Vzgr Rb Amsterdam, 16 juli 2018, Kaspersky v TMG

PUBLICATIE

Nieuwsbericht Telegraaf waarin wordt geclaimd dat cybersecuritybedrijf Kaspersky is gehackt onrechtmatig:

- **Gebruik gemaakt van anonieme bronnen, waarvan betrouwbaarheid en geloofwaardigheid niet kan worden getoetst**
- **Iedere aanwijzing ontbreekt dat op computernetwerk Kaspersky is ingebroken**
- **TMG heeft verwijtbaar nagelaten maatregelen te treffen om uitlatingen [naam 1] controleerbaar maken**

Geconstateerd kan worden dat de journalisten niet controleerbaar hebben gemaakt wat [naam 1] tegenover hen heeft verklaard terwijl dit gemakkelijk had gekund. Zo wordt niet duidelijk waarom [naam journalis 1] geen aantekeningen of audio-opname kon maken. Het gesprek stond immers op de speaker. Dit geldt temeer omdat [naam journalis 1] wel van het keukentafelgesprek een audio-opname heeft gemaakt. Er zijn bovendien telefoon-apps waarmee gemakkelijk een telefoongesprek kan worden opgenomen terwijl met diezelfde telefoon een gesprek wordt gevoerd.

- **aan betrouwbaarheid doet af dat verklaringen journalisten op onderdelen niet op elkaar lijken te passen**
- **geen audio-opname van keukentafelgesprek met [naam 1] overgelegd**

Daarbij komt dat de audio-opname van het keukentafelgesprek niet is overgelegd. Dit is opmerkelijk omdat daarmee afbreuk aan de geloofwaardigheid van [naam 1] had kunnen worden gedaan.

- **geen verder onderzoek gedaan door TMG naar inbraak en geen mogelijkheid tot weerwoord gegeven**

Verweer dat artikel een niet serieus te nemen inhoud heeft en aldus Kaspersky geen schade kan hebben berokkend niet gevolgd

- **mede gelet op de details die over het binnendringen in het computernetwerk worden verteld zorgt verhaal dat uit mond [naam 1] is opgetekend ervoor dat lezer de indruk krijgt dat inbraak echt heeft plaatsgevonden**

Het verhaal over de inbraak in het computernetwerk dat uit de mond van [naam 1] is opgetekend neemt een prominente plaats in de publicatie in. Mede gelet op de details die over het binnendringen in het computernetwerk worden verteld kan dit de lezer de indruk geven dat de inbraak echt heeft plaatsgevonden.

- **berichtgeving kan (potentiële) klanten afschrikken**

Dat Kaspersky hierdoor schade heeft geleden en mogelijk nog zal lijden is voldoende aannemelijk. De berichtgeving kan (potentiële) klanten afschrikken. Een cybersecuritybedrijf dat haar eigen internetveiligheid niet in orde heeft levert commercieel zeer nadelige beeldvorming op. Al met al is de publicatie in De Telegraaf voorshands onrechtmatig tegenover Kaspersky.

Vindplaatsen: **ECLI**

Vzgr Rb Amsterdam, 16 juli 2018
(M.W. van der Veen)
Vonnis
RECHTBANK AMSTERDAM
Afdeling privaatrecht, voorzieningenrechter civiel
zaaknummer / rolnummer: C/13/648511 / KG ZA 18-512 MV/TF
Vonnis in kort geding van 16 juli 2018
in de zaak van
de besloten vennootschap met beperkte aansprakelijkheid
KASPERSKY LAB B.V.,
gevestigd te Utrecht,
eiseres in conventie bij dagvaarding van 15 juni 2018,
verweerster in reconventie,
advocaat mr. O.G. Trojan te 's-Gravenhage,
tegen
1. de besloten vennootschap met beperkte aansprakelijkheid
TMG LANDELIJKE MEDIA B.V.,
gevestigd te Amsterdam,
gedaagde in conventie,
advocaat mr. R.S. Le Poole te Haarlem.
2. [gedaagde 2]
[gedaagde 2] ,
wonende te [woonplaats] ,
gedaagde in conventie,
eiser in reconventie,
advocaat mr. Chr. Alberdingk Thijm te Amsterdam.
Partijen zullen hierna Kaspersky (Lab), TMG en [gedaagde 2] worden genoemd.

1 De procedure

Ter zitting van 2 juli 2018 heeft Kaspersky gesteld en gevorderd overeenkomstig de in kopie aan dit vonnis gehechte dagvaarding. TMG en [gedaagde 2] hebben verweer gevoerd met conclusie tot weigering van de gevraagde voorzieningen, en vervolgens heeft [gedaagde 2] in reconventie gevorderd overeenkomstig de in kopie aan dit vonnis gehechte akte. Kaspersky heeft de vordering in reconventie bestreden. Alle partijen hebben producties en een pleitnota in het geding gebracht. Na verder debat hebben partijen verzocht vonnis te wijzen.
Ter zitting waren voor zover van belang aanwezig:
aan de zijde van Kaspersky: [naam general manager] (general manager), [naam 1] (ter zitting als informant gehoord, hierna [naam 1]) en mr. Trojan,
aan de zijde van TMG: [naam journalis 1] en [naam journalist 2] (beiden journalist van De Telegraaf en ter zitting als informant gehoord), [naam secretaris

hoofdredactie] (secretaris hoofdredactie) en mr. Le Poole en zijn kantoorgenoot mr. G. Nühn,
aan de zijde van [gedaagde 2] : mr. Alberdingk Thijm met een kantoorgenoot.
Na de zitting heeft Kaspersky, zoals ter zitting besproken, een DVD met telefoongesprekken (die voorafgaand aan de zitting al op Cd-rom waren aangeleverd) aan de voorzieningenrechter doen toekomen.

2 De feiten

in conventie en in reconventie

2.1. Kaspersky is een in Utrecht gevestigd Russisch cybersecuritybedrijf dat zich toelegt op de verkoop van softwarepakketten die beschermen tegen computervirussen en andere vormen van cybercrime. Kaspersky maakt deel uit van een internationaal concern met kantoren in 30 landen. De holding is gevestigd in Londen.

2.2. TMG is uitgever van dagblad De Telegraaf. [naam journalis 1] en [naam journalist 2] zijn als journalist aan De Telegraaf verbonden.

2.3. [gedaagde 2] , voormalig staatssecretaris en minister, schrijft sinds 2002 een column in De Telegraaf over financieel-economische actualiteiten. In december 2017 bracht hij samen met [naam 1] het boek “Cybersecurity en Cybercrime” uit.

2.4. [naam 1] is bij het publiek bekend geworden door haar optreden op 29 januari 2018 in Nieuwsuur. Daarin trad zij op als expert cyberveiligheid. Zij sprak over de DDOS-aanvallen waarmee Nederlandse banken kort voordien waren geconfronteerd. Haar uitlatingen bevatten volgens IT-deskundigen onjuistheden hetgeen voor Nieuwsuur aanleiding was aan haar kijkers excuus aan te bieden. Het boek van [naam 1] en [gedaagde 2] is kort daarna uit de handel genomen vanwege beschuldigingen van plagiaat.

2.5. Op 2 februari 2018 heeft [naam journalis 1] [naam 1] overdag persoonlijk in haar woning gesproken. In de avond hebben [naam journalis 1] en [naam journalist 2] drie telefoongesprekken met [naam 1] gevoerd. In het laatste telefoongesprek hebben de journalisten aan [naam 1] voorgelegd dat zij Kaspersky zou hebben gehackt.

2.6. Op 3 februari 2018 heeft De Telegraaf op haar website www.telegraaf.nl en op pagina 6 van de (papieren) zaterdageditie van de krant een artikel van [naam journalis 1] en [naam journalist 2] geplaatst met als titel: “*Meesterspionne of misleidster? Welkom in de wondere wereld van hacker [naam 1] ”* De publicatie betreft een verslag van de op 2 februari 2018 gevoerde gesprekken met [naam 1] . In de publicatie staat voor zover van belang het volgende:

(..) ‘Cybercrime-expert’ [naam 1] was deze week na een optreden in Nieuwsuur opeens het lachertje van de digitale wereld. Maar ze slaat terug: naar eigen zeggen is ze bezig met een ultrageheime operatie waarmee ze een Nederlands kamerlid gaat ontmaskeren als spion voor de Russen. Het is kerstavond 2017 als [naam 1] stilletjes langs het Utrechtse kantoor loopt van een wereldberoemd Russisch softwarebeveiligingsbedrijf. Ze heeft een opdracht: ze moet het computernetwerk binnendringen om informatie te stelen. Digitaal inbreken bij een softwarebeveiligingsbedrijf, er zijn makkelijkere opdrachten te bedenken. Maar voor [naam 1] is dat geen probleem. “De zwakke plek zit in de wifi, zelfs bij dit type bedrijven”, zegt ze. “ Vandaar dat ik ernaartoe ben gereden. “Die kerstavond bestaat haar ‘buit’ onder meer uit veertig IP-adressen, aangetroffen op het gekraakte computernetwerk van het bedrijf waarvan het hoofdkantoor in Moskou staat. [naam 1] stuurt ze door naar een ‘deep throat’ bij een Amerikaanse veiligheidsdienst. Bijna per kerende post krijgt ze bericht dat ze beet heeft: er zit een lek in de Tweede Kamer dat samenwerkt met de Russen! Om wie het gaat, mag ze nog niet bekendmaken: ze heeft op verzoek van de betrokken veiligheidsdiensten ‘een NDA’ ondertekend, ofwel een geheimhoudingsverklaring. We moeten geduld hebben, op termijn zal alles duidelijk worden, verzekert ze. Welkom in de wondere wereld van de 48- jarige [naam 1] uit (..) (hierna volgt een uiteenzetting over wie [naam 1] is en wordt het onder 2.3 genoemde boek en het onder 2.4 genoemde optreden in Nieuwsuur beschreven, VZR) Maar wie is dan deze [naam 1] ? We zoeken haar thuis op. (..) Zij verontschuldigt zich voor het lange wachten. “Ik heb weinig ervaring met de media. [gedaagde 2] , VZR) had me verboden om de pers te woord te staan”, zegt ze (..) Aan de keukentafel doet zij haar levensverhaal. (..) [naam 1] onderbreekt het gesprek aan de keukentafel meermalen om te bellen met haar contacten die stuk voor stuk bevestigen dat zij een zeer bedreven hacker is. (..)

Haat en nijd

Ze grijnst als ze praat over concurrerende hackers en tech-journalisten die haar deskundigheid de afgelopen dagen in twijfel trokken en daarbij verwezen naar een YouTube-filmpje uit 2012 waarop zij in verleidelijke poses te zien is als fotomodel in een exclusief hotel in Dubai. (daarvan is na de 1e alinea van de publicatie een afbeelding geplaatst, VZR)

Bronnenlijst

[gedaagde 2] is voorlopig niet van plan [naam 1] publiekelijk af te vallen. Hij is er nog altijd van overtuigd dat [naam 1] inderdaad een meesterhacker is. (..) Het krantenartikel op pagina 6 van de zaterdageditie is op de voorpagina aangekondigd met de tekst: “Cyberspion of fantast? De wondere wereld van [naam 1] ”

2.7. Op 6 februari 2018 heeft Kaspersky een tweet geplaatst met de volgende tekst: “*Op basis van ons uitgebreid en intern onderzoek is aangetoond dat er geen hack heeft plaatsgevonden zoals # [naam 1] beweerd zou hebben in @Telegraaf.”*

2.8. Op 6 februari 2018 heeft de NOS in een artikel “*Kaspersky wil omstreden cyberexpert [naam 1] aanklagen om laster”* geschreven: *“(..) Hoewel ze geen bedrijf bij naam noemde, was in de hackerswereld snel duidelijk dat het om Kaspersky zou moeten gaan, aangezien dat het enige Russische beveiligingsbedrijf met een vestiging in Utrecht is. (..)”*

2.9. Op 9 februari 2018 heeft het tijdschrift Quote in een artikel op haar website geschreven dat zij beschikt

over een heimelijk opgenomen telefoongesprek tussen [naam 1] en [gedaagde 2] en dat daaruit blijk dat [naam 1] ontkent Kaspersky te hebben gehackt en dat [gedaagde 2] ontkent dat hij de bron is van het "Kaspersky-verhaal".
2.10. Bij brieven van 19 februari 2018 heeft Kaspersky zowel TMG als [naam 1] verzocht om opheldering over wat [naam 1] precies over Kaspersky heeft gezegd in haar gesprek met de Telegraaf.
2.11. In een e-mail van 20 februari 2018 heeft [naam 1] aan (de advocaat van) Kaspersky meegedeeld dat zij niet aan de journalisten van De Telegraaf heeft verklaard een opdracht te hebben gekregen om Kaspersky te hacken. Zij schrijft: *"Ik heb noch rechtstreeks noch indirect naar uw cliënte verwezen."*
2.12. In een e-mail van 22 februari 2018 heeft TMG aan (de advocaat van) Kaspersky meegedeeld dat de publicatie geen onwaarheden bevat. Zij schrijft: *"De beschrijving van de gebeurtenissen bij het kantoor van Kaspersky op kerstavond 2017, zoals opgenomen in het betreffende artikel, vormt een correcte weergave van hetgeen mevrouw [naam 1] tegenover beide verslaggevers heeft bevestigd en verklaard."*
2.13. In een schriftelijke verklaring van [naam journalist 2] staat voor zover van belang het volgende: *"Hierbij verklaar ik (..) journalist bij (..) De Telegraaf, dat ik in de aanloop naar het artikel over [naam 1] van 3 februari 2018 van een bron - aan wie ik anonimiteit heb toegezegd - heb vernomen dat [naam 1] een opdracht had gekregen om het computernetwerk van Kaspersky binnen te dringen om informatie te stelen. (..) De anonieme bron verklaarde aan mij dat [naam 1] dit aan hem vertelde nadat hij via een Tweede Kamerlid had vernomen dat (..) banden zou hebben met Rusland. (..) Toen de bron dit besprak met [naam 1] gaf zij aan dat zij met een speciaal onderzoek bezig was (..) Volgens de bron was zij op Kerstavond 2017 met een speciaal geprepareerde telefoon naar het Nederlandse kantoor van Kaspersky in Utrecht afgereisd. Door met die telefoon langs het kantoor te lopen, kon zijn binnendringen in het netwerk van Kaspersky. Op deze wijze zou ze 40 IP-adressen hebben buitgemaakt. (..) Vrijdagavond 2 februari heb ik samen met collega [naam journalis 1] dit verhaal voorgelegd aan [naam 1] . Niet alleen bevestigde zij het verhaal op hoofdlijnen, ze verstrekte er ook extra details over. Zo vertelde zij onder meer dat ze niet alleen een speciaal geprepareerde telefoon heeft gebruikt om het netwerk te kunnen binnendringen, maar ook een laptop. Ook gaf ze een verklaring voor haar reis naar het kantoor in Utrecht: alleen zo kon ze het computernetwerk binnendringen via het wifi-netwerk van Kaspersky. Ook verklaarde ze dat ze behalve 40 IP-adressen ook andere data heeft buitgemaakt, al wilde ze zelf niet toelichten wat ze daarmee bedoelde. (..)"*
2.14. In een schriftelijke verklaring van [naam journalis 1] staat voor zover van belang het volgende: *"Hierbij verklaar ik, (..), journalist bij (..) De Telegraaf, dat mijn collega [naam journalist 2] en ik op vrijdagmiddag 2 februari 2018 contact hebben gezocht met [naam 1] . Aanleiding was een anonieme bron die [naam journalist 2] had verteld over een hack die [naam 1] zou hebben gepleegd bij Kaspersky in Utrecht, (..) Wij wilden deze informatie aan haar voorleggen en controleren of deze bij haar bekend was. [naam 1] bevestigde de hack en voegde daar zelfs informatie aan toe. (..)"*
2.15. Op 13 maart 2018 heeft een bespreking plaatsgevonden tussen Kaspersky en [naam 1] op het kantoor van mr. Trojan. Tijdens deze bespreking heeft [naam 1] uiteengezet hoe volgens haar de gang van zaken rond het artikel is geweest. Volgens [naam 1] heeft zij op aanraden van [gedaagde 2] [naam journalis 1] thuis ontvangen nadat deze onaangekondigd naar haar huis was gekomen. [gedaagde 2] zou hebben geregeld dat [naam journalis 1] voor 'eerherstel' zou zorgen omdat na het optreden van [naam 1] in Nieuwsuur haar reputatie een flinke deuk had opgelopen. [naam 1] heeft in aanwezigheid van [naam journalis 1] enkele referenties gebeld. Zij heeft verder niets verklaard. Van een interview was geen sprake. Zij heeft zeker niets over Kaspersky gezegd. Kaspersky is in het geheel niet ter sprake gekomen, aldus [naam 1] in het verslag.
2.16. In een transcript van telefoongesprekken tussen [naam 1] en [gedaagde 2] van 3 februari 2018 en 7 februari 2018 die door [naam 1] zijn opgenomen en (deels) ter zitting zijn afgespeeld, staat voor zover van belang het volgende: *"(..)* ***3 februari 2018 16.53 uur.*** *[naam 1] : het enige waar ik me heel veel zorgen over maak, waarom heb je dat verteld van Kaspersky, van die hack? [gedaagde 2] : Dat heb ik niet verteld, joh, ik heb alleen verteld van wat de kamer zei, uit de kamer. [naam 1] : Hoe komen ze dan aan dat van Kaspersky? [gedaagde 2] ; Dat komt omdat ze twee in 1 zeggen, omdat het over Rusland ging. Dinge zei dat ook al tegen mij, het kamerlid. (..) [naam 1] : Het is toch eigenlijk bizar want die telegraaf man, ik heb die telegraaf man hier gehad, die [naam journalis 1] , het enige wat ik gedaan heb is die mensen gebeld en die hebben over mij gepraat. (..)* ***6 februari 2018 12:09 uur.*** *(..) [naam 1] : Wat heeft de tweede kamer gezegd van dat lek? [gedaagde 2] : Alleen met dinge besproken, de enige die dat weet, onze vriend het kamerlid. [naam 1] : Dan had je dat lek van de tweede kamer toch beter niet aan de Telegraaf kunnen vertellen? [gedaagde 2] : Nee joh, dat wisten ze al uit de kamer, de kamer wist het eerder dan ik, hoe kom je, het komt van de kamer vandaan, ik weet het van de kamer, ik heb het lek uit de kamer gehoord. (..) [naam 1] : Ja, maar dan heeft die [naam journalis 1] toch een vuil spelletje gespeeld? En met die leugens… [gedaagde 2] : Natuurlijk heeft hij een vals spelletje gespeeld, natuurlijk heeft hij gelogen. Ik wist het van de kamer, heel simpel, jij zei hoe weet jij die naam (..)*
[naam 1] : Hoe krijgen ze dat dan verzonnen van die Kaspersky want ik heb niets over Kaspersky [gedaagde 2] : Kaspersky komt uit de kamer, het komt uit de kamer (..)"
2.17. Uit door Kaspersky als productie 19 overgelegde WhatsApp-berichten van 2 februari 2018 tot en met 6

februari 2018 tussen [naam 1] en [naam journalis 1] volgt dat [naam 1] daarin ontkent iets over Kaspersky in de media of waar dan ook te hebben gemeld. In een WhatsApp-bericht van 6 februari 2018 heeft [naam journalis 1] aan [naam 1] geappt: *"Je heb tegen ons gezegd dat [gedaagde 2] van jouw onderzoek wist naar (..) Kaspersky, omdat hij per ongeluk documenten over jouw onderzoek in jouw huis zag liggen. (..)"*

2.18. Bij e-mails van 20 april 2018 en 24 mei 2018 heeft Kaspersky [gedaagde 2] verzocht op de verklaringen van [naam journalis 1] , [naam journalist 2] en [naam 1] te reageren. Een reactie is uitgebleven.

2.19. Op 25 mei 2018 heeft [naam 1] bij de notaris onder ede een verklaring afgelegd. Daarin staat voor zover van belang het volgende: *"Ik heb Kaspersky Lab niet gehackt en ben daarvoor (dus) ook niet naar Utrecht gereden. Veel andere elementen van het artikel kloppen ook niet (..) Op vrijdag 2 februari stond [naam journalis 1] (..) onaangekondigd bij mij voor de deur. (..) Uiteindelijk kwamen [gedaagde 2] en ik overeen dat ik [naam journalis 1] enkel wat referenties zou laten verifiëren. Vervolgens heb ik [naam journalis 1] (..) toch binnen gelaten. (..) Ik heb tijdens dit bezoek niets verklaard over mijn levensverhaal, vorige opdrachten en ook niet over Kaspersky Lab. Ik heb dus ook niet verklaard dat ik Kaspersky Lab zou hebben gehackt en/of daarvoor naar Utrecht zou zijn gereden. (..) Eind van die middag en die avond werd ik nog drie keer gebeld door [naam journalis 1] . (..) Het derde telefoongesprek had een volstrekt andere, agressieve toon en verliep akelig. (..) Ik kreeg sterk het gevoel dat [naam journalis 1] en vooral ook [naam journalist 2] probeerden mij erin te luizen. Zij probeerden mij woorden in de mond te leggen over een onderzoek naar Kaspersky Lab en een hack bij Kaspersky Lab, waarop ik reageerde dat hij deze leugens toch niet kon gaan schrijven. (..)"*

2.20. Op 18 juni 2018 heeft een vriend van [naam 1] , die anoniem wil blijven, onder ede bij de notaris verklaard dat hij op vrijdag 2 februari 2018 bij [naam 1] was toen zij door de journalisten van De Telegraaf werd gebeld en dat hij toen heeft gehoord dat [naam 1] ten overstaan van de journalisten heeft ontkend dat zij Kaspersky heeft gehackt.

in reconventie

2.21. Op 14 mei 2018 heeft de minister van Justitie en Veiligheid een brief naar de Tweede Kamer gestuurd, waarin hij meedeelt dat gelet op de nationale veiligheid de overheid heeft besloten om antivirussoftware van Kaspersky niet meer te gebruiken. De reden is dat Kaspersky onder de Russische wetgeving valt en haar medewerking dient te verlenen aan de Russische inlichtingendiensten. Volgens de minister bestaat daardoor risico op digitale spionage en sabotage.

2.22. Op 12 juni 2018 heeft de oprichter van Kaspersky, [naam oprichter] , in een artikel met de titel *"Dutch hacker, big cyber-politics, and the anatomy of 'real' fake news"* op haar website verklaard dat de onder 2.20 vermelde beslissing is gebaseerd op leugens in de media. Als voorbeeld wordt het artikel in de Telegraaf genoemd van 3 februari 2018. In het artikel staat voor zover van belang het volgende: *"(..) The threads of this bewildering story lead to none orther than a former Dutch minister, [gedaagde 2] , who, incidentally, together with the above-mentioned hacker, had previousley written a book about cybersecurity – but which was later withdrawn from circulation due to plagiarism. De Telegraaf claims that an anonymous source told their journalists about the hacking of KL's Dutch office, and evidence points to [gedaagde 2] as the anonymous source, who supposedly whispered the fake narrative to the newspaper. (..)"*

2.23. Uit de op 12 juni 2018 op de website www.nu.nl geplaatste berichtgeving blijkt dat de advocaat van Kaspersky het volgende aan nu.nl heeft gemeld: *"Karspersky Lab concludeert op basis van WhatsApp-verkeer tussen [naam 1] en De Telegraaf-journalist [naam journalis 1] dat die anonieme bron [gedaagde 2] is", zegt Trojan. Over de exacte inhoud van dit verkeer wil hij tot de zitting niets zeggen"*

3 Het geschil in conventie

3.1. Kaspersky vordert - samengevat -:

I TMG te gebieden de volgende tekst duidelijk zichtbaar op de homepage van haar website www.telegraaf.nl te plaatsen, bij een gebruikelijke scherminstelling, boven de pagebreak, in een kader met dikke zwarte belijning en met de titel in vet gedrukte kapitalen en gedurende 12 maanden daar geplaatst te houden:

"RECTIFICATIE KASPERSKY LAB

In de zaterdageditie van De Telegraaf van 3 februari 2018 stond een artikel, waarin de krant verslag deed van een interview met [naam 1] . In dat artikel staat dat [naam 1] de krant zou hebben verteld dat zij op Kerstavond 2017 een in Utrecht gevestigd "wereldberoemd Russisch softwarebeveiligingsbedrijf" met een hoofdkantoor in Moskou gehackt heeft. Hoewel de naam van dit bedrijf niet genoemd wordt, is het duidelijk dat het gaat om Kaspersky Lab. In een door Kaspersky Lab aanhangig gemaakt kort geding bij de rechtbank Amsterdam heeft De Telegraaf niet aannemelijk kunnen maken dan [naam 1] heeft gezegd dat zij Kaspersky Lab heeft gehackt. [naam 1] ontkent dat zij Kaspersky Lab heeft gehackt en dat zij zich in deze zin zou hebben uitgelaten jegens De Telegraaf. De Rechtbank Amsterdam heeft de publicatie onrechtmatig bevonden en De Telegraaf veroordeeld deze rectificatie te plaatsen. Namens de hoofdredactie van De Telegraaf [naam hoofdredactie] ",

althans een rectificatie in door de voorzieningenrechter te bepalen bewoordingen,

II TMG te gebieden op de voorpagina, althans een door de voorzieningenrechter te bepalen pagina van de papieren krant van De Telegraaf, de onder I vermelde tekst duidelijk zichtbaar te plaatsen in een kader met dikke zwarte belijning en met de titel in vet gedrukte kapitalen,

III [gedaagde 2] - als de voorzieningenrechter tot het voorlopige oordeel komt dat hij De Telegraaf heeft verteld dat [naam 1] Kaspersky Lab heeft gehackt of woorden van gelijke strekking heeft gebruikt in zijn contacten met De Telegraaf - te gebieden op eigen

kosten op de voorpagina, althans een door de voorzieningenrechter te bepalen pagina, van de zaterdageditie van de papieren krant van De Telegraaf, de volgende tekst te doen plaatsen in een kader zwarte dikke belijning en met de titel in vet gedrukte kapitalen:

"RECTIFICATIE KASPERSKY LAB

In de zaterdageditie van De Telegraaf van 3 februari 2018 stond een artikel, waarin de krant verslag deed van een interview met [naam 1] . In dat artikel staat dat [naam 1] de krant zou hebben verteld dat zij op Kerstavond 2017 een in Utrecht gevestigd "wereldberoemd Russisch softwarebeveiligingsbedrijf" met een hoofdkantoor in Moskou gehackt heeft. Hoewel de naam van dit bedrijf niet genoemd wordt, is het duidelijk dat het gaat om Kaspersky Lab. In een door Kaspersky Lab aanhangig gemaakt kort geding bij de Rechtbank Amsterdam heeft de voorzieningenrechter geoordeeld dat aangenomen moet worden dat ik de bron ben van dit bericht. Voorts heeft de voorzieningenrechter geoordeeld dat niet is gebleken dat [naam 1] Kaspersky Lab heeft gehackt, noch dat zij zich in die zin heeft uitgelaten. De rechtbank Amsterdam heeft mij veroordeeld deze rectificatie te plaatsen.

[gedaagde 2] ",

althans een rectificatie in door de voorzieningenrechter te bepalen bewoordingen,

IV te bepalen dat gedaagden dwangsommen verbeuren als zij niet aan de opgelegde geboden voldoen,

V althans zodanige voorzieningen te treffen die de voorzieningenrechter passend en doeltreffend oordeelt,

VI gedaagden te veroordelen in de kosten van dit geding, inclusief nakosten.

3.2. Kaspersky stelt hiertoe het volgende. Op basis van de inhoud van het artikel is eenvoudig vast te stellen dat het softwarebeveiligingsbedrijf dat door [naam 1] zou zijn gekraakt Kaspersky betreft. Kaspersky kreeg dan ook veel reacties op het artikel. Zij heeft meteen een intern onderzoek ingesteld en naar buiten gebracht dat daaruit is gebleken dat er geen aanwijzingen waren voor een hack. [naam 1] heeft steeds ten stelligste ontkend dat zij aan de journalisten heeft verklaard dat zij Kaspersky heeft gehackt. Zij heeft verklaard dat zij op advies van [gedaagde 2] thuis met [naam journalis 1] heeft gepraat; het doel was haar reputatie te herstellen door referenties te bellen die haar kwaliteiten als hacker zouden bevestigen. De naam Kaspersky viel volgens [naam 1] die dag pas in de avond in een telefoongesprek tussen de journalisten en haar. Er werd gehengeld naar een bevestiging, aldus [naam 1] . Na de publicatie heeft [naam 1] gebeld met [gedaagde 2] . Uit het transcript van deze gesprekken blijkt dat [naam 1] tegen [gedaagde 2] heeft gezegd dat zij Kaspersky niet heeft genoemd en dat [gedaagde 2] dat heeft beaamd. Ook in een Whatsapp bericht aan [naam journalis 1] ontkent [naam 1] dat zij de bron is van het Kaspersky-verhaal. Hiertegenover staan de verklaringen van de journalisten, die verwijzen naar een anonieme bron, en die volhouden dat [naam 1] het Kaspersky-verhaal heeft bevestigd. De balans slaat door in het voordeel van [naam 1] . Zij heeft aannemelijk gemaakt dat zij niet de bron is van de berichtgeving rond Kaspersky. Waar het bericht over Kaspersky vandaan komt, kan niet met zekerheid worden vastgesteld. Of de theorie van [gedaagde 2] over een bron in de Tweede Kamer klopt of [gedaagde 2] zelf is de bron. De ware toedracht kan in het midden blijven. In beide gevallen geldt dat TMG onzorgvuldig en onrechtmatig heeft gehandeld door zonder steun in de feiten schadelijke berichtgeving over Kaspersky naar buiten te brengen. Mocht in dit kort geding aannemelijk worden dat [gedaagde 2] als bron heeft gefungeerd dan heeft hij eveneens onrechtmatig jegens Kaspersky gehandeld. [gedaagde 2] heeft dan een onwaar verhaal de wereld in geholpen. Het recht op vrijheid van meningsuiting van TMG dient te wijken voor de belangen van Kaspersky. TMG heeft geen zorgvuldige journalistiek bedreven.

3.3. Gedaagden voeren verweer. Hierop wordt hierna, voor zover van belang, nader ingegaan.

4 Het geschil in reconventie

4.1. [gedaagde 2] vordert - samengevat na een wijziging - Kaspersky op straffe van een dwangsom te gebieden de in de akte houdende eis in reconventie bedoelde onrechtmatige beschuldigingen, op welke wijze en via welke persoon dan ook tegen hem gedaan, te staken en gestaakt te houden, althans een passend door de voorzieningenrechter in goede justitie te bepalen gebod op te leggen. [gedaagde 2] vordert daarnaast Kaspersky te veroordelen in de kosten van dit geding.

4.2. [gedaagde 2] stelt hiertoe het volgende. Kaspersky heeft in een op haar website gepubliceerd artikel van 12 juni 2018 [gedaagde 2] genoemd als bron van het Kaspersky-verhaal. Dit terwijl uit het gewraakte artikel van 3 februari 2018 niet blijkt dat er een relatie bestaat tussen Kaspersky en [gedaagde 2] . Verder verspreidt ook de advocaat van Kaspersky het bericht dat [gedaagde 2] de anonieme bron van het Kaspersky-verhaal is. Door in de media deze ernstige beschuldiging over [gedaagde 2] te uiten, terwijl daar feitelijk geen basis voor bestaat, handelt zij onrechtmatig jegens [gedaagde 2] . De onterechte beschuldiging vormt een aantasting van zijn eer en goede naam. [gedaagde 2] is louter bij deze procedure betrokken om publiciteit te genereren. Door een oud-minister te beschuldigen van lekken en het verspreiden van nepnieuws, trek je de aandacht. Het is echter Kaspersky zelf die hiermee nepnieuws verspreidt.

4.3. Kaspersky voert verweer. Hierop wordt hierna, voor zover van belang, nader ingegaan.

5 De beoordeling in conventie

5.1. In geschil is of TMG onrechtmatig heeft gehandeld jegens Kaspersky door publicatie van het onder 2.6 weergegeven krantenartikel in de Telegraaf van 3 februari 2018. Het gaat Kaspersky om het in het artikel opgenomen verhaal van [naam 1] dat zij op Kerstavond 2017 het computernetwerk van een in Utrecht gevestigd "*wereldberoemd Russisch softwarebeveiligingsbedrijf*" is binnengedrongen (heeft gehackt) en 40 IP-adressen heeft buitgemaakt. De aanduiding van het bedrijf is eenvoudig te herleiden tot

Kaspersky. Het is het enige in Utrecht gevestigde softwarebedrijf van Russische origine. Kaspersky vordert dat TMG dit artikel rectificeert.
5.2. Het spoedeisend belang bij de rectificatie vloeit voort uit het feit dat daarmee de schade van de vermeende onrechtmatige publicatie kan worden beperkt. Dat inmiddels meer dan vijf maanden zijn verstreken, doet daar niet aan af. De publicatie kan nog steeds op internet worden geraadpleegd.
5.3. Uitgangspunt is dat toewijzing van de vordering van Kaspersky een beperking inhoudt van het in artikel 10 lid 1 van het Europees Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (EVRM) neergelegde grondrecht van TMG op vrijheid van meningsuiting. Een dergelijk recht kan slechts worden beperkt indien dit bij de wet is voorzien en noodzakelijk is in een democratische samenleving bijvoorbeeld ter bescherming van de goede naam en de rechten van anderen (artikel 10 lid 2 EVRM). Van een beperking die bij de wet is voorzien is sprake, wanneer de uitlatingen van TMG onrechtmatig zijn in de zin van artikel 6:162 van het Burgerlijk Wetboek (BW). Voor het antwoord op de vraag welk recht – het recht op vrije meningsuiting of het recht ter bescherming van eer of goede naam – in dit geval zwaarder weegt, moeten de wederzijdse belangen worden afgewogen. Daarbij geldt dat ook een rechtspersoon op bescherming aanspraak kan maken. Het belang van TMG is dat de krant die zij uitgeeft zich in het openbaar kritisch, informerend, opiniërend en waarschuwend moet kunnen uitlaten over misstanden die de samenleving raken. Het belang van Kaspersky is erin gelegen dat zij niet lichtvaardig wordt blootgesteld aan voor haar schadelijke publiciteit. Welk van deze belangen, die in beginsel gelijkwaardig zijn, de doorslag behoort te geven, hangt af van de omstandigheden van het geval.
5.4. Beoordeeld dient te worden of TMG in haar berichtgeving voldoende zorgvuldig is geweest. Als uitgangspunt dient de door de Raad voor Journalistiek uitgegeven Leidraad. Daarin is opgenomen dat journalisten waarheidsgetrouw, controleerbaar en zo volledig mogelijk berichten, en dat zij eenzijdige en tendentieuze berichtgeving dienen te vermijden. Een journalist die negatieve berichten over derden publiceert, dient die derde in staat stellen daarop een weerwoord te geven (B.3 Leidraad).
5.5. De journalisten stellen dat de informatie over de hack bij Kaspersky afkomstig is van een anonieme bron. Wie de persoon achter de anonieme bron is wil TMG niet bekend te maken. Zij beroept zich op bronbescherming. Er zijn aanwijzingen dat [gedaagde 2] de anonieme bron is, waarover hierna in reconventie meer. TMG noch [gedaagde 2] willen dit echter niet bevestigen. Voor de beoordeling of de journalisten waarheidsgetrouw hebben bericht speelt de anonieme broninformatie een zeer beperkte rol omdat deze niet op betrouwbaarheid en geloofwaardigheid kan worden getoetst.
5.6. [naam 1] ontkent tegen de journalisten te hebben gezegd dat zij Kaspersky heeft gehackt. Zij heeft over haar contact met de journalisten en de inhoud van haar uitlatingen een gedetailleerde schriftelijke verklaring afgelegd. Dat zij niet over Kaspersky heeft gepraat wordt bevestigd door een vriend van [naam 1] die verklaart bij [naam 1] thuis te zijn geweest en die zegt te hebben gehoord wat zij tegen de journalisten heeft gezegd.
5.7. Iedere aanwijzing ontbreekt dat op het computernetwerk van Kaspersky is ingebroken. Kaspersky zegt daarnaar zonder resultaat onderzoek te hebben gedaan.
5.8. Al met al kan het verhaal van [naam 1] over Kaspersky de facto uitsluitend worden getoetst aan wat de journalisten hebben verklaard over wat zij telefonisch van [naam 1] hebben gehoord. Ter zitting heeft [naam journalis 1] verklaard dat hij na een persoonlijk gesprek met [naam 1] aan haar keukentafel hoorde dat zijn collega [naam journalist 2] contact had met een geheime bron die melding had gedaan over de hack door [naam 1] bij Kaspersky op Kerstavond 2017. Nog diezelfde avond heeft [naam journalis 1] dit tijdens een (derde) telefoongesprek aan [naam 1] voorgelegd, waarna zij volgens hem bevestigde dat zij Kaspersky had gehackt en daarover zelfs nieuwe details kon vertellen. Het gesprek stond op de luidspreker waardoor [naam journalist 2] ook hoorde wat er werd gezegd. [naam journalist 2] bevestigt deze gang van zaken.
5.9. Van het bewuste telefoongesprek is geen audio-opname gemaakt. Ook zijn geen aantekeningen of andere steunbewijs overgelegd die de door TMG gestelde uitlatingen van [naam 1] over Kaspersky bevestigen. Op de zitting verklaarde [naam journalis 1] dat hij met zijn mobiele telefoon met [naam 1] belde waardoor het gesprek niet tegelijkertijd kon worden opgenomen. Zijn collega [naam journalist 2] verklaarde dat hij tijdens het gesprek uitsluitend op de computer aantekeningen maakte van wat er werd gezegd en dat deze aantekeningen zijn verwerkt in het artikel en niet apart bewaard zijn. Geconstateerd kan worden dat de journalisten niet controleerbaar hebben gemaakt wat [naam 1] tegenover hen heeft verklaard terwijl dit gemakkelijk had gekund. Zo wordt niet duidelijk waarom [naam journalis 1] geen aantekeningen of audio-opname kon maken. Het gesprek stond immers op de speaker. Dit geldt temeer omdat [naam journalis 1] wel van het keukentafelgesprek een audio-opname heeft gemaakt. Er zijn bovendien telefoon-apps waarmee gemakkelijk een telefoongesprek kan worden opgenomen terwijl met diezelfde telefoon een gesprek wordt gevoerd. Daarbij komt dat geen sprake was van een terloops telefoongesprek waarbij onverwacht door [naam 1] belangrijke uitlatingen werden gedaan. Zij werd immers bewust door de journalisten geconfronteerd met nieuwe informatie over een opzienbarende kwestie. Dat is nagelaten maatregelen te treffen teneinde de uitlatingen van [naam 1] controleerbaar te maken kan TMG worden verweten.
5.10. In het nadeel van TMG weegt verder mee dat de verklaringen van de journalisten op onderdelen niet helemaal op elkaar lijken te passen. Een voorbeeld is

dat [naam journalist 2] in zijn schriftelijke verklaring eerst de informatie die hij van de anonieme bron kreeg heeft beschreven en daarna aangeeft dat [naam 1] in het telefoongesprek het verhaal 'op hoofdlijnen' bevestigde en zelfs daarover aanvullende informatie verstrekte. [naam journalis 1] noemt bij de beschrijving van wat [naam 1] tijdens het telefoongesprek aan extra details noemt informatie die [naam journalist 2] juist van de anonieme bron stelt te hebben gekregen. Het lijkt er dus op dat verschillend is verklaard over van wie welke informatie afkomstig is. Dit doet af aan de betrouwbaarheid van die verklaringen. Het beeld van het verloop van het gesprek met [naam 1] zoals dat uit de publicatie blijkt stemt bovendien niet goed overeen met wat de journalisten over de gang van zaken rond het gesprek met [naam 1] hebben verteld. Uit de schriftelijk verklaring van [naam journalis 1] is niet af te leiden dat hij, zoals hij op de zitting heeft verklaard, pas na het persoonlijk gesprek met [naam 1] , toen hij terugkwam op de redactie, door zijn collega op de hoogte is gesteld over de hack bij Kaspersky, waarna hij in aanwezigheid van [naam journalist 2] meermalen met [naam 1] heeft gebeld en haar in een derde telefoongesprek met die informatie heeft geconfronteerd.

5.11. Daarbij komt dat de audio-opname van het keukentafelgesprek niet is overgelegd. Dit is opmerkelijk omdat daarmee afbreuk aan de geloofwaardigheid van [naam 1] had kunnen worden gedaan. [naam 1] heeft immers in haar verklaring uitdrukkelijk betwist dat zij aan de keukentafel haar levensverhaal heeft gedaan, zoals in het artikel staat. Als dat wel zo was geweest, had [naam journalis 1] dat met zijn audio-opname kunnen aantonen. Voor [naam 1] had dat in haar nadeel kunnen meewegen. In de pleitnota van mr. Le Poole is onder 3.3. weliswaar een klein fragment van de weergave van het gesprek opgenomen waarin het niet gaat over de referenten, maar deze passage is onvoldoende om aan te nemen dat [naam 1] liegt over wat er in het gesprek wel en niet aan de orde is geweest, dan wel dat zij niet geloofwaardig is.

5.12. Ook weegt ten nadele van de journalisten mee dat zij vóór publicatie geen verder onderzoek naar de inbraak hebben gedaan. Kaspersky is bovendien niet conform de Leidraad in de gelegenheid gesteld een weerwoord te geven.

5.13. TMG voert als verweer dat het artikel een door de lezer niet serieus te nemen inhoud heeft. Ook zou de nieuwswaarde van het artikel zijn gelegen in het schetsen van de achtergrond van [naam 1] en niet dat zij een Utrechts bedrijf heeft gehackt. Voorzover TMG hiermee heeft willen betogen dat de uitlating over de hack bij Kaspersky geen schadelijke gevolgen voor dat bedrijf kan hebben gehad omdat het voor de lezer duidelijk was dat die uitlating onzin was, wordt dit standpunt niet gevolgd. Hoewel de toonzetting luchtig is, en het artikel vraagtekens zet bij het waarheidsgehalte van de in het artikel opgenomen uitlatingen van [naam 1] , roept de inhoud bij de lezer een ambivalent beeld op. Enerzijds luidt de titel van de publicatie *"Meesterspionne of misleidster?"* en *"Welkom in de wondere wereld van hacker [naam 1] "*, toont de foto prominent een schaars gekleed model, en wordt op de voorpagina verwezen naar de 'wilde verhalen' op pagina 6. Anderzijds komen in het artikel echter passages voor die een heel ander, serieus beeld oproepen over [naam 1] en haar professionele activiteiten als hacker. Zo worden in het artikel meerdere referenten aan het woord gelaten die stuk voor stuk bevestigen dat [naam 1] een bedreven hacker is. Ook wordt [gedaagde 2] opgevoerd, die volgens De Telegraaf voorlopig niet van plan is [naam 1] publiekelijk af te vallen, en er nog altijd van overtuigd is dat [naam 1] inderdaad een meesterhacker is. Dit ambivalente beeld roept bij de gemiddelde lezer de gedachte op dat - hoewel het een ' wild verhaal' is - (een deel van) wat [naam 1] in het artikel zcegt mogelijk wel degelijk op waarheid berust. Het verhaal over de inbraak in het computernetwerk dat uit de mond van [naam 1] is opgetekend neemt een prominente plaats in de publicatie in. Mede gelet op de details die over het binnendringen in het computernetwerk worden verteld kan dit de lezer de indruk geven dat de inbraak echt heeft plaatsgevonden.

5.14. De conclusie is dat de publicatie van het verhaal van [naam 1] over de inbraak in het computernetwerk voorshands onzorgvuldig is. Zonder nader onderzoek waarvoor in dit kort geding geen plaats is, is slechts op basis van de verklaringen van de journalisten en de informatie uit anonieme bron onvoldoende aannemelijk dat [naam 1] zich heeft uitgelaten over een inbraak op het computernetwerk van Kaspersky. [naam 1] ontkent, er geen aanwijzingen dat die inbraak heeft plaatsgevonden, en door TMG is geen eigen onderzoek gedaan naar die inbraak. Kaspersky is bovendien niet om een reactie gevraagd. Dat Kaspersky hierdoor schade heeft geleden en mogelijk nog zal lijden is voldoende aannemelijk. De berichtgeving kan (potentiële) klanten afschrikken. Een cybersecuritybedrijf dat haar eigen internetveiligheid niet in orde heeft levert commercieel zeer nadelige beeldvorming op. Al met al is de publicatie in De Telegraaf voorshands onrechtmatig tegenover Kaspersky.

5.15. Gelet op het voorgaande zal de gevraagde voorziening worden getroffen. Dit betreft een rectificatie zoals gevorderd, met dien verstande dat de rectificatie, om aandacht te trekken, slechts één dag op de homepage van website en de voorpagina van de zaterdageditie van de papieren krant hoeft te staan. Daarnaast zal de rectificatie als bijschrift aan de oude publicatie (de bron) moeten worden gekoppeld, zodat bij raadpleging daarvan meteen zichtbaar is dat sprake is geweest van een rectificatie. TMG heeft als productie 6 een concept voor een artikel overgelegd dat zij bereid is in De Telegraaf te plaatsen. Kaspersky hoeft met plaatsing van dit artikel geen genoegen te nemen omdat het niet ver genoeg gaat. In dat concept wordt niet erkend dat van onzorgvuldige berichtgeving sprake is.

5.16. Dat de berichtgeving in De Telegraaf ertoe heeft geleid dat de overheid niet langer gebruik maakt van de

diensten van Kaspersky is overigens niet aannemelijk geworden. Uit de overgelegde stukken blijkt voldoende duidelijk dat dit een geheel andere oorzaak heeft.
5.17. De gevorderde dwangsom zal worden beperkt en gemaximeerd als volgt.
5.18. De in conventie gevorderde - al dan niet voorwaardelijke - rectificatie tegen [gedaagde 2] zal worden afgewezen omdat niet met voldoende mate van zekerheid is vast te stellen dat hij de anonieme bron is geweest.
Voorts in reconventie
5.19. Voor het in reconventie jegens Kaspersky gevorderde geldt hetzelfde criterium als in conventie verwoordt. Wil sprake zijn van een beperking die bij de wet is voorzien, dan zullen de door of namens Kaspersky op internet gedane uitlatingen onrechtmatig jegens [gedaagde 2] moeten zijn. Om uit te maken of dat het geval is moet een belangenafweging worden gemaakt. Bij deze belangenafweging speelt de mate waarin de uitlatingen steun vinden in het beschikbare feitenmateriaal een belangrijke rol.
5.20. De gevorderde rectificatie door [gedaagde 2] zal worden afgewezen. Hoewel het overtuigende bewijs ontbreekt, omdat zowel de journalisten als [gedaagde 2] dit niet willen bevestigen, zijn er wel twee aanwijzingen dat [gedaagde 2] als 'anonieme' bron is opgetreden. De eerste aanwijzing is een WhatsApp bericht van 6 februari 2018 waarin [naam journalis 1] aan [naam 1] schrijft: "Je hebt tegen ons gezegd dat [gedaagde 2] van jouw onderzoek wist naar (..) Kaspersky." Een tweede aanwijzing vormt de inhoud van de door [naam 1] na publicatie opgenomen telefoongesprekken tussen haar en [gedaagde 2] , waaruit kan worden afgeleid dat [gedaagde 2] toegeeft dat er rechtstreeks contact is geweest tussen hem en de journalisten van de Telegraaf. Deze aanwijzingen maken dat vooralsnog niet kan worden gezegd dat de verdenkingen in de richting van [gedaagde 2] onterecht zijn en op geen enkele manier door feiten worden ondersteund.
5.21. Ook zijn geen andere omstandigheden gebleken waardoor de belangenafweging alsnog in het voordeel van [gedaagde 2] uitpakt. Los van de vraag of de bij de feiten onder 2.22 en 2.23 vermelde uitlatingen, zoals Kaspersky stelt, wel in zijn geheel aan Kaspersky kunnen worden toegeschreven en of de uitlatingen überhaupt wel beschuldigend zijn, is een rectificatie niet aan de orde. De vordering in reconventie wordt afgewezen.
5.22. TMG zal in conventie in de zaak tegen Kaspersky als de in het ongelijk gestelde partij in de proceskosten worden veroordeeld. De kosten aan de zijde van Kaspersky worden begroot op:
- dagvaarding € 81,00
- griffierecht 626,00
- salaris advocaat 980,00
Totaal € 1.687,00
5.23. De door Kaspersky gevorderde veroordeling in de nakosten is in het kader van deze procedure slechts toewijsbaar voor zover deze kosten op dit moment reeds kunnen worden begroot. De nakosten zullen dan ook op de navolgende wijze worden toegewezen.
5.24. Kaspersky zal in conventie in de zaak tegen [gedaagde 2] als de in het ongelijk gestelde partij in de proceskosten worden veroordeeld. De kosten aan de zijde van [gedaagde 2] worden begroot op:
- griffierecht 291,00
- salaris advocaat 980,00
Totaal € 1.271,00
5.25. [gedaagde 2] zal in reconventie als de in het ongelijk gestelde partij in de proceskosten worden veroordeeld. Gelet op de samenhang met de zaak in conventie zullen deze aan de zijde van Kaspersky worden begroot op nihil.

6 De beslissing

De voorzieningenrechter
in conventie
6.1. gebiedt TMG binnen drie werkdagen na betekening van dit vonnis de volgende tekst duidelijk zichtbaar op de homepage van haar website www.telegraaf.nl te plaatsen, bij een gebruikelijke scherminstelling boven de pagebreak, in een kader met zwarte belijning en met de titel in vet gedrukte kapitalen, en gedurende 1 dag daar geplaatst te houden en daarna als bijschrift aan oude publicatie (de bron) te koppelen, zodat bij raadpleging daarvan meteen zichtbaar is dat sprake is geweest van een rectificatie,
"RECTIFICATIE KASPERSKY LAB
In de zaterdageditie van De Telegraaf van 3 februari 2018 stond een artikel, waarin de krant verslag deed van een interview met [naam 1] . In dat artikel staat dat [naam 1] de krant zou hebben verteld dat zij op Kerstavond 2017 een in Utrecht gevestigd "wereldberoemd Russisch softwarebeveiligingsbedrijf" met een hoofdkantoor in Moskou gehackt heeft. Hoewel de naam van dit bedrijf niet genoemd wordt, is het duidelijk dat het gaat om Kaspersky Lab. In een door Kaspersky Lab aanhangig gemaakt kort geding bij de rechtbank Amsterdam heeft De Telegraaf niet aannemelijk kunnen maken dan [naam 1] heeft gezegd dat zij Kaspersky Lab heeft gehackt. [naam 1] ontkent dat zij Kaspersky Lab heeft gehackt en dat zij zich in deze zin zou hebben uitgelaten jegens De Telegraaf. De Rechtbank Amsterdam heeft de publicatie onrechtmatig bevonden en De Telegraaf veroordeeld deze rectificatie te plaatsen.
Namens de hoofdredactie van De Telegraaf
[naam hoofdredactie] ",
6.2. TMG te gebieden op de voorpagina van de eerstvolgende zaterdageditie van de papieren krant die zal verschijnen drie dagen na betekening van dit vonnis, de onder 6.1 vermelde rectificatietekst duidelijk zichtbaar te plaatsen, in een kader met zwarte belijning en met de titel in vet gedrukte kapitalen,
6.3. veroordeelt TMG om aan Kaspersky een dwangsom te betalen van € 10.000,00 voor iedere dag dat zij niet aan het onder 6.1 en/of 6.2 genoemde gebod voldoet, tot een maximum van € 100.000,00 is bereikt,
6.4. veroordeelt TMG in de zaak tegen Kaspersky in de proceskosten, aan de zijde van Kaspersky tot op heden begroot op € 1.687,00,

6.5. veroordeelt TMG in de zaak tegen Kaspersky in de na dit vonnis ontstane kosten, begroot op € 157,00 voor salaris advocaat, te vermeerderen met € 82,00 en de kosten van het betekeningsexploot ingeval betekening van dit vonnis plaatsvindt,
6.6. veroordeelt Kaspersky in de zaak tegen [gedaagde 2] in de proceskosten, aan de zijde van [gedaagde 2] tot op heden begroot op € 1.271,00,
6.7. verklaart dit vonnis in conventie tot zover uitvoerbaar bij voorraad,
6.8. wijst het meer of anders gevorderde af,
in reconventie
6.9. weigert de gevraagde voorzieningen,
6.10. veroordeelt [gedaagde 2] in de proceskosten, aan de zijde van Kaspersky tot op heden begroot op nihil.
Dit vonnis is gewezen door mr. M.W. van der Veen, voorzieningenrechter, bijgestaan door mr. G.H. Felix, griffier, en in het openbaar uitgesproken op 16 juli 2018.