



UHASSELT

KU LEUVEN



Maastricht University

KNOWLEDGE IN ACTION

Faculteit Rechten

master in de rechten

Masterthesis

Bedrijfsgeheimen en telewerkers

Ginny Geirnaert

Scriptie ingediend tot het behalen van de graad van master in de rechten, afstudeerrichting rechten

PROMOTOR :

Prof. dr. Petra FOUBERT

De transnationale Universiteit Limburg is een uniek samenwerkingsverband van twee universiteiten in twee landen: de Universiteit Hasselt en Maastricht University.



UHASSELT

KNOWLEDGE IN ACTION

www.uhasselt.be

Universiteit Hasselt
Campus Hasselt:
Martelarenlaan 42 | 3500 Hasselt
Campus Diepenbeek:
Agoralaan Gebouw D | 3590 Diepenbeek

2020
2021



UHASSELT

KNOWLEDGE IN ACTION

KU LEUVEN



Maastricht University

Faculteit Rechten

master in de rechten

Masterthesis

Bedrijfsgeheimen en telewerkers

Ginny Geirnaert

Scriptie ingediend tot het behalen van de graad van master in de rechten, afstudeerrichting rechten

PROMOTOR :

Prof. dr. Petra FOUBERT

Samenvatting

Een tweetal jaren geleden trad de Wet betreffende de bescherming van bedrijfsgeheimen stilletjes in werking. Hoewel deze wet zonder veel fanfare zijn intrede deed, had dit gezien het onderwerp van dit wetgevend instrument nochtans moeten gebeuren. De wet heeft immers gezorgd voor een officieel wettelijk kader om bedrijfsgeheimen te beschermen.

Waarom is dit belangrijk? Simpel, als houders van bedrijfsgeheimen bv. bedrijven hun bedrijfsgeheimen niet wettelijk kunnen beschermen, waarom zouden ze dan nog moeite doen om innoverend proberen te zijn? Denk aan alle technologie die op dit moment bestaat. Zonder de mogelijkheid om een octrooi te registeren op een bepaalde nieuwe techniek, zou niemand nog gemotiveerd zijn om technologie verder te avanceren. Vervolgens kan de wet gebruikt worden om geheime informatie van concurrenten te beschermen. Laat dit nu net iets zijn dat van onschatbare waarde is op een moment waarop vele werkgevers verplicht zijn om hun werknemers thuis te laten telewerken.

Daarom werd beslist om in deze masterscriptie te onderzoeken wat de impact is van de Wet betreffende de bescherming van bedrijfsgeheimen op telewerkers. De wet werd immers geschreven op een ogenblik toen nog nooit iemand van Covid-19 had gehoord. Het uitgangspunt van deze scriptie is bijgevolg de centrale onderzoeksvraag: *Wat is de impact van de Wet betreffende de bescherming van bedrijfsgeheimen op een werknemer die thuis werkt?* Om hierop een antwoord te vinden, is gewerkt met een theoretische hoofdstukken en praktische hoofdstukken waarin de centrale vraag verdeeld werd in meerdere subvragen.

De eerste subvragen waren gericht op het opbouwen van een algemeen kader teneinde een goede basis te hebben voor de meer praktische hoofdstukken. Deze subvragen hadden als onderwerp de wet zelf, de richtlijn waarvan de wet de omzetting is en als laatste het begrip bedrijfsgeheimen zelf. Uit deze hoofdstukken kon o.a. vastgesteld worden dat de Wet Bedrijfsgeheimen slechts een wet is in naam en niet in vorm, vermits zij enkel bestaande wetgeving wijzigde. De bespreking van de term bedrijfsgeheimen zelf leidde tot onder meer de vaststelling dat er veel afhangt van de persoonlijke appreciatie van de rechter bij het invullen van de drie constitutieve voorwaarden van dit begrip.

In het tweede deel werden de meer praktische hoofdstukken uiteengezet. De uiteindelijke impact van de Wet Bedrijfsgeheimen op telewerkende werknemers werd in het kernhoofdstuk uitvoerig behandeld. Er werd gewerkt met zelfverzonnen hypotheses om aan te tonen op welke manier de wet en telewerken met elkaar kunnen interageren. Hieruit bleek al snel dat telewerkers niet buiten schot van de wet blijven. Dit had dan weer tot gevolg dat hun werkgevers genoodzaakt worden om juridische stappen te ondernemen om inbreuken van hun bedrijfsgeheimen te vervolgen.

De laatste twee hoofdstukken waren een kritische reflectie van het gedane onderzoek. In het voorlaatste hoofdstuk werd namelijk onderzocht of de wet werkelijk slaagde in zijn vooruitgezette doel van bescherming. Om dit te onderzoeken werd er gewerkt met een repressieve en preventieve invalshoek. Op repressief gebied weet de wet wel te beschermen, maar het is op het preventieve vlak waar de wet haar doel mist. In het allerlaatste hoofdstuk werden daarom enkele aanbevelingen geformuleerd die de wet ten goede zou komen.

Dankwoord

Met het schrijven van deze masterscriptie komt mijn vijfjarige rechtenopleiding eindelijk ten eind.

Toen ik deze opleiding aanvatte, verklaarden de meesten mij voor gek. Ik had immers al een diploma, waarom zou ik dan nog eens rechten gaan studeren?

Het is heel simpel. Rechten had en heeft voor mij altijd een zekere allure gehad. Ik heb altijd veel verschillende interesses gehad, maar ik had nooit ergens een passie voor. Bovendien, wist ik voorheen nooit welk soort beroep ik wilde doen. Tot ik begon aan de UHasselt vijf jaar geleden in de oude gevangenis. Sinds die dag kan ik eindelijk trots zeggen dat ik mijn plaats gevonden heb.

Ik hoop dan ook dat mijn passie voor rechten af te leiden is tijdens het lezen van deze masterscriptie.

Hoewel ik de afgelopen jaren ontzettend veel heb geleerd, zou ik deze scriptie nooit hebben kunnen schrijven zonder bepaalde individuen.

Allereerst, wil ik mijn begeleider professor dr. Foubert bedanken voor haar immens waardevolle begeleiding. Haar feedback heeft ervoor gezorgd dat ik steeds op het rechte pad bleef. Wij juristen hebben nogal eens de neiging om goedbedoeld af te wijken, maar dankzij haar bleef ik op het juiste spoor. Haar wijze raad om de cirkel rond te maken, zal ik bijgevolg nooit vergeten.

Vervolgens wil ik Cynthia en Louwra bedanken om de tijd te nemen om mijn scriptie na te kijken op taalkundig vlak. Zonder jullie, zou mijn scriptie, een scriptii zijn.

Als volgt, wil ik graag Anouchka en Ray bedanken. Dank u wel Anouchka om mijn klankbord te spelen. Dank u wel Ray om mijn klagmuur te spelen.

Als voorlaatste, wil ik mijn vier katten bedanken. Jullie talloze tussenkomsten waren meer dan welkom. Behalve die ene keer dat één van jullie de helft wiste door iets té enthousiast op mijn toetsenbord te komen liggen, maar daar spreken we niet over. Bedankt om mij af te leiden.

De allerlaatste die ik wil bedanken, is de persoon die mijn rots in de branding is geweest, namelijk Bart. Zonder hem zou ik zelfs nooit aan deze opleiding zijn begonnen. Vijf jaar geleden gaf hij mij de moed om me in te schrijven en dit afgelopen jaar heeft hij mij de moed gegeven om deze masterscriptie te schrijven. Er zijn niet genoeg woorden om uit te drukken hoe dankbaar ik ben dat wij samen zijn.

Inhoudsopgave

Samenvatting	I
Dankwoord	III
Inhoudsopgave	V
Inleiding.....	1
Hoofdstuk I Hoe ziet de nieuwe wet eruit?	3
I.A Wet betreffende de bescherming van bedrijfsgeheimen	3
I.B Wijzigingen aan het WER	4
I.C Wijzigingen aan het Gerechtelijk Wetboek.....	4
I.D Wijzigingen aan de wet van 3 juli 1978 (Arbeidsovereenkomstenwet)	4
I.E Overige wijzigingen.....	5
Hoofdstuk II Wat is de achtergrond van de nieuwe wet?	7
II.A Voorgeschiedenis.....	7
II.B De richtlijn.....	9
Hoofdstuk III Bedrijfsgeheimen.....	11
III.A Het begrip bedrijfsgeheimen	11
Hoofdstuk IV Wat is nu de impact van de wet op werknemers thuis?.....	17
IV.A Thuiswerken en telewerken	17
IV.B Op wie is de wet van toepassing?	19
IV.C Hypotheses	19
IV.C.1 Hypothese 1 – Situatieschets.....	21
IV.C.2 Hypothese 2– Situatieschets	21
IV.C.3 Hypothese 3– Situatieschets	22
IV.C.4 Inbreukmaker en onrechtmatige handelingen	22
IV.C.4.1 Inbreukmaker	23
IV.C.4.2 Onrechtmatige handelingen	23
IV.C.5 Beoordeling hypotheses	25
IV.C.5.1 Beoordeling hypothese 1	25
IV.C.5.2 Beoordeling hypothese 2	27
IV.C.5.3 Beoordeling hypothese 3	28
IV.D Hoe kan een werkgever (houder van een bedrijfsgeheim) optreden?	30
IV.D.1 Procedures	30
IV.D.1.1 Procedure ten gronde.....	30

IV.D.1.2	De vordering tot staking zoals in kort geding	34
IV.D.1.3	De procedure in kort geding.....	35
IV.E	Inbreukmakende goederen en rechtmatige handelingen	36
IV.E.1	Inbreukmakende goederen.....	36
IV.E.2	Rechtmatige handelingen	37
Hoofdstuk V	Heeft de Wet Bedrijfsgeheimen zijn doel bereikt in het kader van telewerken? ...	41
V.A	Repressief.....	41
V.B	Preventief	43
Hoofdstuk VI	Wat kan er beter aan de Wet Bedrijfsgeheimen in het kader van telewerken?	45
VI.A	De Duitse implementatiewet	45
VI.B	Aanbevelingen.....	47
VI.B.1	Aanbevelingen gebaseerd op de rechtsvergelijking	47
VI.B.2	Aanbevelingen gebaseerd op de rest van het onderzoek	49
Conclusie	53
Bibliografie	55
Wetgeving	55
Belgische wetgeving.....	55	
Buitenlandse wetgeving.....	57	
Rechtspraak.....	58	
Belgische rechtspraak.....	58	
Buitenlandse rechtspraak.....	58	
Rechtsleer	59	
Belgische rechtsleer	59	
Boeken	59	
Tijdschriften	59	
Varia	60	
Buitenlandse rechtsleer	63	
Boeken	63	
Tijdschriften	63	
Varia	63	

Inleiding

A. Probleemstelling

Het recept van Coca-Cola, het recept van KFC en het recept van McDonald's geheime Big Mac saus, het zijn maar enkele voorbeelden van de werelds meest bekende geheime recepten. Deze recepten zijn echter tevens voorbeelden van bedrijfsgeheimen. De bedrijven die houder zijn van deze recepten hebben sinds de ontdekking van hun recept er alles aan gedaan om de formule geheim te houden. De oorspronkelijke uitvinder van Coca-Cola weigerde in het begin zelfs om het recept op papier te zetten, uit angst dat het gestolen zou worden. Later werd het recept dan alsnog neergeschreven en in een kluis verborgen en wordt op heden nog altijd in een kluis bewaard.¹ KFC maakt dan weer gebruik van verschillende bedrijven die slechts elk een deel van de ingrediënten maken om te verzekeren dat er zo weinig mogelijk mensen zijn die het volledige recept kennen. Bovendien ligt hun recept ook achter slot en grendel in een kluis.²

De voorgaande Amerikaanse bedrijven lijken tot het uiterste te gaan om hun geheimen te beschermen en zij zijn lang niet de enige bedrijven die hun geheimen willen bewaren. Ook Belgische bedrijven willen logischerwijze hun bedrijfsgeheimen beschermen, maar hoe gaat dit te werk in België? Stoppen Belgische bedrijven hun geheimen ook in een kluis of gaan zij anders te werk? Belangrijker, hoe zit het met de bescherming van hun bedrijfsgeheimen ten tijde van de coronacrisis? Want er kan worden verondersteld dat het bedrijfsnetwerk een tikkeltje beter beschermd is dan het thuisnetwerk van een werknemer. Hoe kunnen bedrijven verzekeren dat hun werknemers geen geheimen delen met de partner die ook van thuis uit werkt?

Tot 2018 was er in België geen wettelijk kader voor de bescherming van bedrijfsgeheimen. Echter, ten gevolge van een Europese richtlijn van 2016 betreffende de bescherming van bedrijfsgeheimen, heeft België eindelijk een wet gekregen over de bescherming van bedrijfsgeheimen.³

Deze wet met de naam Wet betreffende de bescherming van bedrijfsgeheimen (Wet Bedrijfsgeheimen vanaf nu) trad in werking op 24 augustus 2018.⁴ Dit is intussen meer dan twee jaar geleden, maar ten tijde van de voorbereiding van deze wet en het maken van de Europese richtlijn zag de wereld er volledig anders uit. Er was namelijk toen nog absoluut geen sprake van Covid-19.

Door Covid-19 hebben vele bedrijven noodgedwongen hun werknemers van thuis uit moeten laten werken ter bescherming van de gezondheid.⁵ Dit is uiteraard volstrekt logisch, maar al het

¹ COCACOLACOMPANY, *Coca-Cola's Formula Is at the World of Coca-Cola*, <https://www.coca-colacompany.com/news/coca-cola-formula-is-at-the-world-of-coca-cola>.

² B. MYERS, *Even KFC's Head Chef Doesn't Know the Secret Recipe*, <https://www.thedailymeal.com/eat/kfc-secret-recipe-fried-chicken>.

³ Richtl.Parl. nr. 2016/943, 8 juni 2016 betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken daarvan, *Pb.L.* 15 juni 2016, afl. 157, 1-18. Vanaf nu Richtlijn Bedrijfsgeheimen of de Europese richtlijn.

⁴ Wet 30 juli 2018 betreffende de bescherming van bedrijfsgeheimen, *BS* 14 augustus 2018, 64584.

⁵ FEDERALE OVERHEIDSDIENST WERKGELEGENHEID, ARBEID EN SOCIAAL OVERLEG, *Update: Coronavirus: preventiemaatregelen en arbeidsrechtelijke gevolgen*, <https://werk.belgie.be/nl/nieuws/update-coronavirus-preventiemaatregelen-en-arbeidsrechtelijke-gevolgen> (Consultatie op 18 december 2020).

voorgaande doet je afvragen hoe het dan zit met de bescherming van bedrijfsgeheimen als ervan thuis uit wordt gewerkt.

Geldt de wet van 2018 voor mensen die thuis werken? Wat zijn nu precies bedrijfsgeheimen? Zijn er bepaalde zaken die hier niet onder vallen? Kunnen werkgevers iets doen om de bescherming van hun bedrijfsgeheimen alsnog te verzekeren? Hoe zit het als een werkgever ontdekt dat een werknemer inderdaad een bedrijfsgeheim heeft gedeeld met de partner, kan de werkgever juridisch dan iets ondernemen?

Met deze masterscriptie zal gepoogd worden om al het voorgaande te beantwoorden.

Onderzoeksvraag

Om de antwoorden te vinden, wordt in deze scriptie gebruik gemaakt van de volgende centrale vraag, namelijk wat is de impact van de Wet betreffende de bescherming van bedrijfsgeheimen op een werknemer die thuis werkt?

Deze centrale vraag zal in verscheidene subvragen opgesplitst en beantwoord worden om dan uiteindelijk een geheel te vormen.

De eerste subvraag betreft hoe de nieuwe wet inzake de bescherming van bedrijfsgeheimen eruitziet. Bijgevolg zal deze vraag in hoofdstuk 1 besproken worden. Als gevolg hiervan zal de tweede subvraag die onderzoek doet naar de achtergrond van deze wet in het volgende hoofdstuk behandeld worden. De derde subvraag neemt het begrip bedrijfsgeheimen zelf onder de loep en komt in hoofdstuk 3 aan bod. In dit hoofdstuk zal worden onderzocht hoe de nieuwe wet een bedrijfsgeheim definieert.

Nadat het algemeen kader is opgebouwd, zal in hoofdstuk 4 onderzocht worden wat op dit ogenblik de precieze impact is van de wet op werknemers die thuis werken. Deze subvraag zal dus het algemeen besproken kader toepassen om een antwoord te vinden hoe thuiswerkende werknemers getroffen worden door de wet. Dit hoofdstuk vormt aldus de kern van deze scriptie en is derhalve het meest omvattend. Om deze subvraag te beantwoorden, wordt eerst het verschil tussen de begrippen telewerken en thuiswerken besproken. Daarna zal gewerkt worden met hypothesen om aan te tonen wat voor impact de wet kan hebben op werknemers die thuis werken. Na dit deel zal onderzocht worden welke juridische stappen werkgevers kunnen nemen tegen inbreuken op hun bedrijfsgeheimen.

Het voorlaatste hoofdstuk peilt met de subvraag "Heeft de Wet Bedrijfsgeheimen zijn doel bereikt in het kader van telewerken?" of de wet daadwerkelijk bedrijfsgeheimen beschermt wanneer ervan thuis uit wordt gewerkt. Heeft de wet voor effectieve bescherming gezorgd of mist de wet zijn doel?

In het allerlaatste hoofdstuk ten slotte zullen door middel van de subvraag "Wat kan er beter aan de Wet Bedrijfsgeheimen in het kader van telewerken" aanbevelingen geformuleerd worden voor de wet. Om aanbevelingen te helpen opstellen, zal overigens een rechtsvergelijking plaatsvinden met Duitsland. De Duitse implementatiewet lijkt op bepaalde vlakken namelijk erg verschillend van de Belgische waardoor deze Duitse wet als inspiratiebron kan dienen.

Hoofdstuk I Hoe ziet de nieuwe wet eruit?

Alvorens te onderzoeken wat de impact is van de Wet Bedrijfsgeheimen op werknemers thuis, is het nodig om te beginnen bij het begin, namelijk de wet zelf. Het is immers niet mogelijk om de impact van een wetgevend instrument te onderzoeken als men niet bekend is met de inhoud van dergelijk instrument. Wat staat er nu eigenlijk in deze wet? Zorgt deze wet voor een nieuwe wet afzonderlijke wet of worden er artikels toegevoegd aan bestaande wetten?

I.A Wet betreffende de bescherming van bedrijfsgeheimen

Zoals reeds vermeld, is de Wet Bedrijfsgeheimen ontstaan ten gevolge van de omzetting van een Europese richtlijn uit 2016.⁶ De bespreking van deze richtlijn zelf zal aan bod komen in het volgende hoofdstuk dat de achtergrond van de wet bespreekt. Lidstaten van de Europese Unie krijgen meestal twee jaar de tijd om een richtlijn om te zetten.⁷ In het geval van de Europese richtlijn die de basis vormt van de Wet Bedrijfsgeheimen was het niet anders. Artikel 19 van de Richtlijn Bedrijfsgeheimen gaf lidstaten als uiterste datum 9 juni 2018 om de richtlijn om te zetten.

De officiële titel van de Wet Bedrijfsgeheimen bedraagt de naam Wet betreffende de bescherming van bedrijfsgeheimen. Deze wet werd afgekondigd op 30 juli 2018. De eigenlijke publicatie gebeurde op 14 augustus 2018. De inwerkingtreding zelf vond dan weer plaats op 24 augustus 2018. De wet voorzorg in artikel 44 dat de bepalingen van de wet onmiddellijk van toepassing waren bij de inwerkingtreding. Dit had dus tot gevolg dat de wet onmiddellijk toepasselijk was op rechtsfeiten die plaatsvonden na 24 augustus 2018. Bovendien voorzorg artikel 44 Wet Bedrijfsgeheimen in de toepassing van de bepalingen van de wet op rechtsfeiten die zich voor de inwerkingtreding hadden plaatsgevonden, maar die nog bleven voortduren na de inwerkingtreding van de wet. Er werd echter wel een uitzondering voorzien voor procedures die reeds aanhangig waren.⁸

Vermits de lidstaten tot 9 juni 2018 hadden om de richtlijn om te zetten en België de wet pas afkondigde op 30 juli 2018, was België in feite net te laat met de omzetting. Wanneer een lidstaat te laat is met het omzetten van een richtlijn, kan de Europese Commissie beslissen om een inbreukprocedure op te starten tegen de lidstaat in kwestie op grond van artikel 258 VWEU.⁹ Aangezien de Wet Bedrijfsgeheimen twee maanden na de omzettingsdeadline in werking is getreden, kan verondersteld worden dat België niet zal worden veroordeeld voor deze vertraging.

Wat betreft de inhoud van de Wet Bedrijfsgeheimen valt op dat de wet enkel bestaande wetgeving wijzigt. Er is dus geen werkelijk nieuwe afzonderlijke wet gecreëerd door de wetgever.¹⁰

De wijzigingen die door de Wet Bedrijfsgeheimen zijn teweeggebracht, zijn terug te brengen tot drie bestaande wetgevende instrumenten. De wet heeft namelijk wijzigingen aangebracht aan het

⁶ Richtl.Parl. nr. 2016/943, 8 juni 2016 betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken daarvan, *Pb.L.* 15 juni 2016, afl. 157, 1-18.

⁷ EUR LEX, *Richtlijnen van de Europese unie*, <https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=LEGISSUM:l14527> (consultatie op 5 februari 2021).

⁸ Art 44, lid 2 Wet Bedrijfsgeheimen.

⁹ HvJ 8 juli 2019 nr. C-543/17, ECLI:EU:C:2019:573, overweging 8; T. JORIS en S. VAN DER JEUGHT, "Hof van Justitie – 8 juli 2019", *RW* 2020, afl. 27, 1078-1079.

¹⁰ A. AERTS, "De arbeidsrechtelijke aspecten van de nieuwe Wet op de Bedrijfsgeheimen", *IRDI* 2018, 243.

Wetboek van economisch recht, aan het Gerechtelijk Wetboek en aan de Arbeidsovereenkomstenwet van 3 juli 1978.

I.B Wijzigingen aan het WER

De eerste wijzigingen die de Wet Bedrijfsgeheimen bewerkstelligde, zijn wijzigingen aan het Wetboek van economisch recht (WER vanaf hier en volgende). Deze veranderingen omvatten onder meer toevoegingen van nieuwe titels, van nieuwe artikelen, nieuwe hoofdstukken en nieuwe afdelingen in een aantal van de boeken van het WER. De Wet Bedrijfsgeheimen heeft vooral het WER aangepast. In de memorie van toelichting gaf de wetgever aan dat ervoor geopteerd werd om het grootste deel van de bepalingen inzake bedrijfsgeheimen onder te brengen in boek XI van het WER. Dit leek volgens de wetgever de meest geschikte plaats voor deze bepalingen, omdat boek XI gekenmerkt wordt door een ruim toepassingsgebied *ratione personae* en niet beperkt is tot B2C- of B2B-relaties.¹¹

I.C Wijzigingen aan het Gerechtelijk Wetboek

Buiten de grote aantal veranderingen aan het WER heeft de Wet Bedrijfsgeheimen tevens een tiental aanpassingen aan het Gerechtelijk Wetboek aangebracht.¹² De wijzigingen van het Ger.W. zijn gelijkend op die van het WER, namelijk ook hier zijn artikelen toegevoegd, bepalingen ingevoerd en bestaande artikelen gewijzigd.

I.D Wijzigingen aan de wet van 3 juli 1978 (Arbeidsovereenkomstenwet)

De Wet Bedrijfsgeheimen heeft slechts 1 artikel van de Arbeidsovereenkomstenwet gewijzigd, met name artikel 17 waarin bepaling 3^o vervangen is.¹³ Dit artikel bevat een aantal verplichtingen voor een werknemer. Door deze wijziging is voornamelijk deeltje a van de bepaling aangepast. Vroeger verplichtte dit deel een werknemer om zich ervan te onthouden om zowel gedurende zijn overeenkomst als na het beëindigen ervan fabrieksgeheimen, zakengeheimen of geheimen in verband met persoonlijke of vertrouwelijke aangelegenheden bekend te maken waarvan hij kennis kan hebben door de uitoefening van zijn beroep. Het huidige aangepaste deel verplicht een werknemer om zich zowel tijdens zijn overeenkomst als na de beëindiging ervan te onthouden om bedrijfsgeheimen in de zin van artikel I.17/1, 1^o WER waarvan hij kennis kan krijgen door de uitoefening van zijn beroepsarbeid op onrechtmatige wijze te verkrijgen, te gebruiken of openbaar te maken in de zin van artikel XI.332/4 WER. Daarnaast verplicht het artikel een werknemer ook om zich te onthouden zowel gedurende de overeenkomst als na het beëindigen ervan om geheimen in verband met persoonlijke of vertrouwelijke aangelegenheden waarvan hij kennis kan krijgen in de uitoefening van zijn beroep bekend te maken. Deze aanpassing heeft artikel 17 AOW dus geüpdatet naar de nieuwe wetgeving in verband met bedrijfsgeheimen. Hoewel de nieuwe versie van artikel 17, 3^o, a niet meer spreekt over fabrieksgeheimen of zakengeheimen dient te worden benadrukt dat deze begrippen onder het begrip bedrijfsgeheim vallen.¹⁴ Voorts dient te worden opgemerkt dat de eerder besproken bepalingen uit het WER die door de Wet Bedrijfsgeheimen zijn gewijzigd en/of toegevoegd tevens van toepassing zijn op een arbeidsrelatie, onverminderd artikel 17, 3^o, a. Dit wil

¹¹ Wetsontwerp betreffende de bescherming van bedrijfsgeheimen, *Parl.St.* Kamer 2017-2018, nr. 54-3154/001, 8-9.

¹² Ger.W. vanaf nu.

¹³ Artikel 43 Wet Bedrijfsgeheimen; Wet 3 juli 1978 betreffende de arbeidsovereenkomsten (Arbeidsovereenkomstenwet/AOW), *BS* 22 augustus 1978, 9277.

¹⁴ Wetsontwerp betreffende de bescherming van bedrijfsgeheimen, *Parl.St.* Kamer 2017-2018, nr. 54-3154/001, 33-34.

zeggen dat een werknemer alle bepalingen inzake de bescherming van bedrijfsgeheimen uit het WER moet naleven. Hij mag aldus geen bedrijfsgeheimen openbaar maken en hij mag ze ook niet op onrechtmatige wijze verkrijgen of gebruiken.¹⁵ Een laatste opmerking gaat over de situatie waarin een werknemer op de hoogte komt van het bestaan van een bedrijfsgeheim. Als een werknemer slechts op de hoogte is van het bestaan van een bedrijfsgeheim door de uitoefening van zijn beroep, maar geen kennis heeft van de inhoud van dit geheim, dan vormt dit uiteraard geen schending van het bedrijfsgeheim.¹⁶

I.E Overige wijzigingen

Het allerlaatste artikel van de Wet Bedrijfsgeheimen was een overgangsregeling.¹⁷ Hierin werd bepaald in het eerste lid dat alle bepalingen van de wet onmiddellijk van toepassing waren met de inwerkingtreding van de wet, met behoud evenwel van de rechten die bij de inwerkingtreding ervan zijn verworven. Aangezien de wet van kracht werd op 24 augustus 2018, moesten alle bepalingen vanaf toen toepassing vinden. Met het laatste deel van de bepaling "*met behoud evenwel van de rechten die bij de inwerking ervan zijn verworven*" bedoelde de wetgever dat de rechtsgevolgen die zich tot aan de inwerkingtreding van de Wet Bedrijfsgeheimen hebben voorgedaan met toepassing van de vroegere wet, behouden blijven.¹⁸ In het tweede lid werd bepaald dat alle gerechtelijke procedures die reeds voor de inwerkingtreding waren ingesteld, afgehandeld moesten worden volgens de bepalingen die van toepassing waren op het moment dat de procedure werd ingesteld. Dit is logisch gelet op het principe van de rechtszekerheid.

¹⁵ H. VANHEES, "De nieuwe wettelijke regeling betreffende de bescherming van bedrijfsgeheimen", *RW* 2018-2019, afl. 42, 1659.

¹⁶ Wetsontwerp betreffende de bescherming van bedrijfsgeheimen, *Parl.St.* Kamer 2017-2018, nr. 54-3154/001, 35.

¹⁷ Artikel 44 Wet Bedrijfsgeheimen.

¹⁸ Wetsontwerp betreffende de bescherming van bedrijfsgeheimen, *Parl.St.* Kamer 2017-2018, nr. 54-3154/001, 35.

Hoofdstuk II Wat is de achtergrond van de nieuwe wet?

Om de wetgeving omtrent bedrijfsgeheimen beter te kunnen begrijpen, wordt in dit hoofdstuk uiteengezet hoe en waarom de Wet Bedrijfsgeheimen er is gekomen. Zonder de achtergrond te kennen, is het immers niet mogelijk om het gehele plaatje te begrijpen. Zoals vermeld zou de Wet Bedrijfsgeheimen er niet gekomen zijn zonder de Richtlijn Bedrijfsgeheimen. Bijgevolg is het niet meer dan logisch om deze richtlijn en zijn voorgeschiedenis van dichterbij te bekijken.

II.A Voorgeschiedenis

De Europese Unie sprak voor het eerst over het thema bedrijfsgeheimen in de EU 2020-strategie. Deze strategie was een langetermijnstrategie van de EU die erop gericht was om een duurzame en sterke economie met veel werkgelegenheid uit te bouwen. Het was een vervolg op de Lissabon-strategie die liep van 2000 tot 2010. Net zoals de Lissabon-strategie, liep de EU 2020-strategie voor een periode van tien jaar. In het kader hiervan heeft de Europese Commissie vijf meetbare streefdoelen opgesteld op het gebied van onderwijs, arbeid, klimaatverandering en energie, onderzoek & ontwikkeling en armoedevermindering.¹⁹ Het was binnen deze context dat de Europese Commissie haar doel bekend maakte in de vorm van een mededeling om een functionerende eengemaakte markt voor intellectuele-eigendomsrechten tot stand te brengen en te bevorderen.²⁰ In deze mededeling somde de Europese Commissie een lijst van beleidsinitiatieven op welke zij het belangrijkste vond voor komende uitdagingen en hierin werden ook bedrijfsgeheimen en productpiraterij opgenomen. De Commissie merkte op dat er aanzienlijke verschillen bestonden in de nationale wetgevingen inzake het toepassingsgebied en de aard van bescherming van bedrijfsgeheimen. Zij merkte tevens op dat er significante verschillen waren betreffende de beschikbare rechtsmiddelen en oplossingen. Dit allemaal had als gevolg dat er verschillende beschermingsniveaus bestonden van bedrijfsgeheimen doorheen de EU. Verder benadrukte de Commissie dat bedrijfsgeheimen de laatste jaren kwetsbaarder waren geworden en dat deze kwestie in het algemeen enorm complex was. Hierdoor kwam de Commissie tot de conclusie dat ze uitgebreid bewijsmateriaal moest verzamelen en zich verder moest beraden vooraleer ze een positie zou innemen betreffende mogelijke toekomstige maatregelen.²¹

Om zich verder te informeren duidde de Commissie in 2011 Hogan Lovells aan om een rechtsvergelijkende studie uit te voeren tussen de 27 lidstaten van de EU inzake de bescherming van bedrijfsgeheimen.²² Uit deze studie kwam voort dat de bescherming van bedrijfsgeheimen enorm varieerde van lidstaat tot lidstaat en dat er verscheidene lidstaten waren met gefragmenteerde

¹⁹ COM(2010)2020, *EUROPA 2020 - Een strategie voor slimme, duurzame en inclusieve groei*, 52010DC2020, <https://www.eumonitor.nl/9353000/1/j9vvik7m1c3gyxp/vio0dsna8gzx>; EUROPA NU, *EU 2020-strategie*, https://www.europa-nu.nl/id/vicyffri83lm/eu_2020_strategie (consultatie op 4 januari 2021).

²⁰ COM(2011)287, *Eengemaakte markt voor intellectuele-eigendomsrechten - Creativiteit en innovatie bevorderen met het oog op economische groei, kwaliteitsjobs en eerste klasproducten en -diensten in Europa*, Brussel, 24 mei 2011, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0287:FIN:NL:PDF>.

²¹ COM(2011)287, *Eengemaakte markt voor intellectuele-eigendomsrechten - Creativiteit en innovatie bevorderen met het oog op economische groei, kwaliteitsjobs en eerste klasproducten en -diensten in Europa*, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0287:FIN:NL:PDF>, 18.

²² Hogan Lovells is een internationaal advocatenkantoor dat kantoren heeft in Amerika, Europa en Azië; <https://www.hoganlovells.com/en/about-us>.

wetgeving omtrent dit onderwerp. Bovendien toonde deze studie aan dat het algemeen niveau van bescherming van bedrijfsgeheimen in de Europese Unie ontzettend laag was.²³

Als gevolg van deze resultaten besloot de Europese Commissie op 29 juni 2012 een conferentie in Brussel te organiseren inzake de problematische bescherming van bedrijfsgeheimen. Deze conferentie had als doel om de rol en het belang van bedrijfsgeheimen voor de Europese economie te bespreken en te discussiëren hoe bedrijfsgeheimen mogelijk beschermd konden worden. Daarnaast wilde de Europese Commissie deze conferentie tevens gebruiken om de standpunten in te winnen van belanghebbenden over een online industriële enquête die later in 2012 naar o.a. bedrijven en professionals gestuurd zou worden.²⁴ Met deze enquête wilde de Europese Commissie peilen naar de mening van bedrijven over de bescherming van bedrijfsgeheimen. Wat dachten zij van het niveau van bescherming? Wilden ze dat de Europese Unie actie ondernam om deze bescherming te verbeteren? In totaal vulde slechts 386 respondenten deze enquête in.²⁵

Slechts een jaar later werd opnieuw een studie gepubliceerd over bedrijfsgeheimen op vraag van de Europese Commissie. Deze studie deed onderzoek naar de juridische en economische structuur van de bescherming van bedrijfsgeheimen in de Europese Unie. Daarnaast bevatte deze studie ook de resultaten van een nieuwe enquête die beantwoord was door 537 bedrijven van verschillende groottes. Op grond van deze studie en enquête werd gepleit voor geharmoniseerde wetgeving voor de bescherming van bedrijfsgeheimen voor de gehele Europese unie.²⁶

²³ H. LOVELLS, *Report on trade Secrets for the European Commission*, London, 23 september 2011, http://publications.europa.eu/resource/cellar/068c999d-06d2-4c8e-a681-a4ee2eb0e116.0001.02/DOC_1, 42-43.

²⁴ COM (2012), *REPORT EUROPEAN COMMISSION CONFERENCE OF 29 JUNE 2012 "TRADE SECRETS: SUPPORTING INNOVATION, PROTECTING KNOW-HOW"*, <https://ec.europa.eu/docsroom/documents/14836?locale=fr>;

²⁵ EUROPESE COMMISSIE, *Public consultation on the protection against misappropriation of trade secrets and confidential business information*, https://ec.europa.eu/growth/content/public-consultation-protection-against-misappropriation-trade-secrets-and-confidential_nl (consultatie op 5 februari 2021).

²⁶ X, *Study on Trade Secrets and Confidential Business Information in the Internal Market*, April 2013, MARKT/2011/128/D, <https://ec.europa.eu/docsroom/documents/14838/attachments/1/translations/en/renditions/pdf>, 151-153.

II.B De richtlijn

Uiteindelijk besloot de Europese Commissie gebaseerd op alles wat de afgelopen jaren was gebeurd om op 28 november 2013 een eerste richtlijnvoorstel te publiceren betreffende de bescherming van bedrijfsgeheimen.²⁷ In combinatie met dit richtlijnvoorstel werd tevens een impact assessment en een implementatieplan gepubliceerd.²⁸ In deze impact assessment werd het doel van het richtlijnvoorstel van de Europese Commissie duidelijk gemaakt, met name het verbeteren van de effectiviteit van de legale bescherming van bedrijfsgeheimen binnen de interne markt. Verder werd gesteld dat de Europese Commissie dit onder andere hoopt te doen door lidstaten de mogelijkheid te geven om toegang te bieden aan hun inwoners tot verhaalsmogelijkheden wanneer er sprake is van misbruik, regels te implementeren die bedrijfsgeheimen beschermen tijdens juridische geschillen en derden doeltreffender af te schrikken van het exploiteren van bedrijfsgeheimen. Bovendien zou dit het concurrentievermogen van Europese bedrijven kunnen verbeteren in de globale economie.²⁹

Dit voorstel werd in 2014 besproken in de Europese Raad en nadat er onderhandelingen plaatsvonden tussen de Europese Raad en de Europese Commissie werd een compromistekst gepubliceerd dat gezien konden worden als het tweede voorstel van de richtlijn.³⁰

Op dit tweede voorstel kwamen een aantal negatieve reacties door enkele organisaties. Een van die organisaties was de Council of Bars and Law Societies of Europe. Zij stelden dat de voorgestelde maatregel die het mogelijk maakt om bedrijfsgeheimen te bewaren tijdens juridische geschillen het recht op een eerlijk proces in gevaar zouden kunnen brengen. Hierdoor zou een rechter partijen toegang kunnen verbieden tot elk document die een bedrijfsgeheim bevat waardoor artikel 6 van het Europees Verdrag voor de Rechten van de Mens mogelijk ondermijnd zou kunnen worden.³¹

De negatieve reacties waren terug te brengen tot één probleem, namelijk dat bedrijven door deze richtlijn te veel rechten zouden krijgen om hun bedrijfsgeheimen te beschermen ten koste van anderen.³²

²⁷ Voorstel (Comm.) voor een richtlijn van het Europees Parlement en de Raad betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken daarvan, 28 november 2013, COM(2013)813 def - 2013/0402(COD).

²⁸ COMMISSION STAFF WORKING DOCUMENT, *Implementation Plan Accompanying the document Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*, 28 november 2013, SWD(2013) 493 final; COMMISSION STAFF WORKING DOCUMENT, *IMPACT ASSESSMENT Accompanying the document Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*, 28 november 2013, SWD(2013) 471 final.

²⁹ COMMISSION STAFF WORKING DOCUMENT, *IMPACT ASSESSMENT Accompanying the document Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*, 28 november 2013, SWD(2013) 471 final, 6-8.

³⁰ RAAD VAN EUROPA, *Persmededeling Concurrentievermogen (Interne Markt, Industrie, Onderzoek en Ruimtevaart)*, 26 mei 2016, 10226/14; R. DE VREY, "De totstandkoming van de Richtlijn Bedrijfsgeheimen", *IRDI* 2016, afl. 2, 146-147.

³¹ CCBE, *CCBE position European Commission proposal for a Directive on the protection of undisclosed know-how and business information (trade secret) against their unlawful acquisition, use and disclosure (COM(2013) 813 final, 2013/0402 (COD))*, https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/DEONTOLOGY/DEON_Postion_Papers/EN_DEON_20141031_CCBE_Trade_secrets.pdf.

³² EPHA, *Joint statement | EU trade secrets directive threat to health, environment, free speech and worker mobility*, <https://epha.org/joint-statement-eu-trade-secrets-directive-threat-to-health-environment-free-speech-and-worker-mobility/> (consultatie op 5 februari 2021); EFJ, *Trade secrets versus public interest: Open*

Ten slotte zag de definitieve compromistekst het licht en werd het compromis aangenomen door het Europees Parlement op 14 april 2016 en werd het op 26 mei 2016 aangenomen door de Europese Raad.³³ Op 8 juni 2016 vond de ondertekening plaats. De richtlijn met de naam "Richtlijn (EU) 2016/943 van het Europees Parlement en de Raad van 8 juni 2016 betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken daarvan" werd vervolgens op 15 juni 2016 in het Publicatieblad van de Europese Unie gepubliceerd. De inwerkingtreding volgde een maand later op 5 juli 2016. Artikel 19.1 van de Richtlijn Bedrijfsgeheimen gaf - zoals vermeld in hoofdstuk I - de lidstaten tot 9 juni 2018 om de richtlijn om te zetten en te implementeren in hun nationale wetgeving.³⁴

Artikel 1 van de Richtlijn Bedrijfsgeheimen toont aan dat de richtlijn van minimumharmonisatie uitgaat, wat betekent dat lidstaten een hoger niveau van bescherming mogen aanbieden indien ze dit willen. Echter, ze kunnen dit enkel doen als ze hierbij de naleving van bepaalde voorziene artikelen uit de richtlijn waarborgen. Op het gebied van de voorziene artikelen in art 1, 1, lid 2 gaat de richtlijn dus uit van maximumharmonisatie.

Voorts, staat te lezen in artikel 1, 2 dat de richtlijn enkele zaken niet belemmert. Een daarvan betreft de uitoefening van het recht op vrijheid van meningsuiting waarbij ook de vrijheid en het pluralisme van de media geëerbiedigd wordt door de richtlijn. De tweede uitdrukkelijke en opmerkelijke, neergeschreven "uitzondering" is inzake de mogelijkheid om bedrijfsgeheimen openbaar te maken aan administratieve of rechterlijke instanties wanneer dit nodig is voor de uitvoering van taken van deze instanties om redenen van algemeen belang. Het feit dat de richtlijn deze twee zaken onverlet laat lijkt tegemoet te komen aan de eerder geuite kritiek op het tweede richtlijnvoorstel door verschillende organisaties.

Als laatste stelt artikel 1, 3 dat de richtlijn niet gebruikt mag worden om de mobiliteit van werknemers te beperken waarbij de richtlijn enkele bijzonderheden met betrekking tot die mobiliteit aankaart. Zo wordt bepaald in artikel 1, 3, b) dat de richtlijn geen enkele grond biedt om werknemers te beperken in het gebruiken van vaardigheden en ervaringen die zij tijdens de normale uitoefening van hun functie op een eerlijke wijze hebben verkregen.

letter to European institutions, <https://europeanjournalists.org/blog/2015/10/13/trade-secrets-versus-public-interest-open-letter-to-european-institutions/> (consultatie op 5 februari 2021).

³³ EUR LEX, *Procedure 2013/0402/COD*, <https://eur-lex.europa.eu/legal-content/NL/HIS/?uri=CELEX:32016L0943>.

³⁴ EUR LEX, *Document 32016L0943 – Datums*, <https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX%3A32016L0943> (consultatie op 7 februari 2021); *Supra* Hoofdstuk I.A Wet betreffende de bescherming van bedrijfsgeheimen.

Hoofdstuk III Bedrijfsgeheimen

In dit hoofdstuk komt het begrip bedrijfsgeheimen zelf aan bod. Wat dient nu in feite verstaan te worden onder dit begrip? Voorziet de Belgische wet een ruime definitie of is het begrip slechts in zeer uitzonderlijke omstandigheden toepasselijk? Waaraan moet informatie voldoen om te kunnen spreken van het begrip? Daarnaast wordt onderzocht wanneer iemand een houder van een bedrijfsgeheim is. Kan iedereen dit zomaar zijn of zijn er strikte vereisten die vervuld moeten worden? Het laatste wat in dit hoofdstuk behandeld wordt, is de vraag of er dankzij de Wet Bedrijfsgeheimen een nieuw intellectueel eigendomsrecht is gecreëerd.

III.A Het begrip bedrijfsgeheimen

Om te weten wanneer er sprake is van het begrip bedrijfsgeheim heeft de richtlijn een definitie voorzien. Deze definitie is letterlijk gekopieerd van artikel 39, 2 van de TRIPS-Overeenkomst.³⁵ De Belgische Wet Bedrijfsgeheimen heeft op zijn beurt deze definitie letterlijk overgenomen en ingevoegd in artikel I.17/1, 1° WER.

De definitie gaat als volgt: "*Voor de toepassing van boek XI, titels 8/1, 9/1 en 10, hoofdstuk 4/1, gelden de volgende definities: 1° bedrijfsgeheim: informatie die aan de volgende cumulatieve voorwaarden voldoet: a) ze is geheim in die zin dat zij, in haar geheel dan wel in de juiste samenstelling en ordening van haar bestanddelen, niet algemeen bekend is bij of gemakkelijk toegankelijk is voor personen binnen de kringen die zich gewoonlijk bezighouden met de desbetreffende soort informatie; b) ze bezit handelswaarde omdat zij geheim is; c) ze is door de persoon die rechtmatig daarover beschikt onderworpen aan redelijke maatregelen, gezien de omstandigheden, om deze geheim te houden;*".

De Europese wetgever specificeerde in overweging 14 van de Richtlijn Bedrijfsgeheimen dat deze definitie betrekking moet hebben op bedrijfsinformatie, knowhow en technologische informatie wanneer er zowel sprake is van een legitiem belang bij het vertrouwelijk houden ervan als ook een legitieme verwachting is ten aanzien van het bewaren van deze vertrouwelijkheid. Tevens dient te worden vermeld dat de Belgische wetgever met deze definitie informatie viseert die geheimen van de fabriek en fabrieksgeheimen omvatten. Volgens vaste rechtspraak dient onder het begrip fabrieksgeheim de knowhow en de technische handelwijzen te worden verstaan die een technisch voordeel opleveren en die ten aanzien van concurrenten een superioriteit opleveren waardoor een economisch voordeel wordt geboden.³⁶

Opdat de definitie en dus het begrip bedrijfsgeheim van toepassing zou zijn, moeten er aan drie constitutieve elementen cumulatief voldaan zijn.

Ten eerste moet het gaan om informatie die geheim is. De bepaling voorziet zelf wanneer informatie geheim is. Namelijk, zo wordt gesteld dat de informatie in haar geheel of in een juiste samenstelling en ordening van haar bestanddelen niet algemeen bekend is of gemakkelijk toegankelijk is voor

³⁵ Artikel 2, 1 Richtlijn Bedrijfsgeheimen; Wereldhandelsorganisatie (WTO) Overeenkomst inzake de handelsaspecten van de intellectuele eigendom (TRIPS) van 15 april 1994, https://www.wto.org/english/docs_e/legal_e/27-trips.pdf.

³⁶ Wetsontwerp betreffende de bescherming van bedrijfsgeheimen, *Parl.St.* Kamer 2017-2018, nr. 54-3154/001, 12-13; Cass. 27 september 1943, *Pas.* 1943, I, 358.

personen binnen kringen die zich gewoonlijk bezighouden met de desbetreffende soort informatie. Dus het kan gaan om een combinatie van elementen die niet algemeen bekend is die ervoor zorgt dat de informatie geheim wordt. Verder moet het informatie betreffen die slechts toegankelijk is voor een beperkt aantal personen. Hieruit dient besloten te worden dat alledaagse informatie niet onder de definitie valt, aangezien dit wél algemeen bekende informatie is en makkelijk toegankelijk is.³⁷ Een nuance hierbij is wel dat algemene kennis een bestanddeel kan uitmaken van een geheim als de combinatie van de bestanddelen waarvan deze algemene kennis uitmaakt niet algemeen bekend is of makkelijk toegankelijk is voor personen binnen kringen die zich gewoonlijk bezighouden met dergelijke soort informatie.³⁸

Vervolgens mag het dus niet om informatie gaan die bijvoorbeeld gemakkelijk toegankelijk is voor vakexperten, want van deze personen kan immers verwacht worden dat zij zich bezighouden met dergelijke informatie. Gaat het daarentegen om informatie die niet gekend is door deze experts wegens een beperkte toegang tot deze informatie en een gebrek aan algemene bekendheid van deze informatie, wel dan zou het wel eens om geheime informatie kunnen gaan.³⁹ Als voorbeeld van dergelijke informatie kan dan gedacht worden aan kennis over prijslijsten of klantenlijsten die slechts door een select groepje mensen binnen een onderneming gekend is.⁴⁰

Het volgende element dat vervuld moet zijn, is dat de informatie handelswaarde moet bezitten doordat ze geheim is. Deze handelswaarde kan feitelijk of potentieel zijn. Dit wil zeggen dat de informatie een concurrentieel voordeel oplevert voor de houder van deze informatie. Met andere woorden de informatie moet dienstig zijn voor de houder. Wat tot gevolg heeft dat deze informatie geld waard is en waardevol zou kunnen zijn voor concurrenten.⁴¹ De Richtlijn Bedrijfsgeheimen zelf gaf als voorbeeld aan dat wanneer deze informatie onrechtmatig verkregen werd, gebruikt werd of openbaar werd gemaakt dat dit schadelijk zou kunnen zijn voor de belangen van de houder van die informatie, omdat hierdoor afbreuk gedaan zou worden aan het concurrentievermogen, de financiële of zakelijke belangen, de strategische positie of het wetenschappelijk en technisch potentieel van die persoon.⁴² Hierdoor kan geconcludeerd worden dat de houder van de informatie dus – zoals bepaald in de eerder vermelde overweging 14 – een legitiem belang zou hebben om de informatie vertrouwelijk te houden. Buiten het voorbeeld uit deze overweging zijn er geen elementen vermeld aan de hand waarvan de handelswaarde van informatie kan worden beoordeeld. In de rechtsleer omtrent de Belgische Wet Bedrijfsgeheimen werden volgende elementen aangereikt waarmee de handelswaarde beoordeeld kon worden: licenties die werden afgesloten voor het gebruik van bepaalde informatie; onderzoeks- en ontwikkelingskosten die werden gemaakt voor het gebruik van bepaalde informatie en de ouderdom van de informatie.⁴³ Het laatste element betreffende de ouderdom van de informatie is gebaseerd op vaste rechtspraak van het Hof van Justitie van de

³⁷ Overweging 14 Richtlijn Bedrijfsgeheimen.

³⁸ C. CLAEYS, "Bescherming van bedrijfsgeheimen. Nieuwe Regeling", *NJW* 2019, afl. 396, 101.

³⁹ T. ROBRECHTS en M. VAN MEERBEECK, "De Belgische Wet Bedrijfsgeheimen een algemeen overzicht", *IRDI* 2018, afl. 3-4, 185-186.

⁴⁰ C. CLAEYS, "Bescherming van bedrijfsgeheimen. Nieuwe Regeling", *NJW* 2019, afl. 396, 100-101.

⁴¹ Voorz. Orb. Brussel 12 maart 2020, *ICIP*, 2020/2, 576; T. ROBRECHTS en M. VAN MEERBEECK, "De Belgische Wet Bedrijfsgeheimen een algemeen overzicht", *IRDI* 2018, afl. 3-4, 186.

⁴² Overweging 14 Richtlijn Bedrijfsgeheimen.

⁴³ L. DEVROE, D. PHILIPPE en T. VAN NOYEN, "Protection des secrets d'affaires – Analyse de la loi du 30 juillet 2018 transposant la directive (UE) 2016/943", *DAOR* 2019, afl.132, 5; T. ROBRECHTS en M. VAN MEERBEECK, "De Belgische Wet Bedrijfsgeheimen: een algemeen overzicht", *IRDI* 2018, afl. 3-4, 186.

Europese Unie waarin gesteld werd dat bedrijfsinformatie geacht wordt haar vertrouwelijk karakter in principe te verliezen indien zij reeds vijf jaar oud is. Op dit principe wordt echter een uitzondering gemaakt als de partij die zich beroept op de vertrouwelijkheid hiervan kan aantonen dat de informatie nog steeds een wezenlijk onderdeel van haar commerciële positie of die van een derde is ondanks de ouderdom van deze informatie.⁴⁴

Het laatste constitutieve element dat aanwezig moet zijn om te kunnen spreken van een bedrijfsgeheim is dat de informatie onderworpen wordt aan redelijke maatregelen om deze informatie geheim te houden door degene die rechtmatig over de informatie beschikt. In feite komt dit element erop neer dat de houder de informatie wil beschermen én dat hij actief moet proberen om de informatie te beschermen. Hij of zij moet zich bijgevolg werkelijk inspannen om de informatie te beschermen. Omtrent het geheim houden benadrukte de Richtlijn Bedrijfsgeheimen dat er werkelijk een legitieme verwachting moet zijn ten aanzien van het bewaren van de geheimhouding.⁴⁵ Wat er daarentegen precies onder "redelijke" en onder "maatregelen" moet worden begrepen staat nergens bepaald. Zowel de Richtlijn Bedrijfsgeheimen als de Wet Bedrijfsgeheimen zelf zwijgen hierover. De Belgische wetgever gaf in zijn memorie van toelichting wel raad hoe dit mogelijk verstaan kan worden. De wetgever stelde dat deze redelijke maatregelen door de rechter beoordeeld zullen worden en dat deze maatregelen verschillende vormen kunnen aannemen. Hierbij gaf hij tevens enkele voorbeelden, met name contractuele bepalingen, virtuele of fysieke beveiligingsmechanismen, het vastleggen van een idee middels het i-depot bij het Benelux Bureau voor de Intellectuele Eigendom, enz.⁴⁶ Uiteindelijk zal het er aldus op neerkomen dat de rechter de genomen maatregelen zal moeten beoordelen in de concrete omstandigheden. Waren ze toereikend voor de omstandigheden waarin de houder zich bevond? Allicht wordt hier bedoeld op het feit dat niet elke houder van dergelijke informatie zich in dezelfde positie zal bevinden. Denk aan het verschil van middelen tussen een groot multinational bedrijf en een klein lokaal bedrijf. Van een grote multinational zal een rechter waarschijnlijk veel meer verwachten qua genomen maatregelen dan van een klein lokaal bedrijf.⁴⁷

Als alle bovenstaande elementen aanwezig zijn, kan er gesproken worden van een bedrijfsgeheim. Uit de bespreking van het voorgaande kan worden afgeleid dat de definitie ruim is waardoor een waaier aan informatie onder de noemer van bedrijfsgeheim kan vallen. In de rechtspraak werden de volgende zaken als bedrijfsgeheim geclassificeerd: technische procedés om conform de milieuwetgeving metaal op een zo efficiënt mogelijke manier te recycleren⁴⁸, en de werking en gedetailleerde informatie van productielijnen.⁴⁹ Vervolgens konden in de rechtsleer de volgende voorbeelden worden teruggevonden als bedrijfsgeheimen vermits de drie constitutieve elementen

⁴⁴ HvJ 14 maart 2017, nr. C-162/15, ECLI:EU:C:2017:205, Evonik Degussa/Commissie, punt 64; HvJ 19 juni 2018, nr. C-15/16, ECLI:EU:C:2018:464, Baumeister, punt 54.

⁴⁵ Overweging 14 Richtlijn Bedrijfsgeheimen.

⁴⁶ Wetsontwerp betreffende de bescherming van bedrijfsgeheimen, *Parl.St.* Kamer 2017-2018, nr. 54-3154/001, 12-13.

⁴⁷ T. ROBRECHTS en M. VAN MEERBEECK, "De Belgische Wet Bedrijfsgeheimen een algemeen overzicht", *IRDI* 2018, afl. 3-4, 185-186.

⁴⁸ Arbh. Antwerpen 12 september 2019, *IRDI* 2019, afl. 2, 163.

⁴⁹ Orb. Antwerpen 9 mei 2019, *RDC* 2020, afl. 3, 382.

vervuld zijn: financiële en/of technische informatie over de knowhow van een onderneming, bedrijfs- en productieprocessen, klantenlijsten, prijslijsten, commerciële informatie, enz.⁵⁰

Op zich lijkt een ruime definitie een positief iets, want zoals gezegd heeft dit tot gevolg dat een veelvoud aan informatie onder het begrip kan vallen. De keerzijde aan dergelijke ruime definitie is dat het niet altijd eenvoudig zal zijn om te determineren wanneer er wel of geen sprake is van een bedrijfsgeheim. Vooral als er gedacht wordt aan de ervaring en kennis die werknemers opdoen. Eerder werd al vermeld dat alledaagse informatie en opgedane ervaring en vaardigheden van een werknemer tijdens de normale uitoefening van zijn functie niet onder het begrip bedrijfsgeheim vallen.⁵¹ Maar wat als die opgedane kennis een bedrijfsgeheim vormt? Artikel XI.332/2 §2, 2° WER stelt immers dat de Wet Bedrijfsgeheimen niet mag worden opgevat als een grond om werknemers te beperken in het gebruik van vaardigheden en ervaringen die zij tijdens de normale uitoefening van hun functie op een eerlijke wijze hebben opgedaan. Hoe verhoudt deze bepaling zich met betrekking tot een situatie waarin een werknemer de kennis van een bedrijfsgeheim te weten is gekomen tijdens de normale uitoefening van zijn functie? Waar en hoe moet hier de grens worden getrokken? Aangezien de Richtlijn Bedrijfsgeheimen nog vrij nieuw is, is er op dit ogenblik nog geen rechtspraak over deze kwestie. Het zal aldus afwachten worden tot hierover rechtspraak verschijnt.

Verder moet worden opgemerkt dat de Europese wetgever (en de Belgische wetgever) geen nieuw intellectueel eigendomsrecht in het leven wilde roepen met de wetgeving betreffende bedrijfsgeheimen. Als gevolg hiervan heeft de houder van het bedrijfsgeheim géén exclusief verbodsrecht zoals de houder van een octrooi dat wel heeft.⁵² Om dit duidelijk te maken heeft de Belgische wetgever de titel van boek XI van het WER veranderd in "Intellectuele eigendom en bedrijfsgeheimen". Daarbovenop is er in boek XI een titel 8/1 ingevoerd door de Wet Bedrijfsgeheimen om de materieelrechtelijke bepalingen betreffende bedrijfsgeheimen in een afzonderlijke titel onder te brengen. Opnieuw om te benadrukken dat bedrijfsgeheimen geen exclusief recht of nieuw intellectueel eigendomsrecht creëren.⁵³

Er is nu al een aantal keren gesproken over de "houder van een bedrijfsgeheim", maar de definitie hiervan is nog niet ter sprake gekomen. Deze definitie staat mede opgesomd in artikel I.17/1, 2° WER: "*houder van het bedrijfsgeheim: iedere natuurlijke of rechtspersoon die rechtmatig over een bedrijfsgeheim beschikt*". Opnieuw is er gekozen voor een ruime definitie. In tegenstelling tot de definitie van bedrijfsgeheimen dienen er slechts twee elementen vervuld te zijn. Het moet gaan om een natuurlijke persoon of een rechtspersoon én deze natuurlijke persoon of rechtspersoon moet rechtmatig over het bedrijfsgeheim beschikken. Het element rechtmatig beschikken kan begrepen

⁵⁰ L. DEVROE, D. PHILIPPE en T. VAN NOYEN, "Protection des secrets d'affaires – Analyse de la loi du 30 juillet 2018 transposant la directive (UE) 2016/943", *DAOR* 2019, afl.132, 5; C. CLAEYS, "Bescherming van bedrijfsgeheimen. Nieuwe Regeling", *NJW* 2019, afl. 396, 101.

⁵¹ Zie ook art. XI.332/2§2, 2° WER.

⁵² Overweging 16 Richtlijn Bedrijfsgeheimen; Wetsontwerp betreffende de bescherming van bedrijfsgeheimen, *Parl.St.* Kamer 2017-2018, nr. 54-3154/001, 3, 5-6; Dit verbodsrecht houdt in dat de houder van een intellectueel eigendomsrecht de mogelijkheid om anderen te verbieden om hieromtrent bepaalde handelingen te stellen; P. GEENTJENS, "Van bits naar atomen: naar een opensourcemodel voor fysieke objecten?", *Jura Falc.* 2019, afl. 3, 481.

⁵³ Wetsontwerp betreffende de bescherming van bedrijfsgeheimen, *Parl.St.* Kamer 2017-2018, nr. 54-3154/001, 13; De reden die de Europese wetgever hiervoor gaf, was dat innovatie en concurrentie bevorderd moet worden, Overweging 1-4 Richtlijn Bedrijfsgeheimen; W. DERIJCKE en O. MALHERBE, "Vous me copierez cent fois... », l'article 871bis du Code judiciaire et la protection du secret d'affaires dans les procédures judiciaires", *JT* 2020, afl. 40, 838-840.

worden als de geheime informatie rechtmatig controleren. Met andere woorden, de persoon die beschermende maatregelen kan opleggen, is degene die rechtmatig zeggenschap heeft.⁵⁴ In de rechtsleer vragen sommige auteurs zich af of een licentienemer evenzeer houder van een bedrijfsgeheim kan zijn.⁵⁵ Dit is naar aanleiding van het voorstel van de Richtlijn Bedrijfsgeheimen waarin werd geconcludeerd op grond van het concept van de rechtmatigheid van de beschikking van het bedrijfsgeheim dat een licentiehouders tevens een houder kan zijn.⁵⁶ Het probleem is dat de Richtlijn Bedrijfsgeheimen deze stelling niet heeft overgenomen en de Belgische wetgever zwijgt hier evenzeer over, waardoor er onzekerheid bestaat op de vraag. Opnieuw is het hopen dat er over dit onderwerp rechtspraak ontwikkeld wordt, zodat deze vraag definitief beantwoord kan worden.

⁵⁴ H. VANHEES, "De nieuwe wettelijke regeling betreffende de bescherming van bedrijfsgeheimen", *RW* 2018-2019, afl. 42, 1645; V. CASSIERS, "La directive 2016/943/UE du 8 juin 2016 sur les secrets d'affaires", *JT* 2017, nr. 21, 389-390.

⁵⁵ H. VANHEES, "De nieuwe wettelijke regeling betreffende de bescherming van bedrijfsgeheimen", *RW* 2018-2019, afl. 42, 1645; T. ROBRECHTS en M. VAN MEERBEECK, "De Belgische Wet Bedrijfsgeheimen een algemeen overzicht", *IRDI* 2018, afl. 3-4, 186-187; V. CASSIERS, "La directive 2016/943/UE du 8 juin 2016 sur les secrets d'affaires", *JT* 2017, nr. 21, 390.

⁵⁶ Voorstel (Comm.) voor een richtlijn van het Europees Parlement en de Raad betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken daarvan, 28 november 2013, COM(2013)813 def - 2013/0402(COD), 8.

Hoofdstuk IV Wat is nu de impact van de wet op werknemers

thuis?

Nu het algemene kader van en rond de Wet Bedrijfsgeheimen is opgebouwd, wordt het tijd om de toepassing ervan onder de loep te nemen. Aangezien de wereld door de Covidcrisis verplicht werd zich aan te passen op allerlei vlakken in het dagelijkse leven – denk aan de verplichte mondkapen - vormde dit de perfecte gelegenheid om te onderzoeken welke impact en gevolgen de Wet Bedrijfsgeheimen heeft (gehad) voor mensen die verplicht werden om thuis te werken. Vermits de Covidcrisis “slechts” sinds vorig jaar begonnen is, zal het logischerwijze nog even duren voordat het duidelijk wordt voor bedrijven of het telewerken ervoor gezorgd heeft dat hun bedrijfsgeheimen gelekt zijn. De mogelijke rechtszaken die hieruit kunnen voortvloeien zullen bijgevolg pas na een aantal jaren voorkomen. Dit heeft tot gevolg dat er in dit hoofdstuk gewerkt zal worden met hypothesen.

Vooraleer de hypothesen uiteen worden gezet, moeten er eerst twee zaken nog worden opgeklaard. Ten eerste, het verschil tussen de begrippen thuiswerken en telewerken. Deze begrippen zijn geen synoniemen en mogen aldus niet met elkaar worden verward, hoewel dit regelmatig gebeurt. Ten tweede, op welke werknemers en werkgevers is de Wet Bedrijfsgeheimen nu van toepassing? Het is immers niet logisch om de bepalingen uit de Wet Bedrijfsgeheimen zomaar willekeurig toe te passen zonder dit vooraf na te gaan.

IV.A Thuiswerken en telewerken

Telewerk is een vorm van thuiswerken of huisarbeid. Huisarbeid en thuiswerken zijn dus wél synoniemen. De voornaamste wetgeving betreffende huisarbeid is de Arbeidsovereenkomstenwet. Huisarbeid staat gedefinieerd in artikel 119.1, paragraaf 1 van de Arbeidsovereenkomstenwet en gaat als volgt: *“Deze titel regelt de tewerkstelling van huisarbeiders die tegen loon arbeid verrichten onder het gezag van een werkgever, in hun woonplaats of op elke andere door hen gekozen plaats, zonder dat zij onder het toezicht of de rechtstreekse controle van deze werkgever staan. Naargelang het geval betreft het een arbeidsovereenkomst voor werklieden of een arbeidsovereenkomst voor bedienden, zoals geregeld door deze wet.”*

Kenmerkend aan huisarbeid zijn de volgende twee elementen uit de definitie. Met name, dat het werk wordt uitgevoerd door de werknemer thuis of een door hem gekozen plaats en het feit dat het werk door hem wordt uitgevoerd zonder onder rechtstreekse controle of toezicht te staan van de werkgever. Afhankelijk van de aard van het werk, zal de arbeidsovereenkomst inzake huisarbeid geregeld worden door een overeenkomst voor bedienden of voor werklieden en zal deze overeenkomst in principe onderworpen zijn aan de relevante wetgeving.⁵⁷ Als gevolg hiervan is huisarbeid mogelijk voor zowel bedienden als voor werklieden.

⁵⁷ De Arbeidsovereenkomstenwet bevat zowel de hoofdzakelijke regeling voor arbeidsovereenkomsten voor bedienden als werklieden. Deze wet is van toepassing op werknemers in de privésector en op persoonsleden in de publieke sector die niet aan een statuut onderworpen zijn.

Hoe past telewerken hier nu in? Telewerken werd voor het eerst geregeld in de collectieve arbeidsovereenkomst nr. 85.⁵⁸ Deze CAO voerde regels in voor telewerk voor de privésector. Later werd de Arbeidsovereenkomstenwet aangepast om afspraken te kunnen maken voor telewerkers in de publieke sector. Hierdoor zijn er drie categorieën van huisarbeiders mogelijk. De eerste twee categorieën betreft de huisarbeiders in de privésector die geen telewerkers zijn en de huisarbeiders in de privésector die wel telewerkers zijn. De laatste categorie zijn de telewerkers in de publieke sector.

Om te weten wanneer er sprake is van telewerken, moet er gekeken worden naar artikel 2 van CAO nr. 85. Dit artikel definieert telewerken als *“een vorm van organisatie en/of uitvoering van het werk waarin, met gebruikmaking van informatietechnologie, in het kader van een arbeidsovereenkomst werkzaamheden die ook op de bedrijfslocatie van de werkgever zouden kunnen worden uitgevoerd, op regelmatige basis en niet incidenteel buiten die bedrijfslocatie worden uitgevoerd”*. Dit artikel vermeldt uitdrukkelijk dat de CAO niet van toepassing is op mobiele telewerkers. Mobiele telewerkers zijn werknemers waarvoor mobiliteit noodzakelijk is voor de uitvoering van hun arbeidsovereenkomst, denk aan thuisverpleegsters of handelsvertegenwoordigers.⁵⁹

In deze definitie wordt gesproken over *“uitvoering van het werk op regelmatige basis”*. Iemand die op regelmatige basis telewerkt, noemt men een regelmatige of structurele telewerker. Een occasionele telewerker daarentegen verricht telewerk op incidentele basis en niet op regelmatige basis. Deze vorm van telewerken werd pas ingevoerd in 2017 door de Wet betreffende werkbaar en wendbaar werk. Deze wet is toepasselijk op werkgevers en werknemers waarop de Wet van 5 december 1968 betreffende de collectieve arbeidsovereenkomsten en de paritaire comités van toepassing is.⁶⁰ Een bijkomend verschil is dat er voor iedere structurele telewerker een schriftelijke overeenkomst moet zijn inzake het telewerken, terwijl dit geen verplichting is bij occasioneel telewerken. Als er al een overeenkomst bestaat, zal deze als een schriftelijk aanhangsel aan de arbeidsovereenkomst worden opgesteld.⁶¹

Wat maakt nu het verschil tussen de begrippen huisarbeid en telewerken? Vermits telewerken een vorm is van huisarbeid zijn ze nauw aan elkaar gelinkt, maar er zijn toch verschillen waarneembaar. Een van de belangrijkste verschillen is dat een telewerker gebruik maakt van informatietechnologie zoals uitdrukkelijk is voorzien in de definitie. Het tweede voornaamste verschil staat in verband met het eerste verschil en betreft het feit dat de werknemer onder toezicht staat van de werkgever. Door middel van de informatietechnologie kan de werkgever rechtstreekse controle uitoefenen op zijn werknemer terwijl een huisarbeider niet onder toezicht of rechtstreekse controle staat.⁶²

⁵⁸ CAO nr. 85/1 van 9 november 2005 betreffende het telewerk, gewijzigd door de collectieve arbeidsovereenkomst nr. 85 bis van 27 februari 2008, <http://www.cnt-nar.be/CAO-COORD/cao-085.pdf>; F. ROBERT en L. TASKIN, *Le télétravail à domicile*, Limal, Anthemis, 2020, 40-41.

⁵⁹ Commentaar bij artikel 2 van CAO nr. 85/1 van 9 november 2005 betreffende het telewerk, gewijzigd door de collectieve arbeidsovereenkomst nr. 85 bis van 27 februari 2008, <http://www.cnt-nar.be/CAO-COORD/cao-085.pdf>.

⁶⁰ Wet 5 maart 2017 betreffende werkbaar en wendbaar werk, *BS* 15 maart 2017, 35718; Wet van 5 december 1968 betreffende de collectieve arbeidsovereenkomsten en de paritaire comités, *BS* 15 januari 1969, 267.

⁶¹ Artikel 6, §1 CAO nr. 85; Cass. 5 oktober 2020, *Soc.Weg.* 2021, afl. 5, 21-24.

⁶² Arbh. Brussel 26 januari 2018, *Soc.Kron.* 2020, afl. 1, 21; Arbh. Brussel 2 juli 2019, nr. 2018/AB/278; L. HELLEMANS en E. KARREMAN, *Telewerk en huisarbeid*, Mechelen, Kluwer, 2018, 7-19.

De belangrijkste wetgevende instrumenten inzake telewerken in de privésector zijn CAO nr. 85 en de Wet betreffende werkbaar en wendbaar werk. Voor telewerkers in de publieke sector bestaan er enkele bepalingen in de Arbeidsovereenkomstenwet, maar deze wet heeft op dit vlak een subsidiair karakter.⁶³ Deze bepalingen van de Arbeidsovereenkomstenwet zijn slechts van toepassing als personen verbonden zijn door een arbeidsovereenkomst en indien er geen koninklijk besluit bestaat dat een bijzondere regeling voorziet voor de desbetreffende publieke dienst.⁶⁴

Door de coronacrisis is er sinds dit jaar echter een nieuw instrument bijgekomen omtrent telewerken, met name CAO nr. 149.⁶⁵ Deze CAO is van aanvullende aard wat o.a. af te leiden is uit artikel 3. Artikel 3 bepaalt namelijk dat de CAO van toepassing is op ondernemingen die op 1 januari 2021 nog geen regelingen hebben getroffen inzake structureel of occasioneel telewerk. Het staat de ondernemingen vrij om te kiezen hoe ze deze regels uitwerken, maar door deze CAO worden ze nu wel verplicht om een regeling uit te werken.

IV.B Op wie is de wet van toepassing?

In de Wet Bedrijfsgeheimen zelf is niks terug te vinden betreffende een specifiek toepassingsgebied van werknemers en werkgevers. In de Richtlijn Bedrijfsgeheimen is hieromtrent ook niks bepaald. De definities die wél in de richtlijn en de wet staan, bieden echter hulp. In de definitie van houder van het bedrijfsgeheim en inbreukmaker wordt er gesproken over iedere natuurlijke of rechtspersoon.⁶⁶ Door het gebruik van deze termen kan aldus worden geconcludeerd dat de wetgeving rond bedrijfsgeheimen op iedereen toepasselijk is die aan de vereisten van deze definities voldoet. Hierdoor kunnen werkgevers - ongeacht of het gaat om een rechtspersoon of een natuurlijke persoon - aldus houder zijn van een bedrijfsgeheim. Als gevolg hiervan kunnen hun telewerkende werknemers inbreukmakers zijn. Let wel, alhoewel er in de definitie van inbreukmaker sprake is van een natuurlijke of rechtspersoon, is dit niet het geval voor de begrippen werknemers en telewerkers. Deze begrippen omvatten enkel natuurlijke personen, maar dit terzijde.⁶⁷

IV.C Hypotheses

Welnu, aangezien de Covidcrisis ervoor heeft gezorgd dat telehuiswerk verplicht werd bij alle ondernemingen waar dit mogelijk is, heeft dit als resultaat dat er meer dan ooit wordt getelewerkt.⁶⁸ Hoewel dit zijn voordelen heeft voor zowel werkgevers als werknemers, heeft dit nochtans ook

⁶³ FEDERALE OVERHEIDSDIENST WERKGELEGENHEID, ARBEID EN SOCIAAL OVERLEG, *Huisarbeid – arbeiders in de publieke sector*, <https://werk.belgie.be/nl/themas/arbeidsovereenkomsten/bijzondere-arbeidsovereenkomsten/huisarbeid-en-telewerk/huisarbeid-1> (consultatie op 5 april 2021).

⁶⁴ Als voorbeeld van een koninklijk besluit in verband met telewerken, kan men kijken naar het Koninklijk Besluit 22 november 2006 betreffende het telewerk in het federaal administratief openbaar ambt, *BS* 1 december 2006, 66747.

⁶⁵ CAO nr. 149 van 26 januari 2021 betreffende aanbevolen of verplicht telewerk omwille van de coronacrisis, [http://www.cnt-nar.be/CAO-ORIG/cao-149-\(26.01.2021\).pdf](http://www.cnt-nar.be/CAO-ORIG/cao-149-(26.01.2021).pdf).

⁶⁶ Art I.17/1, 2° en 3° WER; *Supra* Hoofdstuk III – Het begrip bedrijfsgeheim voor de definitie van houder van het bedrijfsgeheim. De definitie van inbreukmaker komt in dit hoofdstuk zelf aan bod onder titel IV.C.4.

⁶⁷ Artikel 1 Arbeidsovereenkomstenwet, Artikel 1 Wet 12 april 1965 betreffende de bescherming van het loon der werknemers, *BS* 30 april 1965, 4710 (Loonbeschermingswet); Artikel 2, tweede streepje CAO nr. 85.

⁶⁸ Telehuiswerk is telewerken van thuis; FEDERALE OVERHEIDSDIENST WERKGELEGENHEID, ARBEID EN SOCIAAL OVERLEG, *Update: Coronavirus: preventiemaatregelen en arbeidsrechtelijke gevolgen – In welke ondernemingen is telehuiswerk verplicht?*, <https://werk.belgie.be/nl/nieuws/update-coronavirus-preventiemaatregelen-en-arbeidsrechtelijke-gevolgen> (consultatie op 5 april 2021); TELEWERKEN, *In cijfers – Enquête september 2020 bij 1500 werkenden: bijna 1 op 2 doet aan telewerken!*, <https://www.telewerken.be/in-cijfers/> (consultatie op 5 april 2021); SDWORX, *22% van de telewerkers werkt nog elke dag van thuis*, <https://www.sdworx.be/nl-be/pers/2020/2020-09-21-22-percent-van-de-telewerkers-werkt-nog-elke-dag-van-thuis> (consultatie op 5 april 2021).

nadelen. Een van de grootste nadelen aan het telewerken en de focus van deze scriptie gaat om het feit dat dit een enorm gevaar vormt voor gevoelige data van ondernemingen, waaronder de bedrijfsgeheimen gevallen.

Doordat er gebruik wordt gemaakt van telewerken, staan werknemers in principe onder rechtstreekse controle of toezicht van hun werkgever, maar dit toezicht is natuurlijk niet onbeperkt. Allereerst wordt het toezicht beperkt doordat de persoonlijke levenssfeer van de telewerker in acht moet worden genomen. Dit staat tevens uitdrukkelijk voorzien in artikel 9, §2 van CAO nr. 149 en artikel 14, derde lid van CAO nr. 85.⁶⁹ Daarnaast, is het realistisch niet mogelijk om iemand voortdurend te controleren. Laat staan om meer dan tien mensen tegelijkertijd te controleren. Bovendien is dit niet toegelaten door CAO nr. 149. De commentaar die bij artikel 9 is terug te vinden, stelt namelijk dat het niet de bedoeling is dat de werkgever een voortdurende controle uitvoert, maar dat hij op gepaste en proportionele wijze controle uitoefent. Tot slot eindigt de controle bij het einde van de werkuren, wat er daarna in het huis van de telewerker gebeurt, is een raadsel. Een laatste bedenking betreft de apparatuur die gebruikt wordt. Normaal gezien hebben de meeste bedrijven een beveiligd netwerk waarop enkel hun werknemers kunnen en zijn de apparaten die hier staan in principe ook beveiligd. Dit is een ander verhaal als een werknemer thuis werkt. Een werkgever kan een werknemer wel voorzien van bijvoorbeeld een werklaptop, maar als er geen gebruik wordt gemaakt van veilige tools zoals remote access die een persoon toelaten om op een veilige manier verbinding te maken met zijn computer op het werk of via een VPN-verbinding waardoor een werknemer van op afstand aan het bedrijfsnetwerk kan, dan doen dergelijke praktijken weinig voor de veiligheid van de bedrijfsgegevens.⁷⁰ Want wat houdt dan een werknemer tegen om zijn eigen persoonlijke laptop te gebruiken of eventueel die van zijn partner? Daarbij kan ook nog eens gedacht worden aan het netwerk bij de werknemer thuis. Is dit netwerk zelf wel beveiligd? Wat als de werknemer zijn wifi deelt met zijn buurman?

Er zijn dus ontzettend veel risico's voor de gevoelige data van bedrijven wanneer werknemers telewerken. Hieronder zullen enkele situaties geschetst worden die zich mogelijk kunnen voordoen of zich hebben voorgedaan bij de telewerkende werknemers in België tijdens de Coronacrisis. In deze situaties wordt verondersteld dat er telkens effectief sprake is van een bedrijfsgeheim waardoor de toetsing aan de constitutieve voorwaarden van een bedrijfsgeheim niet zal plaatsvinden. Deze keuze is gemaakt om de zaken niet te ingewikkeld te maken en omdat de nadruk van deze scriptie op het al dan niet schenden van bedrijfsgeheimen door telewerkers ligt. Daarna zal onderzocht worden of de desbetreffende werknemer of derde in de omschreven situatie bepalingen uit de Wet Bedrijfsgeheimen heeft geschonden. Om dit na te gaan, zal de werknemer of derde en zijn gedrag

⁶⁹ Artikel 14, derde lid CAO nr. 85 schrijft voor dat CAO nr. 81 van 26 april 2002 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische onlinecommunicatiegegevens toepasselijk is. Artikel 9, §2 CAO nr. 149 verwijst dan weer expliciet naar de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens en de wet van 10 september 2018 tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG.

⁷⁰ J. LORRE, *Sociale media en werkgeverscontrole*, Mechelen, Kluwer, 2012, 108-110; V. CASSIERS, "La protection des secrets d'affaires dans l'environnement numérique" in H. JACQUEMIN en B. MICHAUX (eds.), *Actualités en droit du numérique*, Limal, Anthemis, 2019, (99) 109.

getoetst worden aan de definitie van een inbreukmaker van een bedrijfsgeheim en aan de onrechtmatige handelingen uit de wet. Als laatste komt aan bod hoe de mogelijk getroffen werkgever kan optreden als zijn werknemer of een derde inderdaad een inbreukmaker blijkt te zijn.

IV.C.1 Hypothese 1 – Situatieschets

In deze situatie gaat het om een telewerkende man genaamd heer J die samenwoont met zijn vrouw L en hun twee kinderen. Sinds het begin van de Covidcrisis doet J aan telewerken voor zijn werkgever Q, een bedrijf dat zich specialiseert in het maken van heel populaire en lekkere speculaaskoekjes. J is een vrij hooggeplaatste werknemer waardoor hij toegang heeft tot aanzienlijk gevoelige bedrijfsgeheimen zoals het felbegeerde recept van de razend populaire speculaaskoekjes. J had van zijn werkgever Q een laptop gekregen zodat hij zeker overal kon telewerken, maar J werkt eigenlijk al vanaf het begin van de crisis vanaf zijn persoonlijke laptop thuis. Deze laptop heeft hij immers zelfgekozen en laten samenstellen waardoor J deze preferereert. Op het vlak van beveiliging staat het bedrijf Q nog wat achter, waardoor J zo goed als alles van zijn bedrijfscomputer op zijn persoonlijke laptop gekopieerd heeft. Hierdoor staat er ondertussen heel wat gevoelige informatie op deze laptop waaronder het recept van de speculaaskoekjes. Aangezien L zelf geen laptop heeft, maakt ze regelmatig gebruik van deze laptop met toestemming van J. Op een dag besluit ze dat ze speculaaskoekjes wil maken. Omdat ze geen zin heeft om urenlang naar een goed recept online te zoeken, besluit ze om het recept van het bedrijf Q te nemen dat tussen J zijn persoonlijke bestanden staat. De bestanden zijn immers niet beveiligd en haar kinderen zijn verzot op de speculaaskoekjes van het merk Q. Ten slotte om het haarzelf wat gemakkelijker te maken om het recept stap voor stap te kunnen volgen, beslist ze om het recept naar haar tablet te kopiëren via een usb-stick.

IV.C.2 Hypothese 2– Situatieschets

Deze situatie betreft een telewerkende vrouw L die alleen woont. L doet sinds het begin van de Coronacrisis aan telehuiswerken voor haar werkgever X, een bekende verzekeringsmaatschappij in België. L is een bedrijfsjurist die zich gespecialiseerd heeft in vennootschapsrechten waardoor haar cliënteel voornamelijk bestaat uit vennootschappen. Naast L heeft haar collega I zich ook gespecialiseerd in vennootschapsrechten waardoor beide vrouwen regelmatig samen dossiers behandelen. Ook tijdens het telewerken blijven ze samen aan dossiers werken. Hun laatste dossier heeft betrekking op de overname van een concurrent door hun eigen verzekeraar X. L is de leidinggevende van het dossier terwijl I haar slechts bijstaat. Dit gebeurt wel vaker vermits L ouder is en al een aantal jaren meer ervaring heeft. Hierdoor heeft I niet tot alles van het dossier toegang dat o.a. ook de bedrijfsgeheimen van zowel de verzekeringsmaatschappij X als van het bedrijf M bevat.

De vrouwen spreken een paar keer per week af via Google Meet om alles omtrent het dossier fatsoenlijk te kunnen bespreken. Tijdens hun laatste Google Meet vroeg I of L niet een aantal documenten kon mailen die ze vergeten was te kopiëren van haar bedrijfscomputer. Na hun sessie besluit L de documenten meteen door te sturen om haar collega verder te helpen. Een tijdje nadat ze de documenten had gemaïld naar I besefte L plots dat tussen deze documenten ook informatie zat waar I in principe geen toegang mag tot hebben zoals de bedrijfsgeheimen van beide bedrijven. Net als ze beslist om I te bellen met de vraag om de mail en de bijlagen ervan niet te lezen en te verwijderen, krijgt ze telefoon van een dolenthousiaste I. I wilde namelijk al lang weten welke

bedrijfsgeheimen haar eigen verzekeringsmaatschappij allemaal had en nu dankzij de mail weet ze eindelijk alles.

IV.C.3 Hypothese 3– Situatieschets

De laatste situatie heeft betrekking op S. S is een vrouwelijke ingenieur voor het bedrijf D dat zich gespecialiseerd heeft in het maken van videokaarten. Tegenwoordig zijn hun kaarten zo populair dat ze de vraag niet kunnen bijhouden. Om hieraan tegemoet te komen heeft D aan S en een paar van haar collega's gevraagd om een nieuw model van hun populairste videokaart te bedenken. Het bedrijf hoopt immers van de gelegenheid gebruik te maken om nog meer winst te behalen. S en haar collega's doen net zoals vele anderen sinds het begin van de Coronacrisis aan telewerken. Elke werknemer van het bedrijf waaronder dus ook S en haar collega's heeft een beveiligde werklaptop gekregen teneinde te verzekeren dat niemand de bedrijfsgeheimen waaronder de ontwerpen van de videokaarten zou kunnen bemachtigen. S is echter geen fan van alle veiligheidsprotocollen en heeft dan ook de functie van het inloggen met een wachtwoord uitgeschakeld. Ze ziet hier geen graten in, omdat ze haar laptop toch altijd bij zich heeft.

Hoewel S in principe thuis zou moeten werken, werkt ze af en toe stiekem ergens anders. S is het immers beu om altijd maar thuis te zitten, dus 1 keer in de week zoekt ze ergens een leuk plekje om te telewerken. Deze week besluit ze zich te installeren in het lokale stadspark. Het park is per slot van rekening altijd heel rustig en S is een echte natuurliefhebster. Tijdens het werken in het park wordt S gebeld door een van haar collega's die haar weet te vertellen dat hij een goed idee heeft voor een ontwerp. Hij vraagt haar dan ook om over een halfuurtje beschikbaar te zijn voor een Google Meet met alle andere collega's zodat ze zo snel mogelijk aan dit ontwerp kunnen werken. Uit angst om betrappt te worden door haar collega's besluit ze zo snel mogelijk alles in te pakken en naar huis te gaan. Wanneer ze echter thuiskomt en haar laptop wil pakken voor de Google Meet merkt S dat haar laptop niet in haar laptopvoes zit. Ze beseft dat ze zich door het haasten haar laptop heeft laten liggen in het park. Tevergeefs haast ze zich terug naar het park, maar eenmaal aangekomen, ziet ze haar laptop nergens meer liggen. Want toen S naar huis aan het keren was, heeft een toevallige wandelaar de laptop mee naar huis genomen. Het zou toch maar te gek zijn om een achtergelaten laptop te laten liggen in het gras. Wanneer de wandelaar thuis is, besluit hij uit nieuwsgierigheid een kijkje te nemen op de laptop. Bij het aanzetten van de laptop blijkt dat de laptop nog aanstaat. Als gevolg hiervan is alles blijven openstaan waaraan S aan het werken was in het park waaronder de huidige ontwerpen van de videokaarten van D. S wilde zich hierdoor namelijk laten inspireren om een nieuw ontwerp te kunnen bedenken.

IV.C.4 Inbreukmaker en onrechtmatige handelingen

Voordat de hypothesen getoetst worden, is het tijd om de relevante begrippen toe te lichten. Tot nu toe zijn de begrippen inbreukmaker en onrechtmatige handelingen louter terloops vermeld, maar ze zijn nog niet besproken, omdat ze hier pas werkelijk relevant zijn. Het enige begrip dat nog niet ter sprake is gekomen, is het begrip inbreukmakende goederen. In de hierboven beschreven situaties is er bewust voor gekozen om niet te werken met inbreukmakende goederen, omdat dit de situaties en de toetsing nog complexer zou maken. Daarbij is de essentie van deze scriptie gericht op telewerkers en hoewel zij in principe wel betrokken kunnen worden bij situaties met inbreukmakende goederen, leek dit een stap te ver en zou hierdoor te veel worden afgeweken van het

hoofdonderwerp. Daarom zal dit begrip slechts worden verklaard, maar verder niet gebruikt worden bij de toetsing van de geschetste situaties. Hetzelfde gaat op voor het begrip rechtmatige handelingen. De Wet Bedrijfsgeheimen maakt namelijk een onderscheid tussen rechtmatige en onrechtmatige handelingen. In de omschreven hypothesen is er echter bewust voor gekozen om geen rechtmatige handelingen te laten voorkomen. De reden hiervoor is om te vermijden dat de toetsingen van de situaties nodeloos complex zouden worden en om alles zo overzichtelijk mogelijk te houden. De begrippen inbreukmakende goederen en rechtmatige handelingen zullen dus kort aan het einde van het hoofdstuk aan bod komen. Hoewel ze niet relevant zijn voor de situaties in dit deel, is het nochtans belangrijk om te weten wat deze begrippen inhouden. Want rechtmatige handelingen en inbreukmakende goederen zouden in het dagelijkse bedrijfsleven waaronder het telewerken wel effectief kunnen voorkomen.

IV.C.4.1 Inbreukmaker

De definitie van het begrip inbreukmaker is terug te vinden in artikel I.17/1, 3° WER. Een inbreukmaker is iedere natuurlijke of rechtspersoon die een bedrijfsgeheim onrechtmatig gebruikt, openbaar heeft gemaakt of heeft verkregen.⁷¹ In deze definitie is niets bepaald of het gaat om een rechtstreekse of onrechtstreekse inbreukmaker of een derde-verkrijger, maar artikel XI.332/4, §3 en §4 WER komen hieraan tegemoet. Paragraaf 3 bepaalt immers dat als iemand op het moment van het gebruiken, openbaar maken of het verkrijgen wist of had moeten weten dat het bedrijfsgeheim dat direct of indirect was verkregen via een andere persoon die het bedrijfsgeheim op een onrechtmatige manier gebruikte, dat dit als onrechtmatig beschouwd moet worden. Paragraaf 4 vervolgens bevat een soortgelijke bepaling, maar dan in de context van het aanbieden, in de handel brengen of produceren van inbreukmakende goederen. Wanneer iemand deze activiteiten aanbiedt en gezien de omstandigheden wist of had moeten weten dat het bedrijfsgeheim onrechtmatig werd gebruikt, wordt dit opnieuw beschouwd als onrechtmatig. Deze laatste paragraaf laat zelfs toe om de invoerder van inbreukmakende goederen in België voor een rechter te dagen wanneer de eigenlijke inbreuk buiten België gebeurde. Bij zowel paragraaf 3 en 4 is er aldus een kennisvereiste.

IV.C.4.2 Onrechtmatige handelingen

Het laatste begrip dat moet worden verduidelijkt voordat kan worden overgegaan naar de toetsing van de hypothesen, is het begrip onrechtmatige handelingen. Dit is belangrijk om te weten, want de houder van een bedrijfsgeheim kan alleen optreden tegen onrechtmatige handelingen.

De onrechtmatige handelingen waartegen een houder van een bedrijfsgeheim of in casu een werkgever kan optreden, zijn neergelegd in artikel XI.332/4 WER. In dit artikel staan vier onrechtmatige situaties opgesomd. De eerste betreft de verkrijging van een bedrijfsgeheim wanneer dit gebeurt zonder toestemming van de houder en wanneer dit gebeurt door middel van bepaalde gedragingen.⁷² In paragraaf 1 zijn er twee bepalingen terug te vinden die vastleggen wanneer het verkrijgen van een bedrijfsgeheim zonder toestemming gebeurt in combinatie met een bepaald gedrag. Paragraaf 1, ten eerste stelt dat als de verkrijging gebeurt door middel van onbevoegde toegang, het zich onbevoegd toe-eigenen of kopiëren van documenten, voorwerpen, substanties, materialen of elektronische bestanden waarover de houder van het bedrijfsgeheim rechtmatig

⁷¹ Art. I.17/1, 3° WER

⁷² Art. XI.332/4, §1 WER.

beschikt én die het bedrijfsgeheim bevatten of waaruit het bedrijfsgeheim kan worden afgeleid. Andere gedragingen die gezien de omstandigheden worden beschouwd als in strijd met de eerlijke handelspraktijken staan opgesomd in paragraaf 1, ten tweede. De situatie die in de voorgaande paragraaf wordt omschreven, betreft zodoende een onrechtmatige verkrijging die gebeurt zonder toestemming van de houder van het bedrijfsgeheim én deze verkrijging moet gebeurd zijn door middel van een van de gedragingen die in de bijhorende bepalingen is neergelegd. Een voorbeeld hiervan is diefstal van prijslijsten al dan niet in het kader van economische spionage.

De volgende onrechtmatige handeling, staat neergeschreven in paragraaf 2 en handelt over de situatie waarin iemand een bedrijfsgeheim onrechtmatig gebruikt of openbaar maakt. Wanneer iemand een bedrijfsgeheim openbaar maakt of gebruikt zonder toestemming van de houder van dit bedrijfsgeheim wordt dit als onrechtmatig beschouwd wanneer de persoon die deze gedraging stelt aan een van de voorwaarden voldoet die is neergelegd in de bepalingen van paragraaf 2. De voorwaarden gaan als volgt: *“hij heeft het bedrijfsgeheim op een onrechtmatige manier verkregen; hij maakt een inbreuk op een geheimhoudingsovereenkomst of een andere verplichting tot het niet openbaar maken van het bedrijfsgeheim of hij maakt een inbreuk op een contractuele of andere verplichting tot beperking van het gebruik van het bedrijfsgeheim”*.⁷³ Er moet slechts aan één van de drie voorwaarden voldaan zijn opdat er gesproken kan worden over een onrechtmatig gebruik of een onrechtmatige openbaarmaking. Daarbij moet er opnieuw een gebrek aan toestemming zijn van de houder van het bedrijfsgeheim. Het component van openbaar maken is snel vervuld waardoor een situatie waarin het bedrijfsgeheim slechts aan één enkele partij bekend wordt gemaakt ook valt onder artikel XI.332/4, §2, vermits een van de drie voorwaarden logischerwijze vervuld is.⁷⁴ Een typevoorbeeld is het verkrijgen van een bedrijfsgeheim via diefstal en dit vervolgens online te plaatsen.

De andere twee onrechtmatige situaties inzake bedrijfsgeheimen kwamen eerder al aan bod bij de definitie van een inbreukmaker. Het betreft met name de situatie met een derde(-verkrijger) van een bedrijfsgeheim. Wanneer een persoon op het moment van het gebruiken, openbaar maken of verkrijgen van een bedrijfsgeheim wist of had moeten weten, gezien de omstandigheden, dat het bedrijfsgeheim direct of indirect werd verkregen via een persoon die zelf het bedrijfsgeheim op een onrechtmatige manier openbaar maakte of gebruikte, dan wordt deze situatie tevens gezien als onrechtmatig.⁷⁵ Van de derde is enkel een kennis of kennisvermoeden vereist, waardoor een actieve onrechtmatige handeling niet aanwezig moet zijn. Deze kenniscomponent zal beoordeeld worden op het moment van het gebruiken, openbaar maken of verkrijgen.⁷⁶ De laatste hypothese gaat over een situatie waarin inbreukmakende goederen worden geproduceerd, aangeboden of in de handel worden gebracht of wanneer inbreukmakende goederen voor die doeleinden worden ingevoerd, uitgevoerd of opgeslagen en als de persoon die deze activiteiten uitvoert wist of had moeten weten, gezien de omstandigheden, dat het bedrijfsgeheim onrechtmatig werd gebruikt.⁷⁷ Voor deze situatie is opnieuw

⁷³ Artikel XI.332/4, §2, 1°-3° WER.

⁷⁴ H. VANHEES, “De nieuwe wettelijke regeling betreffende de bescherming van bedrijfsgeheimen”, *RW* 2018-2019, afl. 42, 1645.

⁷⁵ Artikel XI.332/4, §3 WER.

⁷⁶ L. DEVROE, D. PHILIPPE en T. VAN NOYEN, “Protection des secrets d’affaires – Analyse de la loi du 30 juillet 2018 transposant la directive (UE) 2016/943”, *DAOR* 2019, afl.132, 6.

⁷⁷ Artikel XI.332/4, §4 WER.

een kennis of kennisvermoeden vereist, maar deze keer dient de persoon in kwestie wel bepaalde handelingen te stellen. A contrario, als betrokkenen bij deze twee situaties te goeder trouw zijn wegens het gebrek van kennis over de onrechtmatigheid, kan verondersteld worden dat zij niet kunnen worden veroordeeld, omwille van het gebrek aan kennis.

Samenvattend, zijn de onrechtmatige handelingen dus in feite terug te brengen tot het onderscheid in onrechtmatige verkrijging, onrechtmatige openbaarmaking en onrechtmatig gebruik.

IV.C.5 Beoordeling hypotheses

Bij deze zijn de nodige begrippen opgehelderd. Waardoor het eindelijk tijd is om de beschreven situaties één voor één en stap voor stap te toetsen. De eerste stap zal het benoemen zijn van alle gestelde handelingen door de betrokken persoon of personen in een hypothese. Vervolgens zal worden nagegaan welke van deze handelingen onder het begrip onrechtmatige handeling valt. De laatste stap bestaat erin om vast te stellen om welke van de drie onrechtmatige handelingen het precies gaat. Deze laatste stap is van belang, omdat de wet enerzijds een welbepaalde gedraging vereist per soort onrechtmatige handeling⁷⁸ en anderzijds, omdat de verscheidene onrechtmatige handelingen niet altijd op dezelfde manier door de wet worden behandeld, maar hierover meer bij de bescherming van bedrijfsgeheimen door de werkgever. Deze laatste stap zal samen worden besproken met de tweede stap om de toetsing zo overzichtelijk en zo logisch mogelijk te houden.

Deze toetsing gebeurt teneinde te ontdekken of de betrokken persoon/personen onrechtmatige handelingen heeft/hebben gesteld wat tot gevolg heeft dat deze persoon of personen gelabeld kan of kunnen worden als inbreukmaker(s). Eenmaal dit is achterhaald, kan worden overgegaan naar het nemen van juridische stappen door de werkgever. De werkgever moet immers weten jegens wie hij een vordering kan instellen. Zoals gezegd volgt de behandeling van wat de werkgever tegen een inbreukmaker kan doen na de beoordeling van de hypotheses.

IV.C.5.1 Beoordeling hypothese 1

De betrokken personen bij situatie 1 waren J en zijn vrouw L. Door de nalatigheid van J heeft L haarzelf toegang verschaft tot het geheime recept van de speculaaskoekjes van de werkgever van J. Dit recept vormt een van de bedrijfsgeheimen van J zijn werkgever Q. Op het einde besloot ze tevens om dit recept naar haar tablet te kopiëren.

De eerste stap is het benoemen van de gestelde handelingen door zowel J als L.

Handelingen gesteld door J:

- ❖ In plaats van zijn werklaptop te gebruiken, maakt J gebruik van zijn persoonlijke laptop;
- ❖ J heeft alles van zijn bedrijfscomputer naar zijn persoonlijke laptop gekopieerd waaronder bedrijfsgeheimen van zijn werkgever Q;
- ❖ J laat L regelmatig gebruik maken van zijn laptop;
- ❖ J heeft geen enkele vorm van beveiliging op zijn laptop staan.

Handelingen gesteld door L:

⁷⁸ Denk bijvoorbeeld aan de besproken gedragingen die vereist zijn om te kunnen spreken van een onrechtmatige verkrijging, zoals de onbevoegde toegang tot het bedrijfsgeheim.

- ❖ L maakt regelmatig gebruik van J zijn laptop met diens toestemming;
- ❖ L verschaft zichzelf toegang tot het recept van de speculaaskoekjes van het merk Q zonder uitdrukkelijke toestemming van J;
- ❖ L kopieert het recept van de speculaaskoekjes naar haar persoonlijke tablet.

De tweede en derde stap houdt in dat er per persoon wordt nagegaan welke van de uitgevoerde handelingen onrechtmatig zijn en welke soort onrechtmatige handeling(en) in casu heeft/hebben plaatsgevonden.

Onrechtmatige handelingen gesteld door J:

- ❖ Aangezien J een hoog geplaatste werknemer is en toegang heeft tot bedrijfsgeheimen kan verondersteld worden dat hij een geheimhoudingsovereenkomst heeft ondertekend die hem verbiedt om deze bedrijfsgeheimen openbaar te maken op grond van artikel 17, 3^o, a AOW.⁷⁹ Doordat J zijn vrouw L toestemming had gegeven om zijn laptop te gebruiken en vermits hij alles van zijn werk op deze laptop had gezet, zou deze handeling onder artikel XI.332/4, §2, 2^o WER kunnen vallen.⁸⁰ Bij de bespreking van deze bepaling bleek dat het bekendmaken van het geheim aan slechts één partij al kan vallen onder onrechtmatige openbaarmaking. Ondanks het feit dat J niet rechtstreeks het recept aan L heeft laten zien, zou gezegd kunnen worden dat hij hier onrechtstreeks verantwoordelijk voor is. Want hij had haar wél toestemming gegeven om zijn laptop te gebruiken en hij had zijn bestanden niet beveiligd. Alhoewel hij geen uitdrukkelijke toestemming had gegeven aan L om haarzelf toegang te verschaffen tot zijn documenten, zou deze toestemming toch kunnen worden afgeleid uit de toestemming voor het algemeen gebruik van zijn laptop. Daarom kan verondersteld worden dat hij zijn geheimhoudingsovereenkomst met zijn werkgever geschonden heeft. Hierdoor is er door deze handeling sprake van een onrechtmatige openbaarmaking.

Onrechtmatige handelingen gesteld door L:

- ❖ L verschaft haarzelf toegang tot het recept van de speculaaskoekjes terwijl ze hiervoor geen toestemming heeft van de werkgever/de houder van het bedrijfsgeheim Q. Dit is een duidelijk voorbeeld van een onrechtmatige verkrijging uit artikel XI.332/4, §1, 1^o WER⁸¹;
- ❖ Het kopiëren van het recept door L naar haar tablet is opnieuw een voorbeeld van een onrechtmatige verkrijging uit artikel XI.332/4, §1, 1^o WER, vermits zij geen toestemming had van de werkgever Q om deze handeling te stellen⁸²;

⁷⁹ *Supra* Hoofdstuk I – I.D Wijzigingen aan de wet van 3 juli 1978 (Arbeidsovereenkomstenwet).

⁸⁰ Artikel XI.332/4, §2, 2^o WER gaat als volgt: Het gebruiken of openbaar maken van een bedrijfsgeheim wordt als onrechtmatig beschouwd wanneer dit, zonder de toestemming van de houder van het bedrijfsgeheim, wordt verricht door een persoon die aan een van de volgende voorwaarden voldoet: 2^o hij maakt een inbreuk op een geheimhoudingsovereenkomst of een andere verplichting tot het niet openbaar maken van het bedrijfsgeheim.

⁸¹ Artikel XI.332/4, §1, 1^o WER gaat als volgt: De verkrijging van een bedrijfsgeheim zonder de toestemming van de houder van het bedrijfsgeheim wordt als onrechtmatig beschouwd wanneer de verkrijging gebeurde door middel van: 1^o onbevoegde toegang tot of het zich onbevoegd toe-eigenen of kopiëren van documenten, voorwerpen, materialen, substanties of elektronische bestanden waarover de houder van het bedrijfsgeheim rechtmatig beschikt en die het bedrijfsgeheim bevatten of waaruit het bedrijfsgeheim kan worden afgeleid.

⁸² *Supra* vn. 81.

- ❖ De laatste bepaling die in deze situatie toepasselijk zou kunnen zijn, betreft §3 van artikel XI.332/4 WER.⁸³ Op het moment dat L het recept verkreeg, had ze gezien de omstandigheden, namelijk het feit dat het om een gegeerd geheim recept gaat, ergens moeten weten dat ze niet zomaar toegang zou mogen hebben tot dit recept. Of dit werkelijk onder paragraaf drie zou vallen, hangt af in welke mate ze op de hoogte was dat J een inbreuk maakte op zijn geheimhoudingsovereenkomst door haar ongelimiteerde toegang te geven tot zijn laptop en dat hij hierdoor een bedrijfsgeheim onrechtmatig openbaar maakte. Gezien de omstandigheden lijkt het eerder niet zo het geval te zijn, maar het zou een mogelijkheid kunnen zijn.

Uit deze beoordelingen blijkt dat zowel J – de werknemer van Q - als L onrechtmatige handelingen hebben gesteld.

Het enige dat nog rest is om na te gaan of ze onder de noemer inbreukmaker vallen. Om onder dit begrip te vallen, moet er zoals besproken bij het begrip een natuurlijke of rechtspersoon zijn die één van de onrechtmatige handelingen heeft gesteld. In casu zijn beide personen natuurlijke personen en hebben ze elk onrechtmatige handelingen gesteld. Hieruit volgt dat ze beide inbreukmaker zijn en belangrijker dat de werkgever Q tegen elk van hen een vordering kan instellen. Het enige verschil is dat enkel J zijn werknemer is en L een derde is voor hem.

IV.C.5.2 Beoordeling hypothese 2

De personen in hypothese 2 waren I en L, collega bedrijfsjuristen die samen aan een dossier werken waarin bedrijfsgeheimen staan van hun werkgever X. Enkel L had toegang tot het gedeelte van het dossier waarin de bedrijfsgeheimen staan. Door een vergetelheid van L stuurt ze onbewust de documenten met deze geheimen in door via mail naar I. I die niet beter wist, leest echter per ongeluk de bijlagen van de mail voordat L kan ingrijpen.

De eerste stap is het benoemen van de gestelde handelingen door zowel L als I.

Handelingen gesteld door L:

- ❖ L stuurt onbewust bedrijfsgeheimen door via mail naar I.

Handelingen gesteld door I:

- ❖ I opent nietsvermoedend bijlagen van een email waarin bedrijfsgeheimen staan.

De tweede en derde stap houdt in dat er per persoon wordt nagegaan welke van de uitgevoerde handelingen onrechtmatig zijn en welke soort onrechtmatige handeling(en) in casu heeft/hebben plaatsgevonden.

Onrechtmatige handelingen gesteld door L:

⁸³ Artikel XI.332/4, §3 WER gaat als volgt: Het verkrijgen, gebruiken of openbaar maken van een bedrijfsgeheim wordt ook als onrechtmatig beschouwd wanneer een persoon op het moment van het verkrijgen, gebruiken of openbaar maken wist of, gezien de omstandigheden, had moeten weten dat het bedrijfsgeheim direct of indirect werd verkregen van een andere persoon die het bedrijfsgeheim op een onrechtmatige manier gebruikte of openbaar maakte in de zin van paragraaf 2.

- ❖ Doordat L documenten met bedrijfsgeheimen heeft doorgestuurd, valt ze met deze handeling onder artikel XI.332/4, §2, 2° WER.⁸⁴ Er kan worden verondersteld dat ze een geheimhoudingsovereenkomst heeft met haar werkgever X op grond van art 17, 3°, a AOW waardoor ze verplicht is om deze bedrijfsgeheimen geheim te houden.⁸⁵ Hieruit kan worden afgeleid dat ze door het mailen van de geheimen een inbreuk heeft gemaakt op deze overeenkomst, aangezien I geen toestemming had om deze documenten te bezichtigen. Op te merken valt dat de wet geen onderscheid maakt tussen het bewust of onbewust openbaar maken waardoor L een onrechtmatige openbaarmaking heeft gepleegd.

Onrechtmatige handelingen gesteld door I:

- ❖ Door het lezen van de bijlagen van de mail valt I met haar gedrag onder twee verschillende bepalingen. Ten eerste, valt ze onder artikel XI.332/4, §1, 1° WER, omdat ze zonder toestemming van X toegang heeft tot de bedrijfsgeheimen.⁸⁶ Het is niet zeker in welke mate ze bewust de documenten met de geheimen in heeft geopend. Misschien kon het worden afgeleid uit de titel van de documenten, maar misschien ook niet. Het speelt voor de wet geen rol of ze bewust of onbewust de documenten heeft geopend, want zodra ze dit deed, viel ze onder de noemer onrechtmatige verkrijging. De tweede bepaling waar ze onder zou kunnen vallen, is onder artikel XI.332/4, §3 WER.⁸⁷ Op het moment dat ze de bedrijfsgeheimen onder ogen kreeg, had ze moeten beseffen dat L hierdoor de bedrijfsgeheimen onrechtmatig openbaar had gemaakt. In vergelijking met de vorige situatie, is er hier veel meer zekerheid dat I het had moeten weten vermits het om een bedrijfsjuriste gaat. Daarbij speelt ook nog het feit dat ze gespecialiseerd is in het vennootschapsrecht waar geheimhoudingsovereenkomsten regelmatig voorkomen. Bijgevolg heeft I de kenniscomponent vervuld dat vereist is voor deze paragraaf.

Uit deze beoordelingen blijkt dat zowel L als I onrechtmatige handelingen hebben gesteld.

Het enige dat nog rest is om na te gaan of ze onder de noemer inbreukmaker vallen. Om onder dit begrip te vallen, moet er zoals besproken bij het begrip een natuurlijke of rechtspersoon zijn die één van de onrechtmatige handelingen heeft gesteld. In casu zijn beide personen natuurlijke personen en hebben ze elk onrechtmatige handelingen gesteld. Hieruit volgt dat ze beide inbreukmaker zijn en belangrijker dat de werkgever X tegen elk van hen een vordering kan instellen.

IV.C.5.3 Beoordeling hypothese 3

De laatste situatie betrof de werknemer S. Zij verloor haar werklaptop vol bedrijfsgeheimen in een park. Normaal gezien was de laptop beveiligd, maar gezien zij de beveiliging vervelend vond, had ze alle veiligheidsmaatregelen verwijderd. Bovendien stonden er bedrijfsgeheimen open op het moment dat ze de laptop verloor waardoor een mogelijke vinder deze bedrijfsgeheimen meteen zou zien. Wat natuurlijk ook is gebeurd. Een toevallige wandelaar vond de laptop van S in het park en eenmaal

⁸⁴ *Supra* vn. 80.

⁸⁵ *Supra* vn. 79.

⁸⁶ *Supra* vn. 81.

⁸⁷ *Supra* vn. 83.

thuis aangekomen, nam hij een kijkje op de laptop waardoor hij de geheimen zag van D, de werkgever van S.

De eerste stap is het benoemen van de gestelde handelingen door zowel S als de wandelaar.

Handelingen gesteld door S:

- ❖ S had een werklaptop gekregen met beveiliging op. S heeft alle beveiliging uitgeschakeld;
- ❖ S zou in principe thuis moeten telewerken, maar ze gaat geregeld ergens anders telewerken;
- ❖ S laat per ongeluk haar laptop achter in het park terwijl ze ontwerpen van videokaarten aan het raadplegen was. Deze videokaarten vormen bedrijfsgeheimen van haar werkgever D.

Handelingen gesteld door de wandelaar:

- ❖ De wandelaar vindt een laptop die achtergelaten is en neemt deze mee naar huis;
- ❖ De wandelaar neemt bewust de beslissing om te kijken wat er op de laptop staat en ziet de ontwerpen van de videokaarten van D.

De tweede en derde stap houdt in dat er per persoon wordt nagegaan welke van de uitgevoerde handelingen onrechtmatig zijn en welke soort onrechtmatige handeling(en) in casu heeft/hebben plaatsgevonden.

Onrechtmatige handelingen gesteld door S:

- ❖ Vermits S alle beveiliging van haar werklaptop had gehaald en omdat ze op het ogenblik dat ze haar laptop verloor bedrijfsgeheimen had openstaan, valt ze met deze handelingen onder artikel XI.332/4, §2, 2° WER.⁸⁸ Aangezien haar werkgever D zoveel moeite had gedaan om haar werklaptop te beveiligen waarop bedrijfsgeheimen stonden, kan hieruit worden afgeleid dat ze een geheimhoudingsovereenkomst had of toch minstens een verplichting om de ontwerpen van de videokaarten niet openbaar te maken.⁸⁹ Hoewel ze de bedrijfsgeheimen niet openbaar wilde maken, hebben haar handelingen er toch voor gezorgd dat ze deze openbaar heeft gemaakt aan een derde (de wandelaar) waardoor ze de geheimhoudingsplicht geschonden heeft. Als gevolg hiervan is er sprake van een onrechtmatige openbaarmaking.

Onrechtmatige handelingen gesteld door de wandelaar:

- ❖ Hij heeft absoluut geen toestemming van D om toegang te nemen tot de bedrijfsgeheimen die op de laptop van S staan. Hierdoor is er een onrechtmatige verkrijging in de zin van artikel XI.332/4, §1, 1° WER.⁹⁰ Daarnaast, is het niet ondenkbaar dat de wandelaar de ontwerpen gaat kopiëren;
- ❖ Afhankelijk met welk doel de wandelaar de laptop heeft meegenomen uit het park, heeft de wandelaar diefstal gepleegd.⁹¹ Indien de wandelaar de laptop heeft meegenomen met de bedoeling om zichzelf een onrechtmatig voordeel te verschaffen, heeft hij inderdaad diefstal gepleegd. Want hij heeft een goed (de laptop) van iemand anders (S) weggenomen.

⁸⁸ *Supra* vn. 80.

⁸⁹ Bijvoorbeeld opnieuw op grond van artikel 17, 3°, a AOW.

⁹⁰ *Supra* vn. 81.

⁹¹ Het misdrijf diefstal is vastgelegd in artikel 461 Strafwetboek. De gewone diefstal staat in het eerste lid en houdt in dat een persoon een zaak die hem niet toebehoort, bedrieglijk wegneemt.

Voortspruitend op de gedachte dat hij de ontwerpen gaat kopiëren, zou hij mogelijk verleid zijn om de ontwerpen te gebruiken of openbaar te maken. In dit geval, valt de wandelaar met deze gedraging onder artikel XI.332/4, §2, 1° WER, aangezien hij na de diefstal onbevoegd toegang had tot de bedrijfsgeheimen op de laptop.⁹² Er zou derhalve een onrechtmatig gebruik of openbaarmaking zijn afhankelijk van wat de wandelaar verder doet met de bedrijfsgeheimen;

- ❖ De laatste onrechtmatige handeling zou artikel XI.332/4, §3 WER kunnen zijn.⁹³ De wandelaar heeft met name geen flauw idee of de eigenaar van de laptop (S) de ontwerpen op een rechtmatige manier heeft verkregen noch of deze door S op een onrechtmatige manier gebruikt worden of openbaar zijn gemaakt. Uit de bespreking van de handelingen van S werd vastgesteld dat het bedrijfsgeheim op een onrechtmatige manier openbaar was gemaakt, maar dit weet de wandelaar vanzelfsprekend niet. Daarom neigt deze handeling eerder niet onder XI.332/4, §3 WER te vallen, maar het zou wel kunnen in principe.

Uit deze beoordelingen blijkt dat zowel S – de werknemer van D - als de wandelaar onrechtmatige handelingen hebben gesteld.

Het enige dat nog rest is om na te gaan of ze onder de noemer inbreukmaker vallen. Om onder dit begrip te vallen, moet er zoals besproken bij het begrip een natuurlijke of rechtspersoon zijn die één van de onrechtmatige handelingen heeft gesteld. In casu zijn beide personen natuurlijke personen en hebben ze elk onrechtmatige handelingen gesteld. Hieruit volgt dat ze beide inbreukmaker zijn en belangrijker dat de werkgever D tegen elk van hen een vordering kan instellen.

IV.D Hoe kan een werkgever (houder van een bedrijfsgeheim) optreden?

Aangezien alle onrechtmatige handelingen zijn vastgesteld en alle inbreukmakers zijn geïdentificeerd, kan worden overgegaan naar hoe een houder van een bedrijfsgeheim of in casu een werkgever kan optreden tegen deze handelingen en personen. In het kader van de bescherming van bedrijfsgeheimen bestaan een aantal maatregelen en procedures. Het handhavingssysteem dat is ingevoerd door de Richtlijn Bedrijfsgeheimen en de Wet Bedrijfsgeheimen is sterk gelijkend op het handhavingssysteem van intellectuele eigendomsrechten.⁹⁴

IV.D.1 Procedures

Er zijn drie procedures die ter beschikking staan aan de werkgever om op te komen tegen de onrechtmatige handelingen van zijn werknemer en derden. Namelijk de procedure ten gronde, de vordering tot staking zoals in kort geding en het gewone kort geding. De procedures zullen één voor één besproken worden.

IV.D.1.1 Procedure ten gronde

In principe is de ondernemingsrechtbank bevoegd om kennis te nemen van geschillen inzake bedrijfsgeheimen ongeacht het bedrag van de vordering en zelfs wanneer de partijen geen

⁹² Artikel XI.332/4, §2, 1° WER gaat als volgt: Het gebruiken of openbaar maken van een bedrijfsgeheim wordt als onrechtmatig beschouwd wanneer dit, zonder de toestemming van de houder van het bedrijfsgeheim, wordt verricht door een persoon die aan een van de volgende voorwaarden voldoet: 1° hij heeft het bedrijfsgeheim op onrechtmatige manier verkregen.

⁹³ *Supra* vn. 83.

⁹⁴ Richtl.Raad.EP. nr. 2004/48, 29 april 2004 betreffende de handhaving van intellectuele-eigendomsrechten, *Pb.L.* 30 april 2004, afl. 157.

ondernemingen zijn.⁹⁵ Bovendien heeft de Belgische wetgever een centralisatie van de vorderingen betreffende bedrijfsgeheimen willen nastreven door te bepalen dat enkel ondernemingsrechtbanken die gevestigd zijn bij de zetel van een hof van beroep bevoegd zijn om kennis te nemen van dergelijke vorderingen. Desalniettemin, wordt geen afbreuk gedaan aan de specifieke bevoegdheden van arbeidsrechtbanken. Want op grond van artikel 578, 1° Ger.W. blijft de arbeidsrechtbank bevoegd voor geschillen inzake arbeidsovereenkomsten met inbegrip van geschillen die betrekking hebben op schending van een bedrijfsgeheim gedurende die overeenkomst.⁹⁶ Het is enkel wanneer de schending zich voordoet na de beëindiging van de arbeidsovereenkomst, dat de ondernemingsrechtbank in principe bevoegd zal zijn. Met andere woorden, de arbeidsrechtbank primeert op de ondernemingsrechtbank wanneer het geschil inzake bedrijfsgeheimen zich voordoet in de context van een arbeidsovereenkomst. Een andere uitzondering op de bevoegdheid van de ondernemingsrechtbank, is dat als het onrechtmatig gebruiken, openbaar maken of verkrijgen ingeroepen wordt als verweer, dat de rechter die bevoegd is voor de hoofdvordering, bevoegd blijft bij dergelijk verweer.⁹⁷ In casu, zullen de vorderingen van alle betrokken werknemers voor de arbeidsrechtbank gebracht worden, aangezien zij elk hun geheimhoudingsplicht hebben geschonden tijdens de duurtijd van hun arbeidsovereenkomst. Ze werkten immers allemaal als telewerkers voor hun werkgever wanneer de onrechtmatige handelingen plaatsvonden. Voor de vorderingen tegen L en de wandelaar zal de ondernemingsrechtbank bevoegd zijn, omdat zij voor de werkgever in kwestie telkens derden waren.

Artikel XI.336/2 WER geeft de werkgever het recht om de toepassing van de maatregelen, procedures en rechtsmiddelen vastgesteld door de wet ter voorkoming van, of om schadeloosstelling te verkrijgen voor het onrechtmatig verkrijgen, gebruiken of openbaar maken van zijn bedrijfsgeheim te verzoeken. Op grond van dit artikel kan de werkgever een procedure ten gronde inleiden tegen de inbreukmakers. Wanneer de rechter vaststelt dat er in casu sprake is van onrechtmatig gebruik, onrechtmatige openbaarmaking of onrechtmatige verkrijging van een bedrijfsgeheim, kan hij jegens de inbreukmaker een of meerdere maatregelen bevelen en correctieve maatregelen opleggen. Deze beoordeling is casuïstisch waarbij rekening wordt gehouden met de specifieke omstandigheden van de voorliggende situatie. Hierbij zal de rechter onder meer rekening houden met de waarde of andere specifieke kenmerken van het bedrijfsgeheim, de bescherming van grondrechten, de maatregelen die genomen zijn om het bedrijfsgeheim te beschermen, het algemeen belang, de handelwijze van de inbreukmaker, de effecten van de openbaarmaking of van het onrechtmatig gebruik van het bedrijfsgeheim, de rechtmatige belangen van de partijen en de potentiële gevolgen van het bevelen of afwijzen van de gevraagde maatregelen voor de partijen en de rechtmatige belangen van derden.⁹⁸ Toegepast op hypothese 1 zal de rechter bijgevolg rekening houden met het feit dat het bedrijf Q achter staat op het vlak van beveiliging, met het gegeven dat het recept van de speculaaskoekjes door zijn populariteit allicht veel waard zal zijn en dat de openbaarmaking hiervan nefast zal zijn voor de winst van Q.

⁹⁵ Artikel XI.342/1 WER juncto artikel 574, 22° Ger.W.

⁹⁶ Wetsontwerp betreffende de bescherming van bedrijfsgeheimen, *Parl.St.* Kamer 2017-2018, nr. 54-3154/001, 22.

⁹⁷ Wetsontwerp betreffende de bescherming van bedrijfsgeheimen, *Parl.St.* Kamer 2017-2018, nr. 54-3154/001, 22.

⁹⁸ Zie artikel XI.336/4, §1 WER.

De rechter kan de staking of het verbod op de verkrijging, de openbaarmaking of het gebruik van het bedrijfsgeheim bevelen.⁹⁹ Als dit wordt toegepast op hypothese 3 en veronderstellend dat de wandelaar de ontwerpen bv. online heeft geplaatst en hierdoor geld heeft verdiend, zou de rechter hem kunnen bevelen om de openbaarmaking te staken. In het verlengde hiervan kan de rechter tevens een verbod opleggen om inbreukmakende goederen te produceren, in de handel te brengen, te gebruiken, aan te bieden of om inbreukmakende goederen voor deze doeleneinden op te slaan, in te voeren of uit te voeren.¹⁰⁰ Daarbij kan hij de terugroeping van inbreukmakende goederen van de markt bevelen en het ontdoen van de inbreukmakende hoedanigheid van deze goederen.¹⁰¹ Indien nodig kan de rechter zelfs de vernietiging van de inbreukmakende goederen bevelen of hij kan bevelen dat ze uit de handel worden genomen. Het uit de handel laten nemen kan slechts bevolen worden als dit geen afbreuk doet aan de bescherming van het betrokken bedrijfsgeheim en deze goederen kunnen aan de houder of aan een liefdadigheidsorganisatie worden overhandigd indien de houder van het bedrijfsgeheim hierom verzoekt.¹⁰² Ten slotte kan de rechter de volledige of gedeeltelijke vernietiging van de voorwerpen, documenten, substanties, materialen of elektronische bestanden waarop het bedrijfsgeheim staat of wordt belichaamd bevelen of hij kan bevelen dat deze geheel of gedeeltelijk overhandigd worden aan de houder van het bedrijfsgeheim.¹⁰³ In het geval van hypothese 1 zou de rechter de vernietiging van de documenten op J zijn persoonlijke laptop en het document waarin het recept staat op de tablet van L kunnen bevelen. Hij zou zelfs de vernietiging van de persoonlijke laptop en tablet kunnen bevelen.

De maatregelen gebeuren in principe op kosten van de inbreukmaker, op voorwaarde dat dit niet belet wordt door bijzondere redenen en de rechter kan deze maatregelen opleggen onder verbeurte van een dwangsom.¹⁰⁴ Voorts, heeft de rechter de mogelijkheid om de looptijd van de staking of verbod op de verkrijging, de openbaarmaking en het gebruik van het bedrijfsgeheim te beperken. Hij kan mede de looptijd beperken van het verbod om inbreukmakende goederen te produceren, in de handel te brengen, te gebruiken, aan te bieden of om deze goederen op te slaan, in of uit te voeren. De beperking in de tijd kan slechts op voorwaarde dat de looptijd voldoende lang is om de handels- en economische voordelen van de inbreukmaker die hij zou kunnen hebben gehaald uit het onrechtmatig gebruik, verkrijging of openbaarmaking van het bedrijfsgeheim teniet te doen. Bij het beperken van de looptijd dient de rechter eveneens rekening te houden met de elementen uit het eerder vernoemde artikel XI.336/4, §1 WER.¹⁰⁵ Tevens moet worden benadrukt dat de maatregelen die de rechter kan opleggen, geen afbreuk doen aan enige schadevergoeding die de werkgever verschuldigd kan zijn door het onrechtmatig gebruiken, openbaar maken of verkrijgen van het bedrijfsgeheim.¹⁰⁶ Als de rechter inderdaad voor hypothese 3 de staking van de openbaarmaking

⁹⁹ Artikel XI.336/3, §1, 1^o WER.

¹⁰⁰ Artikel XI.336/3, §1, 2^o WER.

¹⁰¹ Artikel XI.336/3, §1, 3^o-4^o WER.

¹⁰² Artikel XI.336/3, §1, 5^o en §2 WER.

¹⁰³ Artikel XI.336/3, §1, 6^o WER.

¹⁰⁴ Zie artikel XI.336/3, §3 WER en artikel 1385*bis* Ger.W.

¹⁰⁵ Artikel XI.336/4, §1, laatste lid WER.

¹⁰⁶ Artikel XI.336/3, §4 WER; Deze schadevergoeding kan gevorderd worden op grond van artikel XI.336/5, §1 WER. Voor deze schadevergoeding worden de gewone principes inzake buitencontractuele aansprakelijkheid toegepast, wat betekent dat het bestaan van een fout, schade en oorzakelijk verband moet worden vastgesteld door de rechter.

heeft bevolen, kan deze staking in de tijd beperkt zijn afhankelijk van hoeveel winst de wandelaar had gemaakt.

De inbreukmaker jegens wie de staking of het verbod wordt opgelegd, kan verzoeken dat deze maatregelen herroepen worden of op een andere wijze niet langer uitwerking hebben indien de informatie niet meer voldoet aan de definitie van een bedrijfsgeheim uit artikel I.17/1, 1° WER en dit niet direct of indirect te wijten is aan de inbreukmaker.¹⁰⁷ Daarnaast kan de inbreukmaker verzoeken aan de rechter dat hij in plaats van maatregelen te bevelen of op te leggen, dat hij beveelt dat er een geldelijke schadeloosstelling moet worden betaald aan de benadeelde partij. De rechter kan dit verzoek pas inwilligen als aan drie voorwaarden is voldaan. Allereerst wist de betrokkene niet of had hij gezien de omstandigheden niet hoeven te weten dat op het moment van het gebruiken of openbaar maken, dat het bedrijfsgeheim verkregen werd via een andere persoon die het bedrijfsgeheim op een onrechtmatige manier gebruikte of openbaar maakte. Ten tweede dat de uitvoering van de betrokken maatregelen hem onevenredige schade zou toebrengen en ten derde, dat de geldelijke schadeloosstelling aan de benadeelde partij redelijkerwijs bevredigend lijkt. Indien de rechter dit verzoek tot geldelijke schadeloosstelling zou inwilligen in plaats van een staking of een verbod te bevelen, dan mag de geldelijke schadeloosstelling niet meer bedragen dan het bedrag van de vergoedingen of royalty's die verschuldigd waren geweest indien die persoon toestemming had gevraagd om het bedrijfsgeheim te gebruiken voor de periode waarin het gebruik van dit bedrijfsgeheim verboden had kunnen worden.¹⁰⁸ De geldelijke schadeloosstelling zou kunnen plaatsvinden bij hypothese 3. De wandelaar had in casu geen idee dat de ontwerpen onrechtmatig openbaar werden gemaakt door S aan hem. Hij wist niet eens van wie de laptop was en het was niet mogelijk voor hem om dit en de onrechtmatige openbaarmaking van S af te leiden uit de omstandigheden. Betreffende de tweede voorwaarde zou deze vervuld kunnen zijn indien nadien bv. blijkt dat hij een reputatie had als een betrouwbare informaticus en dat deze reputatie volledig vernietigd is doordat mensen denken dat hij bedrijfsgeheimen steelt.

De voorlaatste maatregel die ter beschikking staat aan de eiser, is de mogelijkheid om aan de rechter te verzoeken dat zijn beslissing of een samenvatting van zijn beslissing gepubliceerd wordt. Deze publicatie kan plaatsvinden door de beslissing of samenvatting van de rechter te laten aanplakken binnen en/of buiten de inrichtingen van de inbreukmaker. Daarnaast kan de rechter opteren om dit in kranten te laten bekendmaken of op enige andere wijze bv. online op de site van de inbreukmaker als het om een bedrijf gaat of een ondernemer. Dit alles zal gebeuren op kosten van de inbreukmaker, maar bij het uitvoeren van deze maatregel worden de bepalingen inzake de vertrouwelijkheid van bedrijfsgeheimen in acht genomen.¹⁰⁹ Tijdens het nemen van de beslissing tot publicatie dient de rechter rekening te houden met een aantal omstandigheden, zoals de waarde van het bedrijfsgeheim en de effecten van het onrechtmatig gebruik of openbaarmaking van het bedrijfsgeheim. Als laatste moet de rechter in acht houden of de gepubliceerde informatie kan leiden tot de identificatie van een natuurlijke persoon. Als dit zo het geval is, moet de rechter nagaan of de bekendmaking van deze informatie gerechtvaardigd is in het kader van de mogelijke schade die hierdoor teweeg kan worden

¹⁰⁷ Zie artikel XI.336/4, §2 WER.

¹⁰⁸ Artikel XI.336/4, §3 WER; XI.336/4, §3, laatste lid juncto XI.336/3, §1, 1°-2° WER.

¹⁰⁹ Artikel XI.342/3, §1 WER; Artikel 871*bis* Ger.W.

gebracht aan de persoonlijke levenssfeer en reputatie van de inbreukmaker.¹¹⁰ In de hypotheses is er niet echt iemand waar de publicatie zinvol zou zijn, behalve misschien in hypothese 3 als de wandelaar zelf een bedrijf had dat videokaarten maakt.

Als laatste moet vermeld worden dat de rechter op grond van artikel 19, derde lid Ger.W. in elk stand van de rechtspleging voorafgaande maatregelen kan bevelen alvorens recht te doen om de toestand van de partijen voorlopig te regelen of om de vordering te onderzoeken. Onder deze maatregelen vallen de voorziene voorlopige en conservatoire maatregelen uit artikel 10 van de Richtlijn Bedrijfsgeheimen. Het betreft onder meer de staking van of het verbod op het gebruik of openbaarmaking van het bedrijfsgeheim.¹¹¹ In tegenstelling tot de kortgedingprocedure is hier in principe géén spoedeisendheid vereist.

IV.D.1.2 De vordering tot staking zoals in kort geding

De werkgever kan tevens beslissen om zijn vordering tot staking tegen L en de wandelaar in te stellen bij de voorzitter van de ondernemingsrechtbank en de vordering tegen de werknemers bij de voorzitter van de arbeidsrechtbank.¹¹² Voor deze vordering gelden dezelfde uitgangspunten als voor het bevel tot staking dat ten gronde kan worden uitgesproken. Dit betekent dat de voorzitter bijgevolg ook de staking kan bevelen van zowel het onrechtmatig verkrijgen als van het openbaar maken van een bedrijfsgeheim of van het onrechtmatig gebruik ervan.¹¹³ Daarnaast heeft dit tot gevolg dat deze stakingsvordering enkel kan ingesteld worden tegen de inbreukmaker en niet tegen mogelijke tussenpersonen. Hierbuiten verloopt de instelling en de behandeling van de vordering zoals in kort geding.¹¹⁴ In de situaties waren er geen tussenpersonen, dus dit vormt geen probleem. Een van de beste situaties waarvoor een staking toepasselijk zou zijn, betreft de onrechtmatige toegang van I in hypothese 2. Aangezien ze zo graag de inhoud van deze bedrijfsgeheimen wilde weten, is het niet moeilijk om voor te stellen dat ze nadat L haar verwittigd heeft de documenten niet zou verwijderen. Voor deze hypothese zou een staking zeer gepast zijn.

Bij het bevelen van de staking kan de voorzitter bijkomend de voorziene maatregelen uit de procedure ten gronde opleggen. Hij kan dit slechts op voorwaarde dat deze maatregelen kunnen bijdragen tot de stopzetting van de openbaarmaking of het onrechtmatig gebruik van het bedrijfsgeheim of van de gevolgen ervan. Een goede toepassing hiervan zou op hypothese 3 zijn als de wandelaar de ontwerpen online had geplaatst. De voorziene maatregelen tot herstel van de schade die door de inbreuk wordt veroorzaakt, kunnen hier niet aangewend worden.¹¹⁵

Net zoals in een procedure ten gronde moet de voorzitter in concreto beoordelen of de gevorderde maatregel evenredig is en hierbij dient hij rekening te houden met de eerder vernoemde elementen uit artikel XI.336/4 §1 en §2 WER.

¹¹⁰ Artikel XI.342/3, §2 WER.

¹¹¹ Artikel 10 van de Richtlijn Bedrijfsgeheimen is slechts beperkt omgezet, vermits het Belgische gerechtelijke recht de rechter reeds in staat stelde om de voorziene maatregelen in deze bepaling te nemen, zie Wetsontwerp betreffende de bescherming van bedrijfsgeheimen, *Parl.St.* Kamer 2017-2018, nr. 54-3154/001, 27-28.

¹¹² Artikel XVII.21/1 WER.

¹¹³ Wetsontwerp betreffende de bescherming van bedrijfsgeheimen, *Parl.St.* Kamer 2017-2018, nr. 54-3154/001, 24.

¹¹⁴ XVII.21/3 WER.

¹¹⁵ Artikel XVII.21/2 WER.

Ten slotte kan ook hier verzocht worden om publicatie van het vonnis op kosten van de inbreukmaker, maar in tegenstelling tot de procedure ten gronde zal dit slechts toegelaten worden indien de publicatie kan bijdragen tot de stopzetting van de gewraakte daad of de uitwerking ervan.¹¹⁶

IV.D.1.3 De procedure in kort geding

In spoedeisende gevallen kan de werkgever zich richten tot de kortgedingrechter om voorlopige en bewarende maatregelen te verzoeken. Hierbij kan hij eisen dat deze maatregelen worden opgelegd onder verbeurte van een dwangsom.¹¹⁷ Bij de beoordeling over de vordering in kort geding en de evenredigheid ervan moet de kortgedingrechter in concreto beoordelen waarbij hij rekening moet houden met de specifieke omstandigheden.¹¹⁸

De voorziene lijst van maatregelen uit artikel 584 Ger.W. is niet exhaustief waardoor de kortgedingrechter een arsenaal aan maatregelen heeft om uit te kiezen. De meest voor de hand liggende maatregelen in het kader van inbreuken op bedrijfsgeheimen is de staking van of het verbod op het gebruiken, openbaar maken of verkrijgen van een bedrijfsgeheim. Daarnaast kan gedacht worden aan het opleggen van een verbod om inbreukmakende goederen te produceren, in de handel te brengen, aan te bieden, in of uit te voeren of op te slaan. Een mogelijke maatregel in het kader van zowel hypothese 1 als 2 is om een gerechtsdeurwaarder als sekwester aan te stellen om de laptops van J en I en de tablet van L in bewaring te nemen.¹¹⁹

Door de Wet Bedrijfsgeheimen voorziet artikel 584 Ger.W. tegenwoordig uitdrukkelijk een maatregel in verband met bedrijfsgeheimen. Artikel 584, vijfde lid, ten zesde geeft namelijk de kortgedingrechter de mogelijkheid om te bevelen in geval van het onrechtmatig gebruiken, openbaar maken of verkrijgen van een bedrijfsgeheim en mits de houder van het bedrijfsgeheim erom verzocht, dat er ten bewarende titel beslag wordt gelegd op de inbreukmakende goederen of om ze af te geven. Dit kan worden bevolen om te voorkomen dat de goederen in de handel gebracht worden of zich in het handelsverkeer bevinden.

Vermits het om een kortgedingprocedure gaat, mag de kortgedingrechter geen maatregelen bevelen die de rechten van de partijen op definitieve en onherstelbare wijze zouden aantasten.¹²⁰

Belangrijk in het kader van een kortgedingprocedure inzake bedrijfsgeheimen is dat de eiser die maatregelen bekomen heeft, verplicht is om binnen een redelijke termijn een procedure ten gronde in te stellen. Deze termijn wordt bepaald door de rechterlijke instantie die de maatregelen oplegt. Bij gebrek hieraan bedraagt het een termijn van ten hoogste twintig werkdagen of eenendertig dagen, naargelang welke van beide termijnen de langste is vanaf de betekening van de beschikking.¹²¹ Indien hij dit nalaat, kan de verweerder verzoeken dat de voorlopige maatregelen herroepen worden of houden de maatregelen op gevolg te hebben. Bijkomend kan de verweerder

¹¹⁶ Artikel XVII.21/5 WER.

¹¹⁷ Artikel 584, derde lid Ger.W.; Artikel 1385*bis* Ger.W.

¹¹⁸ Artikel 1369*quater* Ger.W.; Dit zijn dezelfde omstandigheden als uit artikel XI.336/4, §1 WER.

¹¹⁹ Artikel 584, vijfde lid, 1° Ger.W.

¹²⁰ Artikel 1039 Ger.W.

¹²¹ Artikel 1369*quinquies*, 1° Ger.W.

dan verzoeken dat de eiser gelast wordt om hem op passende wijze schadeloos te stellen voor de schade die deze maatregelen hem hebben toegebracht.¹²²

De maatregelen houden ook op gevolg te hebben indien de betreffende informatie niet langer voldoet aan de constitutieve elementen om te kunnen worden gekwalificeerd als bedrijfsgeheim én als dit niet toerekenbaar is aan de verweerder.¹²³

Tot slot geeft artikel 1369*sexies* Ger.W. de kortgedingrechter de mogelijkheid om een alternatief te voorzien voor voorlopige maatregelen en om een voorlopige maatregel te koppelen aan een zekerheid. De eerste paragraaf van dit artikel stelt dat de rechtbank aan de voortzetting van het vermeende onrechtmatig gebruik de voorwaarde kan verbinden dat een zekerheid wordt gesteld voor de schadeloosstelling van de werkgever. De tweede paragraaf laat de rechtbank toe om aan de voorlopige maatregelen de voorwaarde te verbinden dat de eiser een passende zekerheid of een gelijkwaardige garantie stelt voor een eventuele schadeloosstelling aan de verweerder of andere getroffen personen.

IV.E Inbreukmakende goederen en rechtmatige handelingen

Alhoewel er in de gekozen hypothesen geen sprake was van inbreukmakende goederen of rechtmatige handelingen, zou dit in werkelijkheid wel kunnen gebeuren. Om dit aan te tonen, zullen een aantal elementen uit de hypothesen bij de bespreking van de begrippen lichtjes worden aangepast. Op die manier zullen de begrippen makkelijker te begrijpen zijn.

IV.E.1 Inbreukmakende goederen

Het begrip inbreukmakende goederen staat gedefinieerd in artikel 1.17/1, 4^o WER. Inbreukmakende goederen zijn goederen waarvan het ontwerp, de werking, het productieproces, de kenmerken of het in de handel brengen aanzienlijk baat hebben bij bedrijfsgeheimen die onrechtmatig zijn gebruikt, openbaar gemaakt of verkregen.¹²⁴ Een verder onderscheid naargelang het gaat om materiële of immateriële goederen wordt niet gemaakt. Desalniettemin, zijn er auteurs in de rechtsleer die pleiten dat het gaat om materiële goederen, immateriële goederen en zelfs diensten.¹²⁵ Het probleem met deze definitie is dat er geen verduidelijking bestaat over wat moet begrepen worden als "aanzienlijk baat hebben" of hoe dit bewezen moet worden. Wanneer is er sprake van aanzienlijke baat en hoe kan dit worden afgeleid? Het lijkt vrijwel onmogelijk om vast te stellen dat een bepaald goed gemaakt is op grond van de kenmerken of het ontwerp van een bedrijfsgeheim zonder gezien te hebben hoe dat bepaald goed gemaakt en ontworpen is. Het zal afwachten worden tot er rechtspraak komt om te zien hoe wordt omgegaan met deze kwestie.

De twee situaties waar inbreukmakende goederen betrokken bij hadden kunnen zijn, betreft hypothese 1 en 3.

Stel bijvoorbeeld in hypothese 1 dat L op het idee was gekomen om de speculaaskoekjes onder haar eigen naam te beginnen verkopen op de wekelijkse markt bij haar in het dorp en dat ze hierdoor

¹²² Artikel 1369*septies* Ger.W.

¹²³ Artikel 1369*quinquies*, 2^o Ger.W.

¹²⁴ Art. I.17/1, 4^o WER.

¹²⁵ V.CASSIERS, "La directive 2016/943/UE du 8 juin 2016 sur les secrets d'affaires", *JT* 2017, nr. 21, 390; H. VANHEES, "De nieuwe wettelijke regeling betreffende de bescherming van bedrijfsgeheimen", *RW* 2018-2019, afl. 42, 1646.

elke week duizenden euro's zou verdienen. Dan zouden deze speculaaskoekjes inbreukmakende goederen zijn, omdat het materiële goederen zijn en het is gemaakt op grond van het recept dat een bedrijfsgeheim vormt dat onrechtmatig is verkregen. Bovendien zou gesteld kunnen worden dat ze aanzienlijke baat heeft doordat ze er zoveel geld mee verdient.

In hypothese 3 hadden er bijvoorbeeld inbreukmakende goederen kunnen zijn als de wandelaar had besloten om de ontwerpen online te zetten en als andere bedrijven deze ontwerpen gebruikten om hun eigen videokaarten te maken. Als deze bedrijven hierdoor veel winst zouden halen, kan er opnieuw sprake zijn van aanzienlijke baat. Daarbij, gaat het om materiële goederen die gemaakt zijn op basis van onrechtmatige openbaargemaakte bedrijfsgeheimen.

IV.E.2 Rechtmatige handelingen

In de besproken hypothesen ging het enkel en alleen om al dan niet onrechtmatige handelingen. Nochtans zijn niet alle handelingen onrechtmatig. De Wet Bedrijfsgeheimen heeft namelijk een aantal uitzonderingen ingevoerd en enkele situaties voorzien waarin er sprake is van rechtmatige handelingen.

Artikel XI.332/3 WER omschrijft wanneer de verkrijging, het gebruik of de openbaarmaking als rechtmatig wordt beschouwd. Er zijn drie specifieke gevallen wanneer de verkrijging van een bedrijfsgeheim als rechtmatig wordt beschouwd.

Als eerste, wanneer het bedrijfsgeheim verkregen wordt volgens een onafhankelijke ontdekking of onafhankelijk ontwerp.¹²⁶ Bijvoorbeeld als L in hypothese 1 maandenlang heeft geprobeerd om een recept te verzinnen voor lekkere speculaaskoekjes en per toeval het recept van werkgever Q weet na te bootsen.

Als tweede, wanneer het bedrijfsgeheim verkregen wordt via observatie, demontage, testen of onderzoek van een voorwerp of product dat ter beschikking is gesteld aan het publiek of dat op een rechtmatige manier in het bezit is van de persoon die de informatie verwerft en als deze persoon niet gebonden is aan een rechtsgeldige verplichting om de verkrijging van het bedrijfsgeheim te beperken.¹²⁷ Dit komt neer op reverse engineering.¹²⁸ Dit zou kunnen gebeuren in situatie 3 als de wandelaar zelf een videokaart van het bedrijf D had gekocht en dat hij door middel van demontage van de videokaart en testen van de componenten in deze kaart zelf op het ontwerp van de videokaart was uitgekomen. De wandelaar was namelijk niet gebonden aan een rechtsgeldige verplichting om de verkrijging van het ontwerp dat het bedrijfsgeheim vormt te beperken.

Het derde geval is wanneer een bedrijfsgeheim verkregen wordt door de uitoefening van het recht van werknemers of werknemersvertegenwoordigers op informatie en raadpleging overeenkomstig het Unierecht, het nationale recht en de nationale praktijken.¹²⁹ Hoewel er nationale praktijken staat, worden hiermee in feite de nationale gebruiken bedoeld. De Belgische wetgever benadrukte in de voorbereidende werken dat de bepalingen met betrekking tot bedrijfsgeheimen geen hindernis mogen vormen voor de toegang tot de raadpleging en informatie van werknemers en hun

¹²⁶ Artikel XI.332/3, §1, 1° WER.

¹²⁷ Artikel XI.332/3, §1, 2° WER.

¹²⁸ Overweging 16 Richtlijn Bedrijfsgeheimen.

¹²⁹ Artikel XI.332/3, §1, 3° WER.

vertegenwoordigers binnen de ondernemingen. Daarbij stelde de wetgever dat de bepalingen geen afbreuk mogen doen aan de wetgevingen die op dat vlak van toepassing zijn noch afbreuk mogen doen aan de aanbevelingen van de Centrale Raad voor het Bedrijfsleven van 17 december 2008.¹³⁰ Dit geval had bijvoorbeeld kunnen spelen in hypothese 2. I had mogelijks kunnen pleiten dat ze toegang moest hebben tot alle onderdelen van het dossier dat het bedrijfsgeheim bevatte op grond van haar recht op informatie. Waardoor ze de bedrijfsgeheimen op een rechtmatige manier had kunnen verkrijgen.

Het laatste geval is niet één bepaald geval, maar een ruime bepaling die voorschrijft dat het verkrijgen van een bedrijfsgeheim rechtmatig is als het verkregen wordt via iedere andere praktijk die in overeenstemming is met de eerlijke handelspraktijken gezien de omstandigheden.¹³¹ De laatste paragraaf van artikel XI.332/3 WER heeft een algemeen karakter en stipuleert dat zowel het gebruiken, openbaar maken als het verkrijgen van een bedrijfsgeheim rechtmatig is voor zover dit gebruiken, openbaar maken of verkrijgen vereist of toegestaan is door het Unierecht of het nationale recht.¹³² Dit doet denken aan artikel XI.332/2 waarin qua inhoud iets gelijkaardigs is te vinden.

In artikel XI.332/2 WER zijn een aantal bepalingen uit artikel 1, lid 2 van de Richtlijn Bedrijfsgeheimen overgenomen. Ten gevolge hiervan is in dit artikel een vrijwaringsbepaling opgenomen en wordt bijgevolg o.a. bepaald dat de bepalingen van de Wet Bedrijfsgeheimen geen afbreuk mogen doen aan de uitoefening van fundamentele rechten met nadruk op het recht op vrijheid van meningsuiting en het recht op vrijheid van informatie. Daarbij, zijn er bepalingen die voorschrijven wanneer bedrijfsgeheimen openbaar gemaakt kunnen worden door houders van bedrijfsgeheimen of door instellingen en organen van de Europese Unie of van de nationale overheid aan rechterlijke of administratieve instanties.¹³³ Het belangrijkste in dit artikel is de tweede paragraaf waarin is vastgelegd dat de bepalingen inzake bedrijfsgeheimen niet mogen worden gebruikt als een grond om de mobiliteit van werknemers te beperken. Daarna wordt benadrukt dat met betrekking tot de uitoefening van deze mobiliteit de bepalingen geen enkele grond vormen om werknemers te beperken in het gebruik van informatie die geen bedrijfsgeheim vormt noch om hen te beperken in het gebruik van vaardigheden en ervaringen die zij op een eerlijke wijze tijdens de normale uitoefening van hun functie hebben verkregen noch om hen andere aanvullende beperkingen op te leggen in hun arbeidsovereenkomsten dan degene die zijn opgelegd in overeenstemming met het Unierecht of het nationale recht.

De laatste uitzonderingen zijn neergelegd in artikel XI.332/5 WER. Dit artikel omschrijft vier gevallen wanneer een verzoek om de toepassing van de procedures, rechtsmiddelen en maatregelen inzake het onrechtmatig gebruiken, openbaar maken of verkrijgen van een bedrijfsgeheim zal worden afgewezen.

Het eerste geval is wanneer de verkrijging, het gebruik of de openbaarmaking van het bedrijfsgeheim plaatsvond tijdens de uitoefening van het recht op vrijheid van meningsuiting en het recht op vrijheid

¹³⁰ Wetsontwerp betreffende de bescherming van bedrijfsgeheimen, *Parl.St.* Kamer 2017-2018, nr. 54-3154/001, 14-15.

¹³¹ Artikel XI.332/3, §1, 4° WER.

¹³² Artikel XI.332/3, §2 WER.

¹³³ Artikel XI.332/2, §1, 1°-3° WER.

van informatie, met inbegrip van de eerbiediging van het recht van de vrijheid en het pluralisme van de media.¹³⁴

Het tweede geval betreft de situatie wanneer de verkrijging, het gebruik of de openbaarmaking plaatsvond bij het onthullen van wangedrag, illegale activiteiten of fouten. Een bijkomende voorwaarde voor deze situatie is dat de verweerder handelde met het oog op de bescherming van het algemeen openbaar belang. Een passend voorbeeld hierbij is een klokkenluider die te goeder trouw handelt.¹³⁵ Deze uitzondering had in elk van de 3 hypothesen kunnen gebeuren. Stel dat L door het raadplegen van de bedrijfsgeheimen op de laptop ontdekte dat Q elk jaar miljoenen euro's illegaal naar een rekening in de Kaaimaneilanden sluisde. Als ze dit dan bekend had gemaakt, zou dit geen onrechtmatige handeling hebben gevormd.

De derde uitzondering handelt over het geval wanneer het bedrijfsgeheim openbaar wordt gemaakt door werknemers aan hun vertegenwoordigers in de context van de rechtmatige uitoefening van hun vertegenwoordigende functies overeenkomstig het Unierecht of het nationale recht. Opnieuw is hier een bijkomende voorwaarde die eist dat deze openbaarmaking noodzakelijk was voor de uitoefening van de vertegenwoordigende functies.¹³⁶ Dit had bijvoorbeeld kunnen plaatsvinden in hypothese 2. Stel dat L het noodzakelijk vond om één of meerdere bedrijfsgeheimen openbaar te maken aan vertegenwoordigers in de ondernemingsraad van X, omdat uit de bedrijfsgeheimen blijkt dat de werkgever X dikwijls foutieve informatie meedeelt aan de ondernemingsraad. De ondernemingsraad heeft immers een ruime adviesbevoegdheid en zonder de juiste informatie, kan de ondernemingsraad niet met kennis van zaken adviseren. Hierdoor is de werking van de ondernemingsraad belemmerd en kan de ondernemingsraad niet goed worden uitgeoefend.¹³⁷ Bijgevolg zou de openbaarmaking van L in dit geval niet onrechtmatig zijn.

De laatste uitzondering is dat het gebruiken, verkrijgen of openbaar maken van het bedrijfsgeheim plaatsvond met het oog op de bescherming van een rechtmatig belang dat erkend is in het Unierecht of het nationale recht.¹³⁸

¹³⁴ Artikel XI.332/5, 1° WER.

¹³⁵ Overweging 20 Richtlijn Bedrijfsgeheimen. In deze overweging staat immers te lezen dat indien de verweerder alle redenen had om te goeder trouw te veronderstellen dat zijn handelen voldeed aan de vermelde criteria dat hij onder de uitzondering van artikel XI.332/5, 2° WER moet kunnen vallen. Hieruit kan afgeleid worden dat er zodoende geen daadwerkelijk sprake moet zijn van illegale activiteiten, fouten of wangedrag vermits de klokkenluider te goeder trouw handelde; Artikel XI.332/5, 2° WER.

¹³⁶ Artikel XI.332/5, 3° WER.

¹³⁷ Artikel 14 en 15 Wet 24 september 1948 houdende organisatie van het bedrijfsleven, *BS* 27 september 1948, 7768; FEDERALE OVERHEIDSDIENST WERKGELEGENHEID, ARBEID EN SOCIAAL OVERLEG, *Ondernemingsraad – werking en opdrachten*, <https://werk.belgie.be/nl/themas/sociaal-overleg/overlegorganen-en-procedures-binnen-de-onderneming-or-cpbw-va-ea-7> (consultatie op 20 april 2021).

¹³⁸ Artikel XI.332/5, 4° WER.

Hoofdstuk V Heeft de Wet Bedrijfsgeheimen zijn doel bereikt in het kader van telewerken?

Uit het onderzoek van het voorgaande hoofdstuk is duidelijk geworden op welke manier de Wet Bedrijfsgeheimen een impact kan hebben op telewerkers die thuis werken en de mensen in hun al dan niet " nabije " omgeving. De wet lijkt op het eerste zicht zeer impactvol te zijn, maar is dit werkelijk zo? Een vraag die zich hierdoor opdringt, betreft dan ook in welke mate de Wet Bedrijfsgeheimen zijn doel bereikt heeft in het kader van telewerken.

Toen deze wet werd voorbereid in 2018, had de wereld nog nooit van Corona gehoord en was telewerken absoluut nog niet de standaard. Daarom zal in dit hoofdstuk worden nagegaan of de wet zijn doel om bedrijfsgeheimen te beschermen heeft bereikt in context van telewerken ondanks het feit dat de wet niet was gemaakt met dit voor ogen. Waarom is dit belangrijk om te achterhalen? Omdat indien blijkt dat de wet niet voldoende adequate bescherming biedt, dan betekent dit dat de wetgever dringend moet ingrijpen. Zeker gezien het feit dat de kans groot is dat telewerken niet meer zal verdwijnen. Want zo zijn er al enkele bedrijven die hebben aangekondigd dat ze permanent overschakelen naar telewerken.¹³⁹ Aldus is er nood aan een wet die bedrijfsgeheimen goed en effectief beschermt in het kader van telewerken.

Het eerste wat opvalt aan de wet, is dat er over telewerken zelf niets is terug te vinden, maar dit is heel logisch, aangezien er vroeger nog geen nood bestond aan telewerk zoals op dit ogenblik. Niemand, waaronder de Belgische wetgever, had ooit kunnen voorspellen dat telewerk zo noodzakelijk zou worden als in de jaren 2020 en 2021. Het feit dat er niks specifiek over telewerken staat vermeld, wil daarom niet automatisch betekenen dat de wet heeft gefaald. Doordat de voorziene bepalingen zo ruim zijn omschreven, kunnen ze ook worden toegepast in de context van telewerk zoals kon worden opgemerkt in de hypothesen van het vorige hoofdstuk.¹⁴⁰

Een tweede bedenking is dat de vraag of de wet zijn doel heeft bereikt vanuit twee verschillende perspectieven kan worden beantwoord. Want de bescherming van bedrijfsgeheimen kan op twee verschillende manieren gebeuren, met name preventief en repressief. Het is vanuit deze invalshoek dat er op deze vraag een antwoord zal worden geformuleerd.

V.A Repressief

Wanneer de vraag betreffende de doelstelling van de wet – met name het beschermen van bedrijfsgeheimen – beantwoord wordt vanuit een repressieve visie, dan zou men eerder geneigd zijn om te zeggen van wel.

Voordat de Wet Bedrijfsgeheimen in werking trad, bestond er in België nog geen wettelijk kader rond bedrijfsgeheimen. Hierdoor werden getroffen partijen genoodzaakt om zich te beroepen op andere bepalingen, zoals artikel 1382 BW om alsnog genoegdoening te krijgen van de inbreukpleger.¹⁴¹

¹³⁹ T. AERTGEERTS en S. VAN WASSENHOVE, *Coworking*, Antwerpen, Intersentia, 2020, 19-21; PARTENA, *Thuiswerken 2.0: wat na de quarantainemaatregelen?*, <https://www.partena-professional.be/nl/nieuws/thuiswerken-20-wat-na-de-quarantainemaatregelen>.

¹⁴⁰ *Supra* Hoofdstuk IV – IV.C Hypotheses.

¹⁴¹ Cass. 2 november 2012, AR C.11.0018.N, *TBO* 2013, nr. 2, 84-88.

Dankzij deze wet is er wel eindelijk een wettelijke grondslag voor de houders van bedrijfsgeheimen om op te treden tegen inbreukmakers. De maatregelen die hen ter beschikking staan, zijn in het vorige hoofdstuk uitvoerig uiteengezet.¹⁴² Wat opmerkelijk is aan deze maatregelen, is dat het voornamelijk om repressieve maatregelen gaat. Het zijn bijna allemaal maatregelen die pas genomen kunnen worden nadat het geheime karakter van het bedrijfsgeheim al geschonden is.

Kijk bijvoorbeeld naar de mogelijkheid om aan de rechter de staking te bevelen van de openbaarmaking. Dit kan pas worden bevolen nadat de rechter heeft vastgesteld dat er sprake is van onrechtmatige openbaarmaking van een bedrijfsgeheim.¹⁴³ Idem voor de mogelijkheid van de houder van een bedrijfsgeheim om de afgifte van inbreukmakende goederen te verzoeken aan de rechter in het kader van zijn het recht op schadevergoeding. Hij kan dit enkel doen nadat de inbreukmakende goederen gemaakt zijn op grond van een onrechtmatig verkregen bedrijfsgeheim.¹⁴⁴ Hetzelfde gaat op voor het nemen van voorlopige en bewarende maatregelen door kortgedingrechter. Er zullen pas om deze maatregelen verzocht kunnen worden wanneer het kwaad al geschied is.¹⁴⁵ Een laatste voorbeeld is de boete waar tot iemand kan worden veroordeeld wegens schending van het verbod tot openbaarmaking of gebruik van bedrijfsgeheimen binnen het kader van gerechtelijke procedures in artikel 871*bis* Ger.W. Deze geldboete, die 500 tot 25.000 euro kan bedragen, kan pas worden opgelegd nadat iemand het verbod heeft geschonden.

Bovendien, zou buiten de wet om ook beroep kunnen worden gedaan op andere artikelen om de schending van het bedrijfsgeheim aan te klagen. In het kader van een arbeidsovereenkomst bij telewerkers zijn de meest voor de hand liggende artikelen; artikel 18 AOW en artikel 1184 BW indien de geheimhoudingsplicht gebaseerd op artikel 17, 3^o, a AOW is verbroken.¹⁴⁶ Op grond hiervan kan de werkgever een schadevergoeding vragen. Indien er een derde bij betrokken is, zou het leerstuk van derde medeplichtigheid aan andermans contractbreuk de grondslag vormen om deze derde in rechte aan te spreken.¹⁴⁷ Opnieuw gaat het hier om repressieve maatregelen.

Aan het repressieve is nochtans wel een groot minpunt en dat heeft betrekking op de bewijslast in de procedures. In principe ligt de bewijslast bij de houder van een bedrijfsgeheim om aan te tonen dat er een bedrijfsgeheim voorhanden is en dat dit geheim is geschonden. Afhankelijk van de feiten van een casus is het niet moeilijk om in te beelden dat dit niet altijd gemakkelijk zal zijn om aan te tonen. In eerste instantie moet de houder van een bedrijfsgeheim beseffen dat er een bedrijfsgeheim gestolen is en dan moet hij bijkomend weten wie hiervoor verantwoordelijk is. Het klinkt misschien absurd, maar wanneer dit in de context van telewerken geplaatst wordt, is het al helemaal onbegonnen werk. Neem bijvoorbeeld hypothese 2 waarin een werknemer per ongeluk bedrijfsgeheimen stuurt naar een collega. Hoe zou de houder van een bedrijfsgeheim dit weten als geen van de twee betrokkenen hierover iets zegt? Wat als deze collega het online had geplaatst en dit door verscheidene anderen verspreid werd. Hoe kan de houder dan weten wie hij moet

¹⁴² *Supra* Hoofdstuk IV – IV.D. Hoe kan een werkgever (houder van een bedrijfsgeheim) optreden?.

¹⁴³ Zie artikel XI.336/3, §1, 1^o WER.

¹⁴⁴ Zie artikel XI.336/5, §3 WER.

¹⁴⁵ 584 Ger.W.; *Supra* Hoofdstuk IV – IV.D. Hoe kan een werkgever (houder van een bedrijfsgeheim) optreden?.

¹⁴⁶ Artikel 18 AOW vereist bedrog, zwarte schuld of herhaaldelijke lichte fout. Het schenden van een bedrijfsgeheim kan gezien worden als zware fout afhankelijk van de schade die de werkgever hierdoor oploopt; D. HEYLEN en I. VERREYNT, *Arbeidsrecht toegepast (zesde editie)*, Antwerpen, Intersentia, 2018, 213.

¹⁴⁷ Zie artikel 1382 BW; S. STIJNS, *Leerboek verbintenissenrecht – Boek 1*, Brugge, die Keure, 2016, 243-247.

aanspreken? Wat als het een casus is dat betrekking heeft op inbreukmakende goederen; hoe kan de houder dan bewijzen dat dit vervaardigd is op grond van zijn onrechtmatig verkregen bedrijfsgeheim? In de rechtspraak werd hierover geoordeeld dat de houder in feite gedeeltelijk negatief bewijs moet leveren, met andere woorden zou hij moeten bewijzen dat de informatie die zijn bedrijfsgeheim vormt niet algemeen gekend is. De rechter in deze zaak verkoos bijgevolg voor een beperkte verdeling van de bewijslast waarbij de inbreukmaker moest bewijzen dat de relevante informatie wél algemeen gekend was.¹⁴⁸

Uit het voorgaande kan besloten worden dat op het vlak van repressieve maatregelen dat de Wet Bedrijfsgeheimen wel wat te bieden heeft. Waardoor men geïnclineerd zou zijn om te zeggen dat bedrijfsgeheimen inderdaad beschermd worden in het kader van telewerken. Er is echter wel ruimte voor verbetering, zeker op het vlak van de bewijslast, maar dit komt in het volgende hoofdstuk aan bod.

V.B Preventief

Het is vanuit de preventieve invalshoek waar de Wet Bedrijfsgeheimen flagrant tekortschiet. De voorziene preventieve maatregelen in de wet kunnen bij wijze van spreken op één hand geteld worden.

Een van de weinige preventieve maatregelen betreft artikel 17, 3^o, a AOW. Gezien het thema van deze scriptie, is deze preventieve maatregel het meeste besproken en behoeft het nog weinig extra uitleg.¹⁴⁹ Dit artikel komt erop neer dat een werknemer zich zowel tijdens zijn arbeidsovereenkomst als na de beëindiging ervan zich moet onthouden van het gebruiken, openbaar maken of verkrijgen van bedrijfsgeheimen waarvan hij kennis heeft gekregen tijdens het uitoefenen van zijn werk. Het gelast de werknemer en ex-werknemer dus op voorhand om bedrijfsgeheimen te bewaren.

De volgende regeling houdt verband met het eerder vermelde artikel 871*bis* Ger.W. In dit artikel is een vertrouwelijkheidsverplichting neergelegd voor alle gerechtelijke procedures waarin een bedrijfsgeheim wordt vermeld of gebruikt. Deze verplichting geldt zowel tijdens het lopen van de procedure als na het aflopen ervan en houdt in dat o.a. partijen, advocaten, gerechtelijk personeel, magistraten en alle andere personen die door hun deelname aan de procedure kennis krijgen van een bedrijfsgeheim dat ze dit geheim niet mogen openbaar maken of gebruiken.¹⁵⁰ Overigens kan de rechter ambtshalve of op verzoek van een belanghebbende partij bijkomende maatregelen nemen om de vertrouwelijkheid van het bedrijfsgeheim te bewaren.¹⁵¹ Een voorbeeld hiervan is de toegang tot documenten waarin bedrijfsgeheimen vervat zijn, beperken tot bepaalde personen.¹⁵² Hoewel deze bepaling als preventief kan worden gezien, moet worden aangestipt dat dit genuanceerd moet worden. Want deze regeling geldt voor gerechtelijke procedures, wat wil zeggen dat er mogelijk al een inbreuk op een bedrijfsgeheim is geweest die geleid heeft tot de gerechtelijke procedure. Als

¹⁴⁸ Voorz. Orb. Brussel 12 maart 2020, *RABG* 2020, afl.20, 1660-1669.

¹⁴⁹ *Supra* Hoofdstuk I – I.D Wijzigingen aan de wet van 3 juli 1978 (Arbeidsovereenkomstenwet).

¹⁵⁰ T. HEREMANS en F. BILLEN, "Bescherming van bedrijfsgeheimen in de vertrouwelijkheidskring", *IRDI* 2020, afl. 2, 181-183.

¹⁵¹ P. CAMPOLINI, "Chapitre 2 - Obtention, utilisation et divulgation illicites de secrets d'affaires après la transposition de la directive (UE) 2016/943" in V. CASSIERS (ed.), *Secrets d'affaires*, Brussel, Larcier, 2020, (43) 76-79.

¹⁵² Zie artikel 871*bis*, §2, 1^o Ger.W.

gevolg hiervan zou het beter zijn om de regeling op te vatten als een middel om verdere verspreiding van een bedrijfsgeheim te voorkomen.

In het verlengde van dit laatste, zou gesteld kunnen worden dat de maatregelen uit artikel XI.336/3 tevens gezien kunnen worden als het voorkomen van verdere verspreiding. Indien een rechter bijvoorbeeld de staking van de openbaarmaking van het bedrijfsgeheim beveelt dan zorgt dit ervoor dat het bedrijfsgeheim niet verder verspreidt.¹⁵³ Dit is evenzeer voor de andere maatregelen zoals het laten vernietigen van bestanden die het bedrijfsgeheim bevatten.¹⁵⁴ Opnieuw echter gelden deze maatregelen voor de situatie waarin er reeds een onrechtmatige handeling is geweest in verband met het bedrijfsgeheim. Bijgevolg kunnen ze moeilijk als werkelijk preventief bestempeld worden.

De laatste regel die aandacht verdient, zit vervat in de definitie van een bedrijfsgeheim, met name in artikel I.17/1, 1^o, c WER. Deze bepaling bevat het derde constitutieve element van een bedrijfsgeheim, namelijk de vereiste dat de houder redelijke maatregelen moet hebben genomen om de informatie geheim te houden.¹⁵⁵ Deze redelijke maatregelen zijn preventief, aangezien dit om maatregelen gaat die dienen om te verhinderen dat de geheime informatie verspreid wordt. Bovendien worden ze door de wet opgelegd, omdat de houder verplicht is om dit te doen als hij zijn informatie als bedrijfsgeheim wil kunnen kwalificeren.

Uit deze bespreking is duidelijk hoe beperkt de Wet Bedrijfsgeheimen is op het gebied van preventieve maatregelen. Dit is betreurenswaardig, omdat hierdoor de bescherming zo goed als volledig afhankelijk is van de inspanningen van de houder van een bedrijfsgeheim, aangezien de wet hem hier zó weinig ondersteuning biedt.

Vooral op het gebied van telewerken is er dringend nood aan verandering. Van de preventieve maatregelen die er zijn, kunnen er slechts twee toegepast worden op telewerken, met name de geheimhoudingsplicht uit de AOW en de redelijke maatregelen die de houder moet nemen. Twee is absurd weinig, vooral op een ogenblik waarin telewerken stilaan tot het nieuwe normaal behoort. Het is nog absurder dat de Belgische wetgever gekozen heeft voor een grotendeels repressieve invalshoek, want dan is het kalf al verdronken. Het enige wat men dan nog rest, is het proberen beperken van de verspreiding. Zeker gezien het tijdperk waar alles online de ronde doet, is het soms onmogelijk om iets van het internet te wissen. De vraag die peilt naar de bescherming van bedrijfsgeheimen vanuit preventieve invalshoek moet bijgevolg resoluut negatief beantwoord worden. De Wet Bedrijfsgeheimen slaagt er niet in om bedrijfsgeheimen te beschermen in het kader van telewerken door een gebrek aan maatregelen.

Tot dat de wetgever ingrijpt, zal de houder van een bedrijfsgeheim zelf zo veel mogelijk maatregelen moeten treffen om zijn bedrijfsgeheim te beschermen. Het beste zal een combinatie van maatregelen zijn, bv. contractuele geheimhoudingsplichten samen met technische maatregelen en het aantal personen die op de hoogte zijn zo beperkt mogelijk houden.¹⁵⁶

¹⁵³ Zie artikel XI.336/3, §1, 1^o WER.

¹⁵⁴ Zie artikel XI.336/3, §1, 6^o WER.

¹⁵⁵ *Supra* Hoofdstuk III – III. A Het begrip bedrijfsgeheimen.

¹⁵⁶ T. ROBRECHTS en M. VAN MEERBEECK, "De Belgische Wet Bedrijfsgeheimen een algemeen overzicht", *IRDI* 2018, afl. 3-4, 193.

Hoofdstuk VI Wat kan er beter aan de Wet Bedrijfsgeheimen in het kader van telewerken?

Uit de analyse van het vorige hoofdstuk kan worden afgeleid dat de Wet Bedrijfsgeheimen nog met een aantal pijnpunten kampt. Daarom zal in dit laatste hoofdstuk getracht worden om enkele aanbevelingen te formuleren die de wet ten goede zouden kunnen komen. Deze aanbevelingen zullen worden gebaseerd op alle voorgaande hoofdstukken en alle geconsulteerde bronnen. Daarnaast zal ook een rechtsvergelijking plaatsvinden met Duitsland om als inspiratie te dienen voor mogelijke bijkomende aanbevelingen. Deze rechtsvergelijking gaat enkel in op de Duitse implementatiewet van de Richtlijn Bedrijfsgeheimen waardoor de rechtsvergelijking beknopt zal zijn en eerder gezien moet worden als een rechtsvergelijking light. Hierdoor zullen niet alle bepalingen van deze wet behandeld worden. Enkel de bepalingen die (grondig) verschillen van de Belgische wet en zodoende kunnen leiden tot verbetering van de Belgische wet zullen worden bediscussieerd.

Om het hoofdstuk zo overzichtelijk mogelijk te houden, komt de rechtsvergelijking met Duitsland eerst aan bod, zodat daarna alle aanbevelingen één voor één besproken kunnen worden.

VI.A De Duitse implementatiewet

Duitsland heeft net zoals België (en alle andere lidstaten van de Europese Unie) de Richtlijn Bedrijfsgeheimen moeten omzetten. In Duitsland is deze implementatiewet - die de naam Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) bedraagt - op 26 april 2019 in werking getreden.¹⁵⁷

Het eerste verschil is dat Duitsland ervoor geopteerd heeft om een echte afzonderlijke wet te maken. Met als resultaat dat alle relevante artikelen met betrekking tot bedrijfsgeheimen te vinden zijn in hetzelfde wetgevend instrument. De wet bevat drieëntwintig artikelen en is onderverdeeld in vier verschillende secties.¹⁵⁸

Het volgende verschil heeft te maken met de bepaling inzake onrechtmatige handelingen, namelijk §4 Handlungsverbote.¹⁵⁹ In de Duitse wet wordt niets gezegd over het al dan niet hebben van de toestemming van de houder van een bedrijfsgeheim. Daarnaast, stelt deze bepaling dat een bedrijfsgeheim niet verkregen mag worden door eender welk gedrag, dat gezien de omstandigheden niet in overeenstemming is met het beginsel van goede trouw. Dit om rekening te houden met de eerlijke handelspraktijken.¹⁶⁰

Vervolgens bepaalt het artikel dat een bedrijfsgeheim niet gebruikt of openbaar mag worden gemaakt door iemand die het bedrijfsgeheim door een handeling uit paragraaf 1, het bedrijfsgeheim heeft verkregen.¹⁶¹ Voorts, mag een bedrijfsgeheim niet gebruikt of openbaar worden gemaakt door

¹⁵⁷ Gesetz zum Schutz von Geschäftsgeheimnissen 18 april 2019, *BGBI. I S.* 466, <http://www.gesetze-im-internet.de/geschgeh/BjNR046610019.html>; A. OHLY, "Das neue Geschäftsgeheimnisgesetz im Überblick", *GRUR* 2019, 441-442.

¹⁵⁸ Sectie 1 is het algemene deel en bevat vooral definities. Sectie 2 bevat de juridische vorderingen die ingesteld kunnen worden wegens inbreuk. Sectie 3 heeft betrekking op de procedures. De laatste sectie behandelt de strafrechtelijke voorschriften; K. REISERER, "Zwei Jahre Gesetz zum Schutz von Geschäftsgeheimnissen: Chancen, aber auch Risiken für alle Arbeitgeber", *DStR* 2021, afl. 18, 1053-1054.

¹⁵⁹ In de Belgische wet stemt deze bepaling overeen met artikel XI.332/4 WER.

¹⁶⁰ §4, (1), 2. GeschGehG.

¹⁶¹ §4, (2), 1. GeschGehG.

iemand die een verplichting schendt om het gebruik van een bedrijfsgeheim te beperken.¹⁶² Als laatste mag een bedrijfsgeheim niet gebruikt of openbaar worden gemaakt door iemand die een verplichting schendt om het bedrijfsgeheim niet te onthullen.¹⁶³ In Duitsland hebben werkgevers verscheidene grondslagen om geheimhoudingsclausules (Verschwiegenheitsverpflichtung) aan arbeidsovereenkomsten toe te voegen.¹⁶⁴ Bijvoorbeeld §241 Bürgerliches Gesetzbuch (BGB) en §611 BGB.¹⁶⁵

Het artikel bevat tevens nog een derde paragraaf, maar deze komt overeen met §3 en §4 van de Belgische tegenhanger.¹⁶⁶

Een volgend interessant verschil betreft §8 met als titel "Auskunft über rechtsverletzende Produkte; Schadensersatz bei Verletzung der Auskunftspflicht" wat vertaalt naar informatie over inbreukmakende goederen; schadevergoeding in geval van niet-nakoming van de informatieplicht. Dit is een artikel waarvan geen Belgische tegenhanger bestaat. Het laat de houder van een bedrijfsgeheim toe om informatie van de inbreukmaker te eisen, waaronder de persoon van wie zij het bedrijfsgeheim hebben verkregen en aan wie zij het hebben bekend gemaakt. Alsook de naam en het adres van de producenten, leveranciers en andere vorige eigenaars van de inbreukmakende goederen. De tweede paragraaf van deze bepaling voorziet in een schadevergoeding wanneer de inbreukmaker bewust of door grove nalatigheid geen, onjuiste, laattijdig of onvolledige informatie verstrekt.

Een ander verschil heeft betrekking op een bepaling die opnieuw geen Belgische tegenhanger heeft, namelijk §12 "Haftung des Inhabers eines Unternehmens" (Aansprakelijkheid van de eigenaar van een onderneming). Dit artikel geeft de houder van een bedrijfsgeheim de mogelijkheid om de vorderingen uit §§6 tot en met 8 in te stellen tegen de werkgever wanneer de inbreukmaker een werknemer of vertegenwoordiger is van deze laatste.

In de Duitse wet is net zoals in de Belgische wet een vertrouwelijkheidsverplichting verankerd in het kader van gerechtelijke procedures in §16.¹⁶⁷ Daar komt bij dat Duitsland deze bepaling versterkt heeft door middel van een aparte sanctie in §17 indien deze vertrouwelijkheidsverplichting geschonden wordt. Deze aparte sanctie houdt een geldboete in die maximaal 100.000 euro kan bedragen of een gevangenisstraf van maximaal zes maanden. Daar staat tegenover dat er in België enkel een geldboete is voorzien wegens schending van deze vertrouwelijkheidsverplichting.¹⁶⁸

Het laatste verschil is §23 "Verletzung von Geschäftsgeheimnissen" wat schending van bedrijfsgeheimen betekent. Deze bepaling is een strafrechtelijk voorschrift bestaande uit acht paragrafen, waarin o.a. geldboetes en vrijheidsstraffen zijn voorzien bij schending van bepalingen

¹⁶² §4, (2), 2. GeschGehG; *Supra* – Hoofdstuk IV – IV.C.2 Hypothese 2 – Situatieschets.

¹⁶³ §4, (2), 3. GeschGehG.

¹⁶⁴ Arbeitsgericht (DE) 3 juni 2020, *MMR* 2021, afl. 2, 181-184.

¹⁶⁵ Bürgerliches Gesetzbuch 18 augustus 1896, *BGBI. I S.* 42, 2909, <https://www.gesetze-im-internet.de/bgb/BJNR001950896.html>; M. BENECKE, "BGB § 611a Arbeitsvertrag – 6. Verschwiegenheitsverpflichtung", *BeckOK ArbR/Joussen* 2021, afl. 59, 463-471; H. KIEL, S. LUNK en H. OETKER, *Münchener Handbuch zum Arbeitsrecht*, München, C.H. Beck, 2018, 33-36.

¹⁶⁶ Artikel XI.332/4, §3 en 4 WER.

¹⁶⁷ 871bis Ger.W.

¹⁶⁸ 871bis, §4 Ger.W; Artikel 871bis Ger.W. stemt overeen met §§16-20 GeschGehG; MAKATSCH en KACHOLDT, "(2) Maßnahmen zum Schutz von Betriebs- und Geschäftsgeheimnissen und vertraulichen Informationen" in F. BIEN, F. JURGEN SACKER, P. MEIER-BECK en F. MONTAG, *Münchener Kommentar zum Wettbewerbsrecht*, München, C.H. Beck, 2020, (88) 88-92.

uit §4. Dergelijk artikel komt niet in de Belgische wet voor. Zo bepaalt paragraaf 1 dat eenieder die §4, (1), 1 of §4, (2), 1 of 3 schendt ter bevordering van zijn eigen concurrentievermogen of die van een derde, uit eigen belang, ten behoeve van een derde of met de bedoeling om de eigenaar van een bedrijf schade te berokkenen, gestraft kan worden met een vrijheidsstraf van hoogstens drie jaar of een geldboete. §23, (5) stelt de poging tot het plegen van de schending van bedrijfsgeheimen strafbaar. Tot slot vermeldt paragraaf 8 dat het misdrijf enkel vervolgd wordt op verzoek, tenzij de wetshandhavinginstantie het nodig acht om ambtshalve in te grijpen wegens speciaal openbaar belang.

VI.B Aanbevelingen

Nu dat alles besproken en onderzocht is in verband met bedrijfsgeheimen en telewerken, zijn er toch een aantal verbeterpunten die aandacht verdienen. Eerst zullen de verbeterpunten die voortvloeien uit de rechtsvergelijking licht aan bod komen. Vervolgens zullen de verbeterpunten die gebaseerd zijn op het onderzoek van de voorgaande hoofdstukken behandeld worden.

VI.B.1 Aanbevelingen gebaseerd op de rechtsvergelijking

Op basis van de rechtsvergelijking light kunnen de volgende aanbevelingen geformuleerd worden.

Doordat België in tegenstelling tot Duitsland gekozen heeft om bestaande wetgeving aan te passen, voelt de Belgische wetgeving in verband met bedrijfsgeheimen gefragmenteerd aan. Om alle bepalingen inzake bedrijfsgeheimen te consulteren, moet men beroep doen op verschillende wetgevende instrumenten. Dit bemoeilijkt bijgevolg het gebruik van de wetgeving door belanghebbenden. Bovendien is het belemmerend voor de rechtszekerheid. Stel dat een juridische leek zich wenst te beroepen op de Wet Bedrijfsgeheimen. Zonder de nodige juridische achtergrond, zou het voor hem moeilijk zijn om te weten op welke wetsartikelen hij zich precies moet beroepen. Het is tevens niet ondenkbaar dat hij hieromtrent twijfels zou hebben. Een mogelijke oplossing zou dus het maken van een afzonderlijke wetgeving zijn evenals Duitsland. De Belgische wetgever zou nog altijd bepaalde bestaande artikelen in hun huidige wetgevende instrumenten kunnen laten staan indien hij zou werken met verwijzingen zoals Duitsland. In de Duitse wet op bedrijfsgeheimen staan namelijk meerdere verwijzingen naar andere gerelateerde artikelen.¹⁶⁹ Zeker met het oog op telewerken, zou de Belgische wetgever verwijzingen naar de relevante bepalingen inzake telewerken kunnen toevoegen aan de Wet Bedrijfsgeheimen.

De Duitse wetgever heeft de bepaling betreffende onrechtmatige handelingen veel ruimer geformuleerd dan de Belgische wetgever.¹⁷⁰ Hierdoor lijken de bedrijfsgeheimen in Duitsland veel beter beschermd. Doordat de Belgische wetgever het ontbreken van toestemming als voorwaarde heeft gesteld voor het bestaan van een onrechtmatige handeling, vallen een aantal handelingen in een grijze zone. Stel dat een werknemer toestemming heeft verkregen tot de toegang van een bedrijfsgeheim en hij heeft dit bedrijfsgeheim met toestemming gekopieerd. Wat als de werknemer het opnieuw besluit te kopiëren in het kader van telewerken, maar voor deze handeling geen

¹⁶⁹ §1, (3), 1 verwijst bijvoorbeeld naar §203 van Strafgesetzbuch (het Duitse Strafwetboek). Dit artikel bevat het misdrijf schending van privégeheimen, waarin ook verwezen wordt naar bedrijfsgeheimen. In België komt dit overeen met artikel 458 Sw; C. ALEXANDER, "IV. Spezielle Vorschriften zum Schutz von Geschäftsgeheimnissen" in J. BORNKAMM, H. KOHLER, J. FEDDERSEN en C. ALEXANDER, *Gesetz gegen den unlauteren Wettbewerb: UWG*, München, C.H. Beck, 2021 (78) 81-83.

¹⁷⁰ §4 GeschGehG en artikel XI.332/4 WER.

toestemming heeft. Wat dan? Onder onrechtmatige verkrijging kan hij niet vallen, want hij had het bedrijfsgeheim al in zijn bezit. Onder onrechtmatige openbaarmaking of gebruik valt hij ook niet, want hij maakt het niet openbaar en hij gebruikt het niet. Omdat er echter geen andere mogelijkheid is, zou hij alsnog onder onrechtmatige verkrijging vallen, maar het is merkbaar dat dit geen ideale oplossing is. In de Duitse wet zou de handeling van deze werknemer zonder twijfel wel onder onrechtmatige handelingen vallen, aangezien de Duitse wet enkel spreekt over ongeautoriseerde toegang. Het zou de Belgische wet derhalve ten goede komen, indien het element van zonder toestemming uit artikel XI. 332/4 WER geschrapt zou worden. In het kader van telewerken zou de schrapping van dit element werkgevers meer rechtszekerheid kunnen geven. Ze zouden namelijk "makkelijker" ongeautoriseerde handelingen inzake hun bedrijfsgeheimen kunnen vervolgen. Om te kunnen telewerken worden er immers dikwijls bestanden gekopieerd of doorgestuurd naar collega's.¹⁷¹ Indien een werknemer dan iets kopieert, terwijl hij het al in zijn bezit had, zou de werkgever hem alsnog zonder problemen kunnen vervolgen wegens onrechtmatige verkrijging.

Een andere aanbeveling heeft betrekking op §8 GeschGehG dat de houder van een bedrijfsgeheim de mogelijkheid geeft om informatie te eisen van de inbreukmaker.¹⁷² De invoering van een soortgelijk artikel in de Belgische wet zou de bewijsproblematiek van de wet Bedrijfsgeheimen al dan niet gedeeltelijk kunnen verhelpen. Hierdoor zou de bewijslast niet meer volledig in handen liggen van de houder van een bedrijfsgeheim. De voorziene schadevergoeding die hieraan is gekoppeld, zou ook moeten worden overgenomen. Dit zou inbreukmakers aansporen om tijdig, correcte informatie mee te delen. Zeker in het kader van telewerken zou dit werkgevers enorm kunnen helpen. Zonder deze mogelijkheid zou het veel moeilijker zijn om te achterhalen wie het bedrijfsgeheim heeft doorgegeven of om alle documenten en bestanden op te sporen die het bedrijfsgeheim bevatten.

In het verlengde hiervan verdient §12 eveneens te worden opgenomen in de Wet Bedrijfsgeheimen.¹⁷³ Op grond van dit artikel kan de houder van een bedrijfsgeheim een vordering instellen tegen de werkgever wanneer zijn werknemer of vertegenwoordiger de inbreukmaker blijkt te zijn. Dergelijk artikel werkt preventief, want dit kan werkgevers aansporen om hun werknemers en vertegenwoordigers het schenden van bedrijfsgeheimen van anderen te ontmoedigen. In de context van telewerk zou dit tevens iets positief zijn, want het geeft werkgevers mogelijk meer gemoedsrust om hun werknemers te laten telewerken.

Het volgende verbeterpunt houdt verband met artikel 871*bis* Ger.W.¹⁷⁴ De Duitse wetgever heeft met een gelijkaardige vertrouwelijkheidsverplichting gewerkt, maar de voorziene sancties wegens schending hiervan zijn strenger in de Duitse wet. De Belgische wetgever slechts een geldboete voorzien die maximaal 25.000 euro kan bedragen terwijl de Duitse wet een geldboete van maximaal 100.000 euro voorziet of een gevangenisstraf van maximaal zes maanden. Vermits de openbaarmaking van bedrijfsgeheimen enorme financiële gevolgen kan hebben voor de houder

¹⁷¹ *Supra* Hoofdstuk IV – IV.C.2 Hypothese 2 – Situatieschets.

¹⁷² *Supra* Hoofdstuk VI – VI.A De Duitse implementatiewet.

¹⁷³ *Supra* Hoofdstuk VI – VI.A De Duitse implementatiewet.

¹⁷⁴ Dit stemt overeen met §16-20 GeschGehG.

ervan, zou het beter zijn als de Belgische wetgever de schending van de vertrouwelijkheidsverplichting zwaarder zou bestraffen.

Respectievelijk, het laatste verbeterpunt op grond van de rechtsvergelijking light betreft §23.¹⁷⁵ De Duitse wet bedrijfsgeheimen bevat een strafrechtelijk voorschrift met zowel geldboetes als vrijheidsstraffen. De Wet Bedrijfsgeheimen heeft geen vergelijkbaar artikel. In het Belgische strafwetboek is echter wel artikel 309 Sw. terug te vinden, maar dit artikel spreekt over "*hij die geheimen van de fabriek..*". Dit artikel heeft enkel betrekking op fabrieksgeheimen en niet op bedrijfsgeheimen. Desalniettemin vallen fabrieksgeheimen wel onder bedrijfsgeheimen, maar het probleem hiermee is dat bedrijfsgeheimen een veel ruimer begrip is.¹⁷⁶ Zodoende zouden bepaalde bedrijfsgeheimen er niet onder vallen en kan er aldus geen beroep gedaan worden op artikel 309 Sw. Daarom verdient het de aanbeveling om de bewoording fabrieksgeheimen uit artikel 309 Sw aan te passen naar bedrijfsgeheimen. Verder zou er een verwijzing naar dit artikel moeten komen in de Wet Bedrijfsgeheimen. In het kader van telewerken zou dergelijk artikel werkgevers meer vertrouwen kunnen geven in het telewerken zelf. Indien er alsnog een onrechtmatige handeling zou plaatsvinden, dan zou de werkgever een extra maatregel hebben waarop hij zich kan beroepen.

VI.B.2 Aanbevelingen gebaseerd op de rest van het onderzoek

Op dit moment lijkt de Wet Bedrijfsgeheimen vooral gericht op onrechtmatige handelingen door werknemers en niet door concurrenten of derden. De reeds voorgestelde toevoeging van §12 zou ervoor zorgen dat de wet zich meer focust op concurrenten. Daarbuiten zouden andere bepalingen die meer de nadruk leggen op concurrenten of derden wenselijk zijn. Er zou bijvoorbeeld een artikel XI.332/4/1 toegevoegd kunnen worden dat zich volledig toelegt op concurrenten. Het zou een kopie kunnen zijn van XI.332/4 WER, maar dan met de bepalingen toegespitst op onrechtmatige handelingen door bedrijven in de stijl van artikel VI. 103/1-109 WER. Om het artikel kracht bij te zetten, zouden hieraan zware geldboetes gekoppeld kunnen worden wegens de schending van het oneerlijke concurrentieverbod. Voor telewerken zou een gelijkaardig artikel kunnen worden toegevoegd, waarbij tevens verwezen wordt naar de relevante wetgeving, bv. CAO nr. 85 en 149. Om de wet beter te structureren, zou men dan kunnen werken met verschillende afdelingen. Een algemene afdeling waarin het oude XI.332/4 WER zou passen; een afdeling inzake B2B en een afdeling inzake telewerken.

Een ander punt dat verbetering behoeft, is artikel I.17/1, 1^o, a WER. Hierin staat neergelegd dat informatie geheim moet zijn wat wil zeggen niet algemeen gekend of gemakkelijk toegankelijk om onder het begrip bedrijfsgeheim te vallen. Het probleem met deze bepaling is dat dit subjectief beoordeeld wordt. Iemand kan bijvoorbeeld denken dat zijn informatie een bedrijfsgeheim vormt, maar uiteindelijk hangt het af van de persoonlijke appreciatie van de rechter. Hierdoor kunnen er meningsverschillen ontstaan, wat al effectief gebeurd is in de rechtspraak. Zo oordeelde de voorzitter van de ondernemingsrechtbank te Antwerpen dat niet elke gevoelige bedrijfsinformatie onder het begrip bedrijfsgeheim valt.¹⁷⁷ Aansluitend hierop lijkt de rechtspraak een precieze identificatie van

¹⁷⁵ *Supra* Hoofdstuk VI – VI.A De Duitse implementatiewet.

¹⁷⁶ *Supra* Hoofdstuk I – I.D Wijzigingen aan de wet van 3 juli 1978 (Arbeidsovereenkomstenwet); *Supra* Hoofdstuk III – III.A Het begrip bedrijfsgeheimen.

¹⁷⁷ Voorz. Orb. Antwerpen 16 oktober 2019, *IRDI* 2020, afl. 1, 109.

de informatie te vereisen.¹⁷⁸ Dit is echter niet af te leiden uit de voorwaarden van artikel I.17/1, 1°, a WER. Op grond hiervan lijkt het aangeraden om een instantie op te richten waarbij mensen die denken te beschikken over een bedrijfsgeheim kunnen navragen of ze er effectief onder vallen. Dit zou onaangename verrassingen in juridische procedures kunnen voorkomen.

Daaropvolgend zou artikel I.17/1, 1°, c WER verbeterd moeten worden. Deze bepaling vereist dat er redelijke maatregelen genomen moeten worden om de informatie geheim te houden.¹⁷⁹ De Belgische wetgever heeft hier wel voorbeelden van gegeven, maar desalniettemin is deze bepaling afhankelijk van het persoonlijk oordeel van de rechter.¹⁸⁰ In een arrest van de ondernemingsrechtbank te Antwerpen van 9 mei 2019 had de houder van een bedrijfsgeheim nagelaten om een geheimhoudingsplicht op te nemen in een overeenkomst met een externe dienstverlener. Hoewel menig persoon geneigd zou zijn om te denken dat hierdoor niet voldoende redelijke maatregelen waren genomen, oordeelde de rechter dat er toch sprake was van een bedrijfsgeheim.¹⁸¹ Aldus zou artikel I.17/1 WER gebaat zijn met een begeleidend artikel waarin meer uitleg gegeven wordt over redelijke maatregelen. Er zouden bv. een aantal elementen in kunnen worden opgenomen of mogelijk criteria zodoende dat potentiële houders van een bedrijfsgeheim hun maatregelen hieraan kunnen toetsen. Er valt te denken aan een aantal voorbeelden van contractuele maatregelen, zoals een geheimhoudingsplicht; technische maatregelen zoals beveiligde documenten en fysieke maatregelen zoals beperkte toegang tot het apparaat waarop de bedrijfsgeheimen zich bevinden.

Het volgende aandachtspunt is gebaseerd op de analyses van de zelfverzonnen hypotheses uit hoofdstuk vier.¹⁸² De hypotheses peilden vooral naar onrechtmatige handelingen van werknemers, maar het werd al snel duidelijk dat derden hier ook onder konden vallen. Er was bewust gekozen voor kwaadwillige derden, maar het is niet ondenkbaar dat bv. de partner thuis per ongeluk een bedrijfsgeheim opent op de laptop van zijn/haar telewerkende partner. Moeten dergelijke personen werkelijk even zwaar gestraft worden als diegenen die bewust onrechtmatige handelingen plegen? De wet maakt immers geen onderscheid tussen opzet of onachtzaamheid.¹⁸³ In het kader van de schadevergoeding uit artikel XI.3365/5 WER, bestaat nochtans wel de mogelijkheid om de aansprakelijkheid van werknemers te beperken wanneer deze zonder opzet heeft gehandeld. Dit is op grond van artikel 18 AOW waarin voorgeschreven is dat de werknemer tijdens de uitvoering van zijn arbeidsovereenkomst enkel aansprakelijk is voor bedrog, zware schuld en herhaaldelijke lichte schuld.¹⁸⁴ Er zou bijvoorbeeld een wetsartikel toegevoegd kunnen worden dat verzachtende omstandigheden bevat en sancties die lichter zijn dan de andere wetsartikelen.

¹⁷⁸ Corr. Leuven 12 november 2019, onuitg., 14; Voorz. Orb. Antwerpen 26 maart 2020, AR 20/19/C, onuitg.; J. LINDEMANS en M. MARIANO, "Belgische rechtspraak inzake bedrijfsgeheimen: 10 vragen (en antwoorden) na 1.000 dagen nieuwe wet", *ICIP-Ing.Cons.* 2020, afl. 3, 603-605.

¹⁷⁹ *Supra* Hoofdstuk III – III.A Het begrip bedrijfsgeheimen.

¹⁸⁰ V. DE LE COUR en N. HEREMANS, "Secrets d'affaires et devoir de diligence: quelles mesures raisonnables pour protéger les secrets d'affaires?", *RDC* 2020, afl. 3, 386-390.

¹⁸¹ Orb. Antwerpen 9 mei 2019, *RDC* 2020, afl. 3, 380-383.

¹⁸² *Supra* Hoofdstuk IV – IV.C Hypotheses.

¹⁸³ Er is enkel een kennisvereiste in artikel XI.332/4, §3 en 4 WER, zie *supra* Hoofdstuk IV – IV.C.4.1 Inbreukmaker.

¹⁸⁴ Wetsontwerp betreffende de bescherming van bedrijfsgeheimen, *Parl.St.* Kamer 2017-2018, nr. 54-3154/001, 18-21; F. HENDRICKX, *Inleiding tot het Belgische Arbeidsrecht*, Brugge, die Keure, 2021, 123-126.

De voorlaatste aanbeveling is eerder een algemeen verbeterpunt en slaat terug op de analyse over de doeltreffendheid van de Wet Bedrijfsgeheimen.¹⁸⁵ De wet bevat voornamelijk repressieve maatregelen en weinig preventieve maatregelen. De Belgische wetgever zou bijvoorbeeld een verplicht aantal maatregelen kunnen opleggen die houders van bedrijfsgeheimen moeten nemen om hun bedrijfsgeheimen te beschermen. Deze maatregelen zouden verband kunnen houden met de redelijke maatregelen uit artikel I.17/1, 1°, c WER. Bijvoorbeeld verplicht hen om een bepaald minimumniveau van IT-beveiliging te hebben om alle elektronische bestanden die bedrijfsgeheimen bevatten te beschermen. Laat werknemers enkel telewerken op bedrijfslaptops met een bepaald minimumniveau van beveiliging. Verplicht bedrijven om elektronische bestanden met bedrijfsgeheimen te versleutelen. Een andere mogelijkheid is de verplichting om geheimhoudingsclausules in de arbeidsovereenkomsten en telewerkovereenkomsten op te nemen met hieraan een boete gekoppeld bij overtreding. Deze verplichtingen zouden zeker ook gepast zijn in het kader van telewerken.

Tot slot, verdient de bewijsproblematiek in de procedures eveneens belangstelling. Met de huidige wetgeving ligt de bewijslast volledig bij de houder van een bedrijfsgeheim. Eerder is al voorgesteld om een Belgische tegenhanger van §8 GeschGehG in te voeren.¹⁸⁶ Om dergelijk artikel te versterken, zou gedacht kunnen worden om de bewijslast bij de inbreuker te leggen, wanneer de inbreuker een contractuele geheimhoudingsplicht heeft geschonden. Aangezien de houder van een bedrijfsgeheim zijn aandeel al had gedaan door zo'n geheimhoudingsplicht in te voeren, zou hij beloond moeten worden door de bewijslast om te keren. Een alternatief is het invoeren van een algemeen kader inzake beslag in het kader van bedrijfsgeheimen. Op dit moment is dit enkel mogelijk in de context van artikel 584, vijfde lid, ten zesde Ger.W. bij een procedure in kortgeding. In de voorbereidende werken besloot de Belgische wetgever om geen beslag in te voeren wegens angst tot misbruik van de procedure.¹⁸⁷ Als gevolg hiervan staat de houder van een bedrijfsgeheim soms voor een onmogelijk karwei wanneer hij moet bewijzen dat de tegenpartij zijn bedrijfsgeheim onrechtmatig heeft verkregen, openbaar gemaakt of gebruikt. Wanneer hierbij nog eens het telewerken wordt betrokken, wordt het alleen maar erger wegens een gebrek aan een gecontroleerde omgeving.

¹⁸⁵ *Supra* Hoofdstuk V Heeft de Wet Bedrijfsgeheimen zijn doel bereikt in het kader van telewerken?.

¹⁸⁶ *Supra* Hoofdstuk VI – VI.B.1 Aanbevelingen gebaseerd op de rechtsvergelijking.

¹⁸⁷ Wetsontwerp betreffende de bescherming van bedrijfsgeheimen, *Parl.St.* Kamer 2017-2018, nr. 54-3154/001, 9; K. NEEFS, "Over vissers in bewijsnood: Bewijsbeslag & bedrijfsgeheimen", *IRDI* 2018, afl. 3-4, 223-224.

Conclusie

Deze scriptie is aangevat met als doel onderzoek te doen naar de impact van de Wet betreffende de bescherming van bedrijfsgeheimen op werknemers die thuis werken. Om een antwoord te kunnen vinden op deze centrale onderzoeksvraag, is er gewerkt met verscheidene subvragen. Deze subvragen corresponderen met de verschillende uitgewerkte hoofdstukken in deze scriptie. De eerste drie hoofdstukken zijn theoretisch teneinde een goede basis te kunnen maken, alvorens over te gaan naar de toepassing en analyse van deze wet. De andere drie hoofdstukken zijn een toepassing van deze onderzochte theorie.

Hoofdstuk I heeft de Wet Bedrijfsgeheimen onder de loep genomen. Hierin werd onderzocht hoe deze wet zelf eruitzag. Uit dit onderzoek werd al snel duidelijk dat de Belgische wetgever geen aparte wet inzake bedrijfsgeheimen heeft gemaakt. In de plaats daarvan is gekozen om bestaande wetgeving daar waar nodig is, aan te passen. De voornaamste gewijzigde instrumenten door de Wet Bedrijfsgeheimen zijn het Wetboek Economisch recht, het Gerechtelijk Wetboek en de Arbeidsovereenkomstenwet.

In lijn hiervan deed hoofdstuk II onderzoek naar de achtergrond van deze wet. Dit achtergrondonderzoek werd gedaan om de wet beter te kunnen begrijpen. Dit hoofdstuk was opgesplitst in twee delen. In het eerste deel werd de voorgeschiedenis van de Europese richtlijn behandeld. Hieruit kwam voort dat de Europese Unie al jaren eerder haar zinnen had gezet op bedrijfsgeheimen voordat de richtlijn het licht zag. In het tweede deel kwam de richtlijn zelf kort aan bod.

Het laatste theoretische hoofdstuk is Hoofdstuk III, waarin het begrip bedrijfsgeheimen uiteen werd gezet. Het voornaamste wat uit dit hoofdstuk onthouden moet worden, is dat er drie constitutieve voorwaarden moeten zijn vervuld om informatie als een bedrijfsgeheim te kunnen kwalificeren. Ten eerste, moet de informatie geheim zijn. Ten tweede, moet de informatie handelswaarde bezitten doordat ze geheim is. Als laatste moet deze informatie onderworpen worden aan redelijke maatregelen om de informatie geheim te houden. Wat interessant was aan het onderzoek van deze voorwaarden, is dat bovenkwam dat de invulling van deze voorwaarden afhangt van de persoonlijke appreciatie van de rechter. Want noch de Europese wetgever noch de Belgische wetgever hebben richtlijnen of criteria vastgelegd hoe deze voorwaarden moeten worden ingevuld.

Daarna komt het eerste praktische hoofdstuk wat meteen ook de essentie van deze scriptie vormt. In hoofdstuk IV werd namelijk onderzocht wat de impact is van de Wet Bedrijfsgeheimen op werknemers die thuis werken. Logischerwijze is dit het meest omvattende hoofdstuk en is het opgedeeld in vijf delen, waarbij sommige delen nog eens verder opgesplitst zijn. Om dit hoofdstuk nog beter in te kaderen, werd in de eerste deel het verschil tussen de begrippen telewerken en thuiswerken verklaard. Daarna werd er gewerkt met zelfverzonnen hypothesen om aan te tonen hoe de wet en telewerken samen kunnen spelen. Om deze hypothesen te beoordelen, werden de begrippen inbreukmaker en onrechtmatige handelingen uitvoerig behandeld en vervolgens toegepast. Hieruit was af te leiden dat de wet gemakkelijk kon worden toegepast in het kader van telewerken. In het voorlaatste deel werd toegelicht welke juridische stappen een werkgever als houder van een bedrijfsgeheim kan ondernemen.

In hoofdstuk V werd vervolgens gepeild of de Wet Bedrijfsgeheimen zijn doel had bereikt in de context van telewerken. De wet werd immers gemaakt op een moment waarin telewerken slechts uitzonderlijk plaatsvond. Om dit na te gaan, werden twee perspectieven gebruikt, met name een repressief en preventief perspectief. Vanuit de repressieve invalshoek kon worden besloten dat de wet zijn doel had bereikt, vermits het merendeel van de artikelen repressief van aard zijn. Vanuit het preventieve perspectief moest besloten worden dat de wet zijn doel niet had bereikt. Dit valt te verklaren vanwege o.a. het feit dat de wet, de houders van een bedrijfsgeheim allesbehalve aanspoort om preventieve maatregelen te nemen, zeker in de context van telewerken.

Het sluitstuk van deze scriptie bestaat uit hoofdstuk VI waarin aanbevelingen voor de Wet Bedrijfsgeheimen geformuleerd worden. Dit hoofdstuk bestaat opnieuw uit twee delen. In het eerste deel werd de Duitse implementatiewet van de Richtlijn Bedrijfsgeheimen beknopt behandeld. Duitsland moest immers ook de richtlijn omzetten en de Duitse wetgever had duidelijk een andere aanpak dan de Belgische wetgever. Omdat de Belgische wet niet artikelsgewijs besproken is, werd ervoor gekozen om enkel de Duitse artikelen te bespreken die verschillen van de Belgische wet. Vervolgens werd het tweede deel opgesplitst om de aanbevelingen te formuleren. In het eerste subdeel werden aanbevelingen aan de hand van de Duitse rechtsvergelijking opgesteld. In het laatste subdeel ten slotte werden de aanbevelingen gebaseerd op de rest van het onderzoek. In beide delen konden een aantal aanbevelingen geformuleerd worden. Wat erop wijst dat de Wet Bedrijfsgeheimen allesbehalve volmaakt is.

Op grond van het gevoerde onderzoek moet aldus de centrale vraag beantwoord worden als zijnde dat de Wet Bedrijfsgeheimen een waarneembare impact heeft op telewerkers. Door de analyses van de hypotheses uit hoofdstuk vier, kon de interactie van telewerken en de wet snel worden waargenomen. Voor telewerkers die thuis werken geldt de wet dus onverlet. Zij moeten dus ook in hun eigen woning waakzaam blijven dat zij de bedrijfsgeheimen van hun werkgever blijven respecteren. Alhoewel dit in principe positief is, zijn er toch enkele problemen. Zo werd het al snel duidelijk dat inbreuken op bedrijfsgeheimen ontzettend vlug gebeuren. Daarnaast, voorziet de wet vooral repressieve maatregelen en weinig preventieve maatregelen. Als werkgevers hun bedrijfsgeheimen willen beschermen en dit vooral in de context van telewerken, moeten ze werkelijk zelf het heft in eigen handen nemen, door een combinatie van verscheidene preventieve maatregelen te nemen. Dit is betreurenswaardig, omdat de Wet Bedrijfsgeheimen specifiek als doel heeft om bedrijfsgeheimen te beschermen. Hoewel de wet niet gemaakt was met het oog op telewerken, heeft de wet desalniettemin een merkbare impact. De impact zou echter groter kunnen zijn als de voorgestelde aanbevelingen aan de wet zouden worden toegevoegd.

Bibliografie

Wetgeving

Belgische wetgeving

- ❖ Richtl.Raad.EP. nr. 2004/48, 29 april 2004 betreffende de handhaving van intellectuele-eigendomsrechten, *Pb.L.* 30 april 2004, afl. 157.
- ❖ Richtl.Parl. nr. 2016/943, 8 juni 2016 betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken daarvan, *Pb.L.* 15 juni 2016, afl. 157.
- ❖ Voorstel (Comm.) voor een richtlijn van het Europees Parlement en de Raad betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken daarvan, 28 november 2013, COM(2013)813 def - 2013/0402(COD).
- ❖ COMMISSION STAFF WORKING DOCUMENT, *IMPACT ASSESSMENT Accompanying the document Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*, 28 november 2013, SWD(2013) 471 final.
- ❖ COMMISSION STAFF WORKING DOCUMENT, *Implementation Plan Accompanying the document Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*, 28 november 2013, SWD(2013) 493 final.
- ❖ Burgerlijk wetboek.
- ❖ Gerechtelijk Wetboek.
- ❖ Strafwetboek.
- ❖ Wetboek van Economisch recht.
- ❖ Wet 24 september 1948 houdende organisatie van het bedrijfsleven, *BS* 27 september 1948, 7768.
- ❖ Wet 12 april 1965 betreffende de bescherming van het loon der werknemers, *BS* 30 april 1965, 4710 (Loonbeschermingswet).
- ❖ Wet van 5 december 1968 betreffende de collectieve arbeidsovereenkomsten en de paritaire comités, *BS* 15 januari 1969, 267.

- ❖ Wet 3 juli 1978 betreffende de arbeidsovereenkomsten (Arbeidsovereenkomstenwet/AOW), *BS* 22 augustus 1978, 9277.
- ❖ Wet 5 maart 2017 betreffende werkbaar en wendbaar werk, *BS* 15 maart 2017, 35718.
- ❖ Wet 30 juli 2018 betreffende de bescherming van bedrijfsgeheimen, *BS* 14 augustus 2018, 64584 (Wet Bedrijfsgeheimen).
- ❖ Wet 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *BS* 5 september 2018, 68616.
- ❖ Wet 5 september 2018 tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG, *BS* 10 september 2018, 69589.
- ❖ KB 22 november 2006 betreffende het telewerk in het federaal administratief openbaar ambt, *BS* 1 december 2006, 66747.
- ❖ CAO nr. 81 van 26 april 2002 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische onlinecommunicatiegegevens, <http://www.cnt-nar.be/CAO-COORD/cao-081.pdf>.
- ❖ CAO nr. 85/1 van 9 november 2005 betreffende het telewerk, gewijzigd door de collectieve arbeidsovereenkomst nr. 85 bis van 27 februari 2008, <http://www.cnt-nar.be/CAO-COORD/cao-085.pdf>.
- ❖ CAO nr. 149 van 26 januari 2021 betreffende aanbevolen of verplicht telewerk omwille van de coronacrisis, [http://www.cnt-nar.be/CAO-ORIG/cao-149-\(26.01.2021\).pdf](http://www.cnt-nar.be/CAO-ORIG/cao-149-(26.01.2021).pdf).
- ❖ Wetsontwerp betreffende de bescherming van bedrijfsgeheimen, *Parl.St.* Kamer 2017-2018, nr. 54-3154/001.

Buitenlandse wetgeving

- ❖ Wereldhandelsorganisatie (WTO) Overeenkomst inzake de handelsaspecten van de intellectuele eigendom (TRIPS) van 15 april 1994, https://www.wto.org/english/docs_e/legal_e/27-trips.pdf.
- ❖ Strafgesetzbuch (StGB) 15 mei 1871, *BGBI. I S. 3322*, <https://www.gesetze-im-internet.de/stgb/BJNR001270871.html>.
- ❖ Bürgerliches Gesetzbuch 18 augustus 1896, *BGBI. I S. 42, 2909*, <https://www.gesetze-im-internet.de/bgb/BJNR001950896.html>.
- ❖ Gesetz zum Schutz von Geschäftsgeheimnissen 18 april 2019, *BGBI. I S. 466*, <http://www.gesetze-im-internet.de/geschgehg/BJNR046610019.html> (GeschGehG).

Rechtspraak

Belgische rechtspraak

- ❖ HvJ 14 maart 2017, nr. C-162/15, ECLI:EU:C:2017:205, Evonik Degussa/Commissie.
- ❖ HvJ 19 juni 2018, nr. C-15/16, ECLI:EU:C:2018:464, Baumeister.
- ❖ HvJ 8 juli 2019 nr. C-543/17, ECLI:EU:C:2019:573.
- ❖ Cass. 27 september 1943, *Pas.* 1943, I, 358.
- ❖ Cass. 2 november 2012, AR C.11.0018.N, *TBO* 2013, nr. 2, 84-88.
- ❖ Cass. 5 oktober 2020, *Soc.Weg.* 2021, afl. 5, 21-24.
- ❖ Arbh. Antwerpen 12 september 2019, *IRDI* 2019, afl. 2, 160-165.
- ❖ Arbh. Brussel 26 januari 2018, *Soc.Kron.* 2020, afl. 1, 21.
- ❖ Arbh. Brussel 2 juli 2019, nr. 2018/AB/278.
- ❖ Corr. Leuven 12 november 2019, onuitg., 14.
- ❖ Orb. Antwerpen 9 mei 2019, *RDC* 2020, afl. 3, 380-383.
- ❖ Voorz. Orb. Antwerpen 16 oktober 2019, *IRDI* 2020, afl. 1, 109.
- ❖ Voorz. Orb. Antwerpen 26 maart 2020, AR 20/19/C, onuitg.
- ❖ Voorz. Orb. Brussel 12 maart 2020, *RABG* 2020, afl.20, 1660-1669.

Buitenlandse rechtspraak

- ❖ Arbeitsgericht (DE) 3 juni 2020, *MMR* 2021, afl. 2, 181-184.

Rechtsleer

Belgische rechtsleer

Boeken

- ❖ AERTGEERTS, T. en VAN WASSENHOVE, S., *Coworking*, Antwerpen, Intersentia, 2020, 90 p.
- ❖ CAMPOLINI, P., "Chapitre 2 - Obtention, utilisation et divulgation illicites de secrets d'affaires après la transposition de la directive (UE) 2016/943" in CASSIERS, V. (ed.), *Secrets d'affaires*, Brussel, Larcier, 2020, 43-99.
- ❖ CASSIERS, V., "La protection des secrets d'affaires dans l'environnement numérique" in JACQUEMIN, H. en MICHAUX, B. (eds.), *Actualités en droit du numérique*, Limal, Anthemis, 2019, 99-136.
- ❖ HELLEMANS, L. en KARREMAN, E., *Telewerk en huisarbeid*, Mechelen, Kluwer, 2018, 112 p.
- ❖ HENDRICKX, F., *Inleiding tot het Belgische Arbeidsrecht*, Brugge, die Keure, 2021, 332 p.
- ❖ HEYLEN, D. en VERREYDT, I. *Arbeidsrecht toegepast (zesde editie)*, Antwerpen, Intersentia, 2018, 478 p.
- ❖ LORRE, J., *Sociale media en werkgeverscontrole*, Mechelen, Kluwer, 2012, 163 p.
- ❖ ROBERT, F. en TASKIN, L., *Le télétravail à domicile*, Limal, Anthemis, 2020, 292 p.
- ❖ STIJNS, S., *Leerboek verbintenissenrecht – Boek 1*, Brugge, die Keure, 2016, 590 p.

Tijdschriften

- ❖ AERTS, A., "De arbeidsrechtelijke aspecten van de nieuwe Wet op de Bedrijfsgeheimen", *IRDI* 2018, 240-249.
- ❖ CASSIERS, V., "La directive 2016/943/UE du 8 juin 2016 sur les secrets d'affaires", *JT* 2017, nr. 21, 385-397.
- ❖ CLAEYS, C., "Bescherming van bedrijfsgeheimen. Nieuwe regeling", *NJW* 2019, afl. 396, 98-105.
- ❖ DE LE COUR, V. en HEREMANS, N. "Secrets d'affaires et devoir de diligence: quelles mesures raisonnables pour protéger les secrets d'affaires?", *RDC* 2020, afl. 3, 384-391.

- ❖ DE VREY, R., "De totstandkoming van de Richtlijn Bedrijfsgeheimen", *IRDI* 2016, afl. 2, 144-149.
- ❖ DERIJCKE, W. en MALHERBE, O., "Vous me copierez cent fois... », l'article 871bis du Code judiciaire et la protection du secret d'affaires dans les procédures judiciaires", *JT* 2020, afl. 40, 837-848.
- ❖ DEVROE, L., PHILIPPE, D. en VAN NOYEN, T., "Protection des secrets d'affaires. Analyse de la loi du 30 juillet 2018 transposant la directive (UE) 2016/943 ", *DAOR* 2019, afl. 132, 3-23.
- ❖ GEENTJENS, P., "Van bits naar atomen: naar een opensourcemodel voor fysieke objecten?", *Jura Falc.* 2019, afl. 3, 429-536.
- ❖ HEREMANS, T., BILLEN, F., "Bescherming van bedrijfsgeheimen in de vertrouwelijkheidskring", *IRDI* 2020, afl. 2, 180-184.
- ❖ JORIS, T. en VAN DER JEUGHT, S., "Hof van Justitie – 8 juli 2019", *RW* 2020, afl. 27, 1078-1080.
- ❖ LINDEMANS, J. en MARIANO, M., "Belgische rechtspraak inzake bedrijfsgeheimen: 10 vragen (en antwoorden) na 1.000 dagen nieuwe wet", *ICIP-Ing.Cons.* 2020, afl., 599-616.
- ❖ NEEFS, K., "Over vissers in bewijsnood: Bewijsbeslag & bedrijfsgeheimen", *IRDI* 2018, afl. 3-4, 222-228.
- ❖ ROBRECHTS, T. en VAN MEERBEECK, M., "De Belgische Wet Bedrijfsgeheimen: een algemeen overzicht", *IRDI* 2018, afl. 3-4, 182-193.
- ❖ VANHEES, H., "De nieuwe wettelijke regeling betreffende de bescherming van bedrijfsgeheimen", *RW* 2018-2019, afl. 42, 1642-1660.

Varia

- ❖ CCBE, *CCBE position European Commission proposal for a Directive on the protection of undisclosed know-how and business information (trade secret) against their unlawful acquisition, use and disclosure (COM(2013) 813 final, 2013/0402 (COD))*, https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/DEONTOLOGY/DEON_Postion_Papers/EN_DEON_20141031_CCBE_Trade_secrets.pdf.

- ❖ COM (2012), *REPORT EUROPEAN COMMISSION CONFERENCE OF 29 JUNE 2012 "TRADE SECRETS: SUPPORTING INNOVATION, PROTECTING KNOW-HOW"*, <https://ec.europa.eu/docsroom/documents/14836?locale=fr>.
- ❖ COM(2010)2020, *EUROPA 2020 - Een strategie voor slimme, duurzame en inclusieve groei*, 52010DC2020, <https://www.eumonitor.nl/9353000/1/j9vvik7m1c3gyxp/vio0dsna8gzx>.
- ❖ COM(2011)287, *Eengemaakte markt voor intellectuele-eigendomsrechten - Creativiteit en innovatie bevorderen met het oog op economische groei, kwaliteitsjobs en eersteklasproducten en -diensten in Europa*, Brussel, 24 mei 2011, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0287:FIN:NL:PDF>.
- ❖ EFJ, *Trade secrets versus public interest: Open letter to European institutions*, <https://europeanjournalists.org/blog/2015/10/13/trade-secrets-versus-public-interest-open-letter-to-european-institutions/>.
- ❖ EPHA, *Joint statement | EU trade secrets directive threat to health, environment, free speech and worker mobility*, <https://epha.org/joint-statement-eu-trade-secrets-directive-threat-to-health-environment-free-speech-and-worker-mobility/>.
- ❖ EUR LEX, *Document 32016L0943 - Datums*, <https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX%3A32016L0943>.
- ❖ EUR LEX, *Procedure 2013/0402/COD*, <https://eur-lex.europa.eu/legal-content/NL/HIS/?uri=CELEX:32016L0943>.
- ❖ EUR LEX, *Richtlijnen van de Europese unie*, <https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=LEGISSUM:I14527>.
- ❖ EUROPA NU, *EU 2020-strategie*, https://www.europa-nu.nl/id/vicyffri83lm/eu_2020_strategie.
- ❖ EUROPESE COMMISSIE, *Public consultation on the protection against misappropriation of trade secrets and confidential business information*, https://ec.europa.eu/growth/content/public-consultation-protection-against-misappropriation-trade-secrets-and-confidential_nl.
- ❖ FEDERALE OVERHEIDSDIENST WERKGELEGENHEID, ARBEID EN SOCIAAL OVERLEG, *Update: Coronavirus: preventiemaatregelen en arbeidsrechtelijke gevolgen*, <https://werk.belgie.be/nl/nieuws/update-coronavirus-preventiemaatregelen-en-arbeidsrechtelijke-gevolgen>.

- ❖ FEDERALE OVERHEIDSDIENST WERKGELEGENHEID, ARBEID EN SOCIAAL OVERLEG, *Update: Coronavirus: preventiemaatregelen en arbeidsrechtelijke gevolgen – In welke ondernemingen is telethuiswerk verplicht?*, <https://werk.belgie.be/nl/nieuws/update-coronavirus-preventiemaatregelen-en-arbeidsrechtelijke-gevolgen>.

- ❖ FEDERALE OVERHEIDSDIENST WERKGELEGENHEID, ARBEID EN SOCIAAL OVERLEG, *Huisarbeid – arbeiders in de publieke sector*, <https://werk.belgie.be/nl/themas/arbeidsovereenkomsten/bijzondere-arbeidsovereenkomsten/huisarbeid-en-telewerk/huisarbeid-1>.

- ❖ FEDERALE OVERHEIDSDIENST WERKGELEGENHEID, ARBEID EN SOCIAAL OVERLEG, *Ondernemingsraad – werking en opdrachten*, <https://werk.belgie.be/nl/themas/sociaal-overleg/overlegorganen-en-procedures-binnen-de-onderneming-or-cpbw-va-ea-7>.

- ❖ LOVELLS, H., *Report on trade Secrets for the European Commission*, London, 23 september 2011, http://publications.europa.eu/resource/cellar/068c999d-06d2-4c8e-a681-a4ee2eb0e116.0001.02/DOC_1, 71 p.

- ❖ PARTENA, *Thuiswerken 2.0: wat na de quarantainemaatregelen?*, <https://www.partena-professional.be/nl/nieuws/thuiswerken-20-wat-na-de-quarantainemaatregelen>.

- ❖ RAAD VAN EUROPA, *Persmededeling Concurrentievermogen (Interne Markt, Industrie, Onderzoek en Ruimtevaart)*, 26 mei 2016, 10226/14.

- ❖ SDWORX, *22% van de telewerkers werkt nog elke dag van thuis*, <https://www.sdworx.be/nl-be/pers/2020/2020-09-21-22-percent-van-de-telewerkers-werkt-nog-elke-dag-van-thuis>.

- ❖ TELEWERKEN, *In cijfers – Enquête september 2020 bij 1500 werkenden: bijna 1 op 2 doet aan telewerken!*, <https://www.telewerken.be/in-cijfers/>.

- ❖ X, *Study on Trade Secrets and Confidential Business Information in the Internal Market*, April 2013, MARKT/2011/128/D, <https://ec.europa.eu/docsroom/documents/14838/attachments/1/translations/en/renditions/pdf>, 160 p.

Buitenlandse rechtsleer

Boeken

- ❖ ALEXANDER, C., "IV. Spezielle Vorschriften zum Schutz von Geschäftsgeheimnissen" in BORNKAMM, J., KOHLER, H., FEDDERSEN, J. en ALEXANDER, C., *Gesetz gegen den unlauteren Wettbewerb: UWG*, München, C.H. Beck, 2021 78-84.
- ❖ KIEL, H., LUNK, S. en OETKER, H., *Münchener Handbuch zum Arbeitsrecht*, München, C.H. Beck, 2018, 33-36. 3860 p.
- ❖ MAKATSCH en KACHOLDT, "(2) Maßnahmen zum Schutz von Betriebs- und Geschäftsgeheimnissen und vertraulichen Informationen" in BIEN, F., JURGEN SACKER, F., MEIER-BECK, P. en MONTAG, F., *Münchener Kommentar zum Wettbewerbsrecht*, München, C.H. Beck, 2020, 88-100.

Tijdschriften

- ❖ BENECKE, M. "BGB § 611a Arbeitsvertrag – 6. Verschwiegenheitsverpflichtung", *BeckOK ArbR/Joussen* 2021, afl. 59, 1014-1025.
- ❖ OHLY, A., "Das neue Geschäftsgeheimnisgesetz im Überblick", *GRUR* 2019, 441-451.
- ❖ REISERER, K., "Zwei Jahre Gesetz zum Schutz von Geschäftsgeheimnissen: Chancen, aber auch Risiken für alle Arbeitgeber", *DStR* 2021, afl. 18, 1053-1056.

Varia

- ❖ COCACOLACOMPANY, *Coca-Cola's Formula Is at the World of Coca-Cola*, <https://www.coca-colacompany.com/news/coca-cola-formula-is-at-the-world-of-coca-cola>.
- ❖ HOGAN LOVELLS, *About us*, <https://www.hoganlovells.com/en/about-us>.
- ❖ MYERS, B., *Even KFC's Head Chef Doesn't Know the Secret Recipe*, <https://www.thedailymeal.com/eat/kfc-secret-recipe-fried-chicken>.