Uiteindelijk wees de rechtbank de eis af, omdat de afnemer onvoldoende aan haar stelplicht had voldaan. Deze uitkomst daargelaten, onderstreept het verloop van dit geschil vooral het belang van het opstellen van een toereikende exitstrategie bij IT-outsourcingsovereenkomsten. Als partijen tevoren werkbare transitieafspraken hadden gemaakt, had de 'hack' in de laatste week van de dienstverlening vermoedelijk niet tot zo een hoogoplopend geschil geleid.

ONVOORZIENE OMSTANDIGHEDEN

De drempel voor het ontbinden van een overeenkomst of het wijzigen van de gevolgen ervan op grond van onvoorziene omstandigheden ligt over het algemeen hoog. Artikel 6:258 BW biedt immers slechts een grondslag hiervoor indien de wederpartij naar maatstaven van redelijkheid en billijkheid ongewijzigde instandhouding van de overeenkomst niet mag verwachten. De COVID-19-crisis heeft hierin wel wat wijzigingen gebracht, nu de rechtbanken in 2020 een beroep op onvoorziene omstandigheden wat vaker dan anders hebben toegewezen.[28] Voor zover ons bekend heeft zich binnen het IT-recht echter nog geen zaak voorgedaan waarbij COVID-19 een doorslaggevende rol speelde.

Wel ontbond de rechtbank Den Haag (ECLI:NL:RBDHA:2020:3847) op 22 april 2020 een overeenkomst betreffende toekomstige betalingstermijnen in een geschil tussen leverancier MIC en afnemer Vrouwenpoli Boxmeer. Partijen waren het er over eens dat het door MIC geleverde softwaresysteem 'performanceproblemen' kende. Hoewel niet vast kwam te staan dat MIC hier enig verwijt in trof, moest de Vrouwenpoli bij voortzetting van de overeenkomst hoge onvoorziene kosten maken en ontbrak enig vertrouwen van de medewerkers van de Vrouwenpoli in het softwaresysteem. Ter zitting gaven beide partijen aan geen vertrouwen te hebben in een 'conflictloze voortzetting van de overeenkomst', waarbij MIC ook meldde dat de Vrouwenpoli slechts een kleine klant voor haar was, terwijl een goede werking van de software (ondanks dat deze conform de overeenkomst geleverd was) voor de Vrouwenpoli juist essentieel was. De rechtbank oordeelde in dit licht dat de belangen van Vrouwenpoli bij ontbinding van de overeenkomst zwaarder wogen dan de belangen van MIC bij de voortzetting ervan.[29]

ELEKTRONISCHE HANDTEKENINGEN

Invulling van het betrouwbaarheidsvereiste

Wat betreft de elektronische handtekeningen is noemenswaardig dat de rechtbank Zeeland-West-Brabant (ECLI:NL:RBZWB:2020:4817) op 7 oktober 2020 de eerste concrete handvatten heeft geboden voor de invulling van de betrouwbaarheidseis uit artikel 3:15a BW.[30] Ingevolge dit artikel hebben ook andere dan gekwalificeerde elektronische handtekeningen dezelfde rechtsgevolgen als een natte handtekening indien de gebruikte methode voor ondertekening voldoende betrouwbaar is. De wet noemt al als relevante omstandigheid het doel waarvoor de handtekening is gebruikt. De rechtbank voegt daar de aard van de overeenkomst en de manier van totstandkoming van de overeenkomst en de handtekening aan toe.[31]

In casu ging het om de ondertekening middels Adobe Sign van een overeenkomst van borgtocht die Swishfund had opgesteld. Het verificatieproces dat Swishfund vóór ondertekening gebruikte om de identiteit van haar

klant te identificeren, zag echter vooral op de contracterende onderneming en in mindere mate op de vertegenwoordigingsbevoegdheid van de ondertekenende bestuurder. Het enige direct aan de bestuurder te relateren document waarover Swishfund beschikte, was een kopie van zijn identiteitsbewijs. Dit terwijl vaststond dat er voorafgaand aan het sluiten van de overeenkomst op geen enkel moment direct persoonlijk contact was geweest tussen Swishfund en de bestuurder, ook al hadden partijen nog niet eerder zaken met elkaar gedaan. Hoewel volgens de rechtbank geen enkele ondertekeningsmethode bestand is tegen misbruik, riskeerde Swishfund misbruik door personen die beschikking hadden over de e-mailadressen en bankgegevens van een vennootschap en over persoonsgegevens van haar bestuurders. Gelet daarop, en gezien het doel van het aangaan van de overeenkomst (te weten: de borgstelling voor een geldlening tot een aanzienlijk bedrag), kon de 'gewone' elektronische handtekening niet als voldoende betrouwbaar worden aangemerkt.[32]

NOTEN

1 Schenk, W. 'Hoe succesvol is de corona-app?' 30 december 2020, *Trouw*. Beschikbaar via https://www.trouw.nl/binnenland/hoe-succesvol-is-de-corona-app~bbe88a94/.
2 Modderkolk, H. 'Nieuws over het coronavirus? Pas op voor valse berichten en malware'. 15 maart 2020, *de Volkskrant*. Beschikbaar via https://www.volkskrant.nl/nieuws-achtergrond/nieuws-over-het-coronavirus-pas-op-voor-valse-berichten-en-malware~bd18d08b/.
3 *Ransomware*, ook wel gijzelsoftware genoemd, is een middel dat gebruikt wordt om via internet in te breken en gegevens te stelen of te gijzelen. Letterlijk vertaald betekent *ransom*: losgeld. De geblokkeerde gegevens worden tegen betaling (vaak in de vorm van bitcoins) weer vrijgegeven.
4 *Distributed Denial of Service* aanvallen zijn pogingen om een computer, computernetwerk of dienst on- of moelijk bereikbaar te maken door meerdere computers tegelijk een aanval op een doelwit te laten uitvoeren.
5 Interpol: *Cybercrime: COVID-19 Impact*. 4 August 2020. Beschikbaar via https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.
6 IT-overeenkomsten kwalificeren in het algemeen als overeenkomst van opdracht ex art. 7:400 BW.
7 r.o. 4.1, 4.4 - 4.5, (*O'Cliance/gedaagde*).
8 r.o. 39 (*verschaffing inloggegevens*).
9 r.o. 3.5 - 3.7 (*verhuizing op ICT-gebied*).
10 r.o. 4.5-4.6 *(Smart Connections/ALLSAFE).*
11 Een Customer Relations Management (CRM) softwaresysteem is een softwarepakket dat onder andere voorziet in de communicatie tussen bedrijven en hun klanten, maar daarnaast ook in de analyse van klantgegevens en het effect van marketingactiviteiten.
12 Een ISO-norm dient in de praktijk als waarborg en fungeert als een erkende en hoge norm voor kwaliteit van (onderdelen van) de dienstverlening. Dit is in onze optiek niet gelijk te trekken met een in de branche geldende 'algemene norm'. Dat de Rechtbank Amsterdam heeft geoordeeld dat afnemers de ISO-norm als standaardnorm van de dienstverlening mogen verwachten, ook in het geval deze niet met zoveel woorden is overeengekomen, gaat wat ons betreft dan ook té ver.
13 r.o. 3.8 (*OTYS/Ordina*).
14 r.o. 3.9, 3.18, 3.22, 3.24 (*Blue Ocean/[X] Software*).
15 r.o. 4.5 (*PRLG/Uniface*).
16 r.o. 4.2, 4.19-4.21 (*Split~Vision/Gemeente Leeuwarden*).
17 r.o. 5.4-5.7, 5.14-5.17 (*SW Solutions/De Vries Trappen*).
18 r.o. 3.9, 3.11, 3.14-3.17 (*Equihold/Capgemini*).
19 r.o. 4.1, 4.5, 4.9, 4.12 (*Lizard Apps/Haerst*).
20 De vraag of het Haerst onder gegeven omstandigheden moet worden toegestaan de software te blijven gebruiken totdat zij vervangende software kan laten ontwikkelen, is onderwerp van een nog lopende procedure. Vonnis is kort geding - Rechtbank Gelderland 7 november 2017, ECLI:NL:RBGEL:2017:5705 (*Lizard Apps/Haerst*).
21 Deze in de IT-sector veelvoorkomende werkwijze houdt in dat de afnemer bij het sluiten van de overeenkomst geen concreet eindresultaat voorschrijft, maar dat de leverancier samen met de afnemer gedurende de ontwikkeling wensen opstelt en waar nodig aanpast. De leverancier levert daarbij gefaseerd met behulp van sprints en tussentijdse tests de software op.
22 r.o. 3.4 en 3.4.2 (*Vancis/Horizon College*).
23 Prince2 is een acroniem voor 'Projects in Controlled Environments, version 2'. Een belangrijk verschil met de agilemethodiek is dat Prince2 een voorspellende (planmatige) aanpak is, terwijl Agile zich kenmerkt door incrementele ontwikkelingen op de korte termijn, los van enig overkoepelend plan.
24 r.o. 3.4.3-3.4.5 (*Vancis/Horizon College*).
25 Hoge Raad 11 oktober 2019, ECLI:NL:HR:2019:1581, r.o. 3.2.2 (*Fraanje/Alukon*).
26 r.o. 9-14 (*Interport/Groeneveld).*
27 r.o. 2.4, 3.3-3.6 (*eiseres/gedaagde*).
28 Dat lag anders in bijvoorbeeld het huurrecht, waar COVID-19 regelmatig tot wijziging van huurovereenkomsten leidde. Zie Jacobs, N. en Ter Meer, L. *Huurrecht en beroep op onvoorziene omstandigheden wegens Covid-19.* 28 januari 2021, Kennedy Van der Laan. Beschikbaar via https://kvdl.com/artikelen/huurrecht-en-beroep-op-onvoorziene-omstandigheden-vanwege-covid-19.
29 r.o. 4.42-4.47 (*Medned Information Consultancy/Vrouwenpoli Boxmeer*).
30 In de IT-Kroniek over 2017-2018 verwezen we al naar Rechtbank Den Haag 8 mei 2018, ECLI:NL:RBDHA:2018:6370 (*Van Gansewinkel/gedaagde*). Die zaak leverde echter geen concrete handvatten op omdat er meer onregelmatigheden dan alleen de geldigheid van de handtekening een rol speelden.
31 r.o. 4.4 (*eiser/Swishfund Nederland*).
32 r.o. 4.5-4.8 (*eiser/Swishfund Nederland*).