

RECHTSLEER

DOCTRINE

ECONOMISCH STRAFRECHT / DROIT PÉNAL ÉCONOMIQUE

De straf(proces)rechtelijke impact van de Europese klokkenluidersrichtlijn: pleidooi voor een parlementair debat

Joris LAMBRECHTS¹

I. Inleiding	972
II. De richtlijn	973
§ 1. <i>Algemeen</i>	973
A. <i>De ratio achter de richtlijn</i>	973
B. <i>Gelden er beperkingen?</i>	974
§ 2. <i>Het toepassingsgebied</i>	974
A. <i>Materieel</i>	974
B. <i>Personeel</i>	974
1. <i>Wie kan melden?</i>	974
2. <i>Wie moet in bescherming voorzien?</i>	974
§ 3. <i>Hoe moet/kan gemeld worden?</i>	975
§ 4. <i>Waartegen biedt de richtlijn bescherming?</i>	975
III. Bijzondere vraagstukken van straf(proces)rechtelijke aard	976
§ 1. <i>Vrijwaring door de klokkenluider van diens eigen strafrechtelijke aansprakelijkheid</i>	976
A. <i>Algemeen</i>	976
B. <i>Kwalificatie handelingen klokkenluiders</i>	977
1. <i>Algemeen</i>	977
2. <i>Offline-misdrijven gepleegd door klokkenluiders</i>	977
C. <i>Gronden van verweer voor de klokkenluider</i>	980
1. <i>De mensenrechtelijke principes</i>	980
2. <i>De noodtoestand</i>	982
3. <i>Het algemeen of bedrieglijk opzet</i>	983
§ 2. <i>Vrijwaring van de resultaten van het onderzoek na het luiden van de klok: wat met Antigoon?</i>	984
IV. Conclusie	986

SAMENVATTING

Uiterlijk 17 december 2021 moet België richtlijn nr. 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 hebben omgezet. Deze heeft betrekking op de bescherming van personen die inbreuken op het Unierecht melden. Ondanks de cruciale rol die deze melders (of anders gezegd: klokkenluiders) innemen in onze hedendaagse maatschappij, blijft het voorlopig stil rond deze omzetting. Nochtans rijzen diverse juridische vragen waarop idealiter het parlement een antwoord biedt. Huidige bijdrage lijst enkele van deze vragen op in een straf(proces)rechtelijke context en formuleert een aanzet van antwoord.

¹ Manager Compliance & Forensics Finvision.

RÉSUMÉ

La Belgique doit avoir transposé la directive n° 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 au plus tard le 17 décembre 2021. Il s'agit de la protection des personnes qui signalent des infractions au droit de l'Union. Malgré le rôle crucial que jouent ces dénonciateurs (ou autrement dit: les lanceurs d'alerte) dans notre société contemporaine, on est pour l'instant discret sur cette transposition. Cependant, diverses questions juridiques se posent auxquelles idéalement le parlement devrait apporter une réponse. La contribution actuelle répertorie certaines de ces questions dans un contexte pénal (procédural) et formule une première réponse.

I. INLEIDING

Bij de redactie van huidige bijdrage scheiden slechts 5 maanden ons van de uiterlijke datum voor de omzetting van richtlijn nr. 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 inzake de bescherming van personen die inbreuken op het Unierecht melden. Uiterlijk op 17 december 2021 moeten de EU-lidstaten deze richtlijn ter bescherming van klokkenluiders² hebben omgezet in hun respectievelijk nationaal recht.³

De impact van de richtlijn oogt substantieel. Dit geldt in het bijzonder, maar niet uitsluitend, voor de private sector en ondernemingen/ondernemers hierin actief. Het bevreedt daarom dat tot op heden elk behoorlijk en breed gedragen parlementair debat ontbreekt. Met uitzondering van een wetsvoorstel van PVDA-PTB⁴ en voorstellen tot resolutie ingediend door Groen-Ecolo⁵ en DéFI⁶, blijft het stil vanuit wetgevende hoek. Langs de kant van de uitvoerende macht

is dit niet anders. De huidige federale regering engageerde zich expliciet⁷ de richtlijn binnen de termijn om te zetten. Maar de concretisering van dit engagement bleef tot op heden beperkt tot het uitschrijven en intussen gunnen van een aanbesteding⁸ voor bijstand bij implementatie van de richtlijn.

Het voorgaande staat in schril contrast met een andere ambitie van diezelfde federale regering. In haar regeerakkoord liet zij uitdrukkelijk noteren een democratische vernieuwing te beogen. Hiervoor zou worden gewerkt met een reeks hervormingen in de schoot van de regering én een reflectie-oefening in het parlement.⁹ De invoering van een brede bescherming voor klokkenluiders¹⁰ is een van de onderwerpen waarvoor zo'n reflectie-oefening zich leent.

Klokkenluiders zijn in een alsmaar transparanter wordende samenleving een belangrijke motor van maatschappelijke

² Hierna: de richtlijn.

³ Art. 26, 1. van de richtlijn. In afwijking op dit algemene principe, voorziet art. 26, 2. in de mogelijkheid deze inwerkingtreding uit te stellen ten aanzien van juridische entiteiten in de private sector met 50 tot 249. Zij kunnen voor hun interne meldkanalen (cf. *infra*) uitstel krijgen tot 17 december 2023.

⁴ Wetsvoorstel teneinde klokkenluiders een wettelijke status te verlenen en bescherming te bieden (*Parl.St.* Kamer 2019-20, nr. 55-1380/001).

⁵ Voorstel van resolutie over de bescherming van de fundamentele vrijheid van de klokkenluiders en de journalisten (*Parl.St.* Kamer 2019-20, nr. 55-1069/001). Deze fractie maakte toen nog geen deel uit van de huidige federale regering.

⁶ Voorstel van resolutie over legitieme maatregelen ter bescherming van klokkenluiders die ten bate van het algemeen belang vertrouwelijke informatie van overheidsorganisaties en van ondernemingen onthullen (*Parl. St.* Kamer 2020-21, nr. 55-1730/001).

⁷ Cf. p. 82 van het regeerakkoord van 30 september 2020. Een dergelijk engagement is in feite overbodig. Art. 288 van het verdrag betreffende de werking van de Europese Unie bepaalt sowieso dat een richtlijn (en dus ook de termijn waarbinnen zij uiterlijk dient omgezet te zijn in nationaal recht) verbindend is ten aanzien van het te bereiken resultaat en dit voor elke lidstaat waarvoor de richtlijn is bestemd. Het engagement van de huidige federale regering is dus niets meer dan een bevestiging van een al bestaande internationaalrechtelijke verplichting.

⁸ Bijzonder bestek nr. 2020/69615/E3/BAT/Omzetting richtlijn (EU) nr. 2019/1937 – Onderhandelingsprocedure zonder voorafgaande bekendmaking betreffende een studie betreffende de verplichtingen van de federale overheid op grond van richtlijn (EU) nr. 2019/1937 en omzetting in Belgische wetgeving.

⁹ P. 82 van het regeerakkoord van 30 september 2020.

¹⁰ Sommige Nederlandstalige auteurs pleiten voor het gebruik van de termen “melders” en “meldprocedures”. “Klokkenluiders” of “klokkenluidersregelingen” lijken te beladen termen (B. DE BIE en J. HOFKENS, *Doeltreffende klokkenluidersregelingen*, Mechelen, Kluwer, 2011, 18 en G. VYNCKIER, G. VANDE WALLE en P. DE BAETS, “Je hoeft de klokken niet te luiden om misstanden te melden: naar een normalisatie van meldprocedures in de professionele organisatie”, *Or.* 2015, afl. 72, 9). Andere Nederlandstaligen gebruiken de termen “melder”, “klokkenluider”, “meldpunt”, “klokkenluidersregeling” door elkaar (C. MANDERS, E. VAN FLORESTEIN en J. STAPPERS, “De Richtlijn bescherming klokkenluiders bezien vanuit Nederlands perspectief”, *Tijdschrift voor Compliance* 2019, afl. 6, 438-443). Dergelijke afwegingen zijn niet eigen aan Nederlandstaligen. Ook Franstalige en Engelstalige auteurs maken ze (cf. F. COTON en J.-F. HENROTTE, “Le lanceur d’alerte: une personne concernée par le traitement de ses données à caractère personnel, mais également par son avenir professionnel ...”, *RDTI* 2015, afl. 61, 44; A. LACHAPPELLE, “L’encadrement juridique du lancement d’alerte au sein de l’Union européenne”, *RDTI* 2020, afl. 78-79, 17-18; L. GROENEWALD, *Whistleblowing Management Handbook*, Pretoria, The Ethics Institute, 2020, 6 en A. LACHAPPELLE, *La dénonciation à l’ère des lanceurs d’alerte fiscale*, Brussel, Larcier, 2021, 38-49). In elk geval is het Nederlandstalige “klokkenluider” de oorspronkelijke vertaling van het Engelstalige begrip “whistleblower” zoals geformuleerd door BOVENS (M.A.P. BOVENS, *Verantwoordelijkheid en organisatie*, Zwolle, Tjeenk Willink, 1990, 261 et seq.) die zelf voortbouwde op de meest courante definitie van MICELI en NEAR (“Whistleblowing is the disclosure by organisation members (former or current) of illegal, immoral, or illegitimate practices under the control of their employees, to persons or organisations that may be able to effect action.” uit M.-P. MICELI en J.-P. NEAR, “Characteristics of organizational climate and perceived wrongdoing associated with whistle-blowing”, *Personnel Psychology* 1985, afl. 38, 525).

verandering.¹¹ Ze verdienen een bescherming waarvan de mogelijkheden en grenzen worden vastgesteld na een inhoudelijk overleg dat de klassieke meerderheid vs. minderheid discussie overstijgt. Dit biedt maatschappelijk draagvlak en rechtszekerheid voor alle betrokken partijen, zijnde de klokkenluider, de ontvanger van de melding, de onderneming die de klokkenluidersregeling moet implementeren en de betrokkene waarover wordt gemeld. Het rechtsdomein bij uitstek waar deze duidelijkheid moet zijn, is het straf(proces)recht. Meer nog dan voor elk ander vraagstuk is het cruciaal te weten wat de straf(proces)rechtelijke consequenties van ieders handelen (kunnen) zijn.¹²

Huidige bijdrage wil daarom een aanzet tot debat zijn en enkele straf(proces)rechtelijke bedenkingen formuleren. Die bedenkingen zijn niet noodzakelijk nieuw of exhaustief. Maar als het parlement de tijd neemt om fundamenteel na te denken over de omzetting van de richtlijn, kan het hieraan een bescheiden bijdrage leveren. Neemt het parlement die tijd niet, dan biedt deze bijdrage mogelijk een houvast voor hij/zij die in de toekomst de klok wil luiden, de melding opvolgen en zijn/haar eigen strafrechtelijke verantwoordelijkheid wil vrijwaren. Omdat de straf(proces)rechtelijke vragen onlosmakelijk samenhangen met de richtlijn zelf, worden eerst de krijtlijnen van die laatste besproken.

II. DE RICHTLIJN

§ 1. Algemeen

A. De ratio achter de richtlijn

De ratio achter de richtlijn is anders dan het onderwerp op het eerste gezicht doet vermoeden. Niet zozeer mensenrechtelijke principes liggen eraan ten grondslag. Wel economische overwegingen vormen de basis.¹³ Schandalen zoals *LuxLeaks*, de *Panama Papers* en *Football Leaks* betroffen in essentie fiscaal geïnspireerde meldingen met bijgevolg een impact op de (lid)statelijke inkomsten. Deze schandalen waren de ultieme hefboom om de richtlijn gestemd te krijgen. Ook was er een Europese studie uit 2017¹⁴ die het economisch verlies door de niet afdoende bescherming van klokkenluiders begrootte op 5,8 tot 9,6 miljard EUR op Europees niveau.¹⁵

Samen met de traditionele rol van de EU, maken deze elementen dat de richtlijn in de eerste plaats erop is gericht de

interne markt en de financieel-economische belangen van de EU te vrijwaren. Een vaststelling die op het eerste gezicht cynisch kan lijken. Men mag evenwel niet uit het oog verliezen dat dergelijke – aanvankelijk zuiver materiële – overwegingen ook meer inhoudelijke maatschappelijke verandering kunnen veroorzaken.¹⁶

Het welslagen van de richtlijn, waarbij private ondernemingen de bescherming van klokkenluiders en een hieraan gekoppeld compliancebeleid niet louter pro forma implementeren, hangt in sterke mate af van de meerwaarde die deze ondernemingen erin zien. Hoewel onze maatschappij zich zonder twijfel bewuster wordt van het belang van ethiek en duurzaamheid¹⁷, blijven “harde cijfers” toch het ultieme argument. Daarom is het interessant te weten dat een goede klokkenluidersregeling binnen private organisaties¹⁸ een uitstekend middel is om fraude te voorkomen of (snel) te detecteren.¹⁹ Men vermijdt dat problemen aanslepen of in de openbaarheid komen.²⁰ Meer algemeen is het een hoeksteen

¹¹. Zoals ook al gesteld in J. LAMBRECHTS, “Commotie over te snelle spuit ook aanzet voor spoedige omzetting Europese klokkenluidersrichtlijn”, *Juristenkrant* 2021, afl. 430, 16.

¹². Dit betekent vanzelfsprekend niet dat een toekomstige omzetting van de richtlijn geen andere vragen moet beantwoorden. Zie o.a. in dit meer algemene verband: J. LAMBRECHTS, “Europese Richtlijn ter bescherming van klokkenluiders: analyse van een (r)evolutie”, *NJW* 2021, afl. 435, 46-61.

¹³. A. LACHAPPELLE, “L’encadrement juridique du lancement d’alerte au sein de l’Union européenne”, *RDIT* 2020, afl. 78-79, 15-16.

¹⁴. J. MCGUINN, L. ROSSI en M. FERNANDES, *Estimating the economic benefits of whistleblower protection in public procurement*, 2017, www.europa.eu.

¹⁵. Deze begroting had bovendien uitsluitend betrekking op openbare aanbestedingen.

¹⁶. Cf. D. KAFERNARIS, “The future of the Whistle-blowing Directive: criticising its legal bases”, *Queen Mary Law Journal* 2021, afl. 1, 67-68 en A. LACHAPPELLE, *La dénonciation à l’ère des lanceurs d’alerte fiscale*, Brussel, Larcier, 2021, 672-673.

¹⁷. Zie bv. de 5^{de} wijziging van richtlijn nr. 2011/16 van 15 februari 2011 betreffende de administratieve samenwerking op het gebied van de belastingen en tot intrekking van richtlijn nr. 77/799/EEG (beter gekend als “DAC6”). Deze richtlijn verplicht fiscale tussenpersonen in specifieke gevallen tot melding van bepaalde grensoverschrijdende fiscale constructies. Meer algemeen formuleerde de Europese Commissie in april 2021 ook een richtlijn rond zgn. “Corporate Sustainability Reporting” die kadert in een sterk groeiende aandacht rond alles wat ESG-principes betreft (Environmental, Social and Corporate Governance).

¹⁸. Waar deze bijdrage zich op focust. Zij laat de publieke context buiten beschouwing.

¹⁹. Cf. ook § 47 van de preambule bij de richtlijn: “Voor een doeltreffende opsporing en preventie van inbreuken op het Unierecht is het van vitaal belang dat de relevante informatie snel degenen bereikt die het dichtst bij de bron van het probleem staan. (...) Dit beginsel moet bijdragen tot een cultuur van gedegen communicatie en maatschappelijk verantwoord ondernemen, waarbij melders worden geacht in aanzienlijke mate bij te dragen tot zelfreinigend vermogen en uitmuntendheid.” Hierbij kan ook verwezen worden naar de cijfers van de Association of Certified Fraud Examiners. In hun jaarverslag van 2020 (*Report to the Nations*) werd nogmaals bevestigd dat bijna de helft (43%) van alle fraudegevallen aan het licht komen door een tip. Een goed werkende klokkenluidersregeling (die tips faciliteert) is bijgevolg cruciaal.

²⁰. V. JUNOD, “La liberté d’expression du whistleblower” (noot onder EHRM 12 februari 2008), *Rev. trim. DH* 2009, afl. 77, 260 en C. MANDERS, E. VAN FLORESTEIN en J. STAPPERS, “De Richtlijn bescherming klokkenluiders bezien vanuit Nederlands perspectief”, *Tijdschrift voor Compliance* 2019, afl. 6, 442.

van ethisch en duurzaam ondernemerschap.²¹ Finaal kan het de eigen aansprakelijkheid van de onderneming vrijwaren.²²

B. Gelden er beperkingen?

De richtlijn is zo opgevat dat zij het status quo niet in negatieve zin kan beïnvloeden. Zij doet met name geen afbreuk aan bestaande (sectorspecifieke) bescherming van klokkenluiders die niet kan worden afgebouwd omdat de richtlijn een lagere standaard bepaalt (art. 3, 1.). Anderzijds kunnen lidstaten het toepassingsgebied (materieel of personeel) verruimen t.o.v. de richtlijn (art. 25). Lidstaten kunnen dus een verregaandere bescherming bieden dan vereist op Europees niveau.

Opnieuw in lijn met de traditionele invulling van het Europees recht, blijven enkele nationale prerogatieven van kracht. Overeenkomstig artikel 3, 2. en 3. is de richtlijn niet van toepassing op meldingen over openbare aanbestedingen die betrekking hebben op defensie of andere veiligheidsaspecten, tenzij die dan geregeld zijn door andere EU-regelgeving (art. 3, 2.). Ook doet de richtlijn geen afbreuk aan de verantwoordelijkheid van lidstaten hun eigen nationale veiligheid te regelen of de bevoegdheid hun essentiële veiligheidsbelangen te beschermen. Zij doet evenmin afbreuk aan:

- de bescherming van “*gerubriceerde gegevens*” (lees: geclassificeerde informatie die omwille van haar inhoud of aard slechts beperkt of zelfs geheel niet verspreid mag worden);
- het medisch beroepsgeheim en dat van advocaten;
- het geheim van het rechterlijk beraad; en
- straf(proces)rechtelijke regels.

§ 2. Het toepassingsgebied

A. Materieel

De richtlijn biedt bescherming voor klokkenluiders die zaken melden i.v.m. (art. 2, 1., a) – inbreuken op de EU-regelgeving rond) overheidsopdrachten, financiële diensten, producten en markten en het voorkomen van het witwassen van geld en de financiering van terrorisme, productveiligheid en -conformiteit, veiligheid van het vervoer, milieubescherming, stralingsbescherming en nucleaire veiligheid, veiligheid van levensmiddelen en diervoeders alsook dierengezondheid en -welzijn, volksgezondheid, consumentenbescherming en de bescherming van de persoonlijke levenssfeer en persoonsgegevens en de beveiliging van netwerken en informatiesystemen. Ook wanneer de financiële belangen

van de EU in het gedrang komen of de interne markt *in se* verstoord dreigt te raken, dan kan daarover gemeld worden (art. 2, 1., b) en c)). Lidstaten kunnen dit materiële toepassingsgebied uitbreiden (art. 2, 2.).

Een inbreuk is een onwettige handeling of nalatigheid waarbij volstaat dat het doel van de geschonden rechtsregel wordt omzeild (art. 5). Het volstaat om bescherming te genieten dat de klokkenluider gegronde redenen heeft op het moment van de melding om aan te nemen dat bepaalde informatie juist was (art. 6, 1.).

B. Personeel

1. Wie kan melden?

Zowel klokkenluiders uit de publieke als uit de private sector hebben recht op bescherming. De informatie die ze melden, moet vernomen zijn in een professionele/werk gerelateerde context. De richtlijn beschermt aldus werknemers, ambtenaren, zelfstandigen, aandeelhouders, leden van bestuurs-, leidinggevende of toezichthoudende organen van een onderneming (al dan niet belast met het dagelijks bestuur), vrijwilligers, (al dan niet bezoldigde) stagiairs en eenieder die werkt onder toezicht en leiding van aannemers, onderaannemers en leveranciers (art. 4, 1.).

Er mag ook informatie gemeld worden wanneer de samenwerking intussen eindigde (art. 3, 2.) of nog moet starten. Informatie bekomen tijdens het rekruteringsproces of tijdens een precontractuele fase is dus eveneens gevisieerd (art. 3, 3.).

De bescherming geldt ten slotte niet alleen t.a.v. de klokkenluider, maar ook t.a.v. facilitators²³, dit zijn derde personen gelieerd met de klokkenluider zoals collega's of familieleden en juridische entiteiten waarvan de klokkenluider eigenaar is, waarvoor hij werkt of op enige andere wijze mee verbonden is in een professionele context (art. 3, 4.). Vakbondsvertegenwoordigers vallen daar ook onder (§ 41 preambule).

2. Wie moet in bescherming voorzien?

Juridische entiteiten (in de private of publieke sector) moeten voorzien in een intern kanaal waarlangs gemeld kan worden en in procedures voor onderzoek van en rapportering over de meldingen. Dit gebeurt, waar het nationaal recht dit bepaalt, in overleg en in samenspraak met de sociale partners (art. 8, 1.). In de private sector geldt deze verplichting pas vanaf 50 medewerkers of meer (art. 8, 3.). Dit kanaal mag,

²¹ V. JUNOD, “Lanceur d’alerte: quoi de neuf depuis Guja?”, *Rev.trim.DH* 2014, 463.

²² Cf. F. VYNCKE, “La mise en place d’un programme effective d’intégrité”, *DAOR* 2010, afl. 93, 13-14 en A. LACHAPPELLE, *La dénonciation à l’ère des lanceurs d’alerte fiscale*, Brussel, Larcier, 2021, 156-157.

²³ Dit is een natuurlijke persoon die de klokkenluider bijstaat in het meldingsproces in een werkgerelateerde context en wiens bijstand vertrouwelijk moet zijn.

maar moet niet, intern beheerd worden.²⁴ Private ondernemingen met 50 tot 249 werknemers, mogen (als uitzondering op de regel) de krachten bundelen en gezamenlijk voorzien in een (desgevallend uitbestede) klokkenluidersregeling en -platform (art. 8, 6.).

§ 3. Hoe moet/kan gemeld worden?

Er zijn drie wegen om de klok te luiden:

- het interne kanaal: opgericht binnen de schoot van de onderneming (waarbij het eigenlijke beheer desgevallend wordt uitbesteed);
- het externe kanaal: opgericht door de overheid; of
- de openbaarmaking: dit is een publieke bekendmaking (bv. via klassieke media/persartikelen maar evengoed op platformen zoals *WikiLeaks*).

De klokkenluider moet voorrang geven aan een interne melding, vervolgens aan een externe melding en pas finaal opteren voor de publieke (desgevallend anonieme) bekendmaking (art. 7, 1. en 15). Is de melding anoniem in deze interne, externe of publieke fase, dan beslissen de lidstaten autonoom of hieraan verplicht een gevolg moet worden gegeven (art. 6, 2.). De lidstaten worden wel verondersteld de interne meldingskanalen boven de externe aan te moedigen. Indien de inbreuk doeltreffend kan worden behandeld en indien de klokkenluider van mening is dat er geen risico op represailles bestaat, zou hij een interne melding moeten kiezen (art. 7, 2.). De klokkenluider kan echter beslissen dit interne kanaal over te slaan en meteen het externe (vanuit de overheid opgerichte) kanaal te benutten.²⁵

Afhankelijk van de structuur en beperkte omvang van een onderneming kan het beheer van een melding gebeuren door een stafmedewerker die in een goede positie verkeert om rechtstreeks te melden aan het hoofd van de organisatie (zoals een compliance-verantwoordelijke, HR-manager, integriteitsmedewerker, jurist of privacy-verantwoordelijke, de CFO, de directeur audit of een lid van de raad van bestuur) (§ 56 preambule).

Klokkenluiders die beslissen hun melding publiek te maken, moeten aan bijkomende criteria voldoen om bescherming te genieten (*cf.* art. 15):

- eerst een interne en/of externe melding te hebben gedaan waaraan geen passend gevolg werd gegeven binnen de voorziene termijnen; of
- gegronde redenen te hebben om aan te nemen dat er een dreigend of reëel gevaar is voor het algemene belang of er een risico bestaat op represailles bij gebruik van het externe kanaal, het niet waarschijnlijk

is dat de inbreuk doeltreffend zal worden verholpen, de bijzondere omstandigheden het vereisen (bv. bewijsmateriaal dat dreigt te verdwijnen) of iemand uit het externe kanaal kan samenspannen met een persoon betrokken bij de inbreuk.

Klokkenluiders die rechtsreeks naar de pers stappen moeten niet aan deze criteria beantwoorden wanneer zij bescherming genieten op basis van (een eventueel nationale invulling van) het recht op vrije meningsuiting.

De lidstaten dienen (direct of indirect) ervoor te zorgen dat de identiteit van de klokkenluider vertrouwelijk blijft behoudens diens uitdrukkelijk andersluidend akkoord. Wel zijn er uitzonderingen mogelijk, zoals het recht op een eerlijk proces van de persoon waarover de melding wordt gedaan lopende een onderzoek of gerechtelijke procedure. Men zal indien mogelijk – dus tenzij dit het onderzoek of een gerechtelijke procedure zou dwarsbomen – de klokkenluider vooraf verwittigen dat zijn identiteit zal worden onthuld (art. 16).

§ 4. Waartegen biedt de richtlijn bescherming?

De richtlijn biedt klokkenluiders bescherming tegen elke vorm van (dreigen met of poging tot) represailles. Deze kunnen diverse vormen aannemen zoals (art. 19) schorsing, ontslag of een soortgelijke maatregel, degradatie of het onthouden van een bevordering, overdracht van taken, verandering van tewerkstellingslocatie, loonsverlaging of verandering van de werktijden, het onthouden van een opleiding, een negatieve prestatiebeoordeling of arbeidsreferentie, een disciplinaire maatregel, berisping of andere sanctie (evt. van financiële aard), dwang, intimidatie, pesterijen en uitsluiting, discriminatie, nadelige of ongelijke behandeling, niet-omzetting van een tijdelijke arbeidsovereenkomst in een van onbepaalde duur (indien de klokkenluider de gerechtvaardigde verwachting had dat dit hem zou worden aangeboden), niet-verlenging of vroegtijdige beëindiging van een tijdelijke arbeidsovereenkomst, het toebrengen van schade (incl. reputatieschade met een expliciete vermelding van sociale media) of financieel nadeel (omzetsdaling en inkomstendering), opname op een (in)formele “zwarte lijst” binnen een bepaalde sector of bedrijfstak, vroegtijdige beëindiging of opzegging van een contract (voor levering van goederen of diensten), intrekken van een licentie of vergunning of psychiatrische of medische verwijzingen. Dit maakt bijvoorbeeld het ontslag van een klokkenluider niet onmogelijk. Wel mag dit geen “*nauw verband*” hebben met de gedane melding. Werkgevers blijven gerechtigd hun werknemers te

²⁴. Het beheer van een klokkenluidersplatform uitbesteden is dus mogelijk en wordt door bepaalde auteurs ook als de meer wenselijke optie gezien (*cf.* K. DE BISSCHOP en E. CARLIER, “Klokkenluidersregelingen in een grensoverschrijdende context”, *Or.* 2009, afl. 2, 55; A. HOEKSTRA, J. TALSMAN en M. ZWEEGERS, *De vertrouwenspersoon integriteit – Stand van zaken en ontwikkelingsperspectieven*, Utrecht, Huis voor Klokkenluiders, 2018, 14 en G. HADDERS en K. HENRIKSSON, *The WhistleB Handbook*, Stockholm, Vulkan, 2020, 34).

²⁵. Wat duidt op een zekere subjectiviteit bij deze beoordeling. Niet zozeer de objectieve casus, maar het oprechte aanvoelen van de klokkenluider lijkt relevant.

evalueren en aan die evaluatie gevolgen te koppelen (§ 44 preambule).

Meer concreet voorziet de richtlijn de volgende maatregelen ter bescherming van de klokkenluider, maar ook de (rechts)persoon waarover wordt gemeld. De klokkenluider (art. 21, 2.-8.):

- wordt (onder voorbehoud van de algemene beperkingen van de richtlijn *cf. supra*) niet geacht onrechtmatig informatie te hebben onthuld en kan dus op geen enkele wijze aansprakelijk worden gesteld voor zijn melding of openbaarmaking voor zover hij redelijke gronden had om aan te nemen dat de melding of openbaarmaking noodzakelijk was voor het onthullen van de inbreuk²⁶;
- kan niet aansprakelijk worden gesteld voor de verwerving of toegang tot de gemelde of openbaar gemaakte informatie, tenzij die verwerving of toegang een strafbaar feit uitmaakt;
- die lopende een procedure ten gevolge een benadeling kan aantonen dat hij een melding deed, geniet het (weerlegbare) vermoeden dat die benadeling een

repesaillemaatregel uitmaakt (waarna het aan de benadelende (rechts)persoon is om die benadeling naar behoren te motiveren);

- moet toegang hebben tot passende maatregelen, waaronder een kort geding, om de gevolgen van represailles te herstellen in afwachting van definitieve gerechtelijke procedures;
- kan niet burgerrechtelijk aansprakelijk zijn als gevolg van een melding of openbaarmaking indien hij redelijke gronden had om aan te nemen dat de melding of openbaarmaking noodzakelijk was voor het onthullen van de inbreuk.

De persoon waarover wordt gemeld (art. 22) heeft recht op een eerlijk proces omvattende onder meer het vermoeden van onschuld, het recht te worden gehoord en het recht op toegang tot het dossier. Hun identiteit wordt zo lang en veel als mogelijk afgeschermd en geheim gehouden. Bovendien moeten er doeltreffende, evenredige en afschrikkende sancties worden voorzien voor klokkenluiders die bewust onjuiste informatie melden of openbaar maken (art. 23, 2.).

III. BIJZONDERE VRAAGSTUKKEN VAN STRAF(PROCES)RECHTELIJKE AARD

§ 1. Vrijwaring door de klokkenluider van diens eigen strafrechtelijke aansprakelijkheid

A. Algemeen

Als het gaat over de autonome straf(proces)rechtelijke bevoegdheid neemt de richtlijn bij momenten een duale houding aan. Zo luidt § 28 van de preambule bij de richtlijn:

“Hoewel deze richtlijn in bepaalde omstandigheden moet voorzien in een beperkte vrijstelling van aansprakelijkheid, ook strafrechtelijke aansprakelijkheid, in geval van een schending van de vertrouwelijkheidsplicht, mag zij geen afbreuk doen aan nationale strafprocedureregels, en met name niet aan de regels die de integriteit van het onderzoek en de procedure of de rechten van de verdediging van de betrokkenen moeten waarborgen. (...)”

Hieruit valt op het eerste gezicht af te leiden dat de richtlijn een impact heeft op het materieel strafrecht (omdat een vrijstelling van strafrechtelijke aansprakelijkheid moet worden voorzien), maar niet zozeer op het formeel nationaal strafrecht (zijnde het strafprocesrecht – “*mag zij geen afbreuk doen aan nationale strafprocedureregels*”). Dit laatste zou (in tegenstelling tot het eerste) een bevoegdheid zijn en blijven van de lidstaten. Tegelijk (en dus in die zin bevestigend)

bepaalt § 91 van de preambule van de richtlijn dat wettelijke of contractuele verplichtingen van personen, zoals loyauiteitsclausules of *non disclosure agreements*, niet mogen ingeroepen worden om meldingen te verbieden, bescherming te ontfangen aan klokkenluiders of represaillemaatregelen te nemen. Het is dan wel belangrijk dat de melding (of desgevallend publieke bekendmaking) nodig is voor het onthullen van de inbreuk.²⁷ In één adem vermeldt de richtlijn vervolgens dat – indien aan deze voorwaarden is voldaan – geen enkele burgerrechtelijke, strafrechtelijke, bestuursrechtelijke of arbeidsrechtelijke aansprakelijkheid mag rusten op de klokkenluider.

De navolgende § 92 bepaalt dan weer dat klokkenluiders (indien zij op rechtmatige wijze toegang verwerven of verkrijgen tot de informatie die ze navolgend melden) moeten vrijgesteld worden van aansprakelijkheid. Het gaat hierbij voor klokkenluiders om rechtmatige toegang en om de “*gevallen waarin zij kopieën van die documenten maken of deze verwijderen uit de bedrijfsruimten van de organisatie waar zij werkzaam zijn, zulks in strijd met contractuele clausules of andere clausules die bepalen dat de betreffende documenten eigendom van de organisatie zijn*”. De richtlijn haalt hier expliciet het voorbeeld aan van klokkenluiders die informatie hebben verworven door het raadplegen van e-mailverkeer van collega's of dossiers waar zijn normaal

²⁶ Het melden van overbodige informatie geeft bovendien geen aanleiding tot bescherming tenzij de klokkenluider hier redelijke gronden voor had (§ 91 preambule).

²⁷ Het gaat er (nog steeds *cf.* § 91) dan om dat de klokkenluider redelijke gronden had om aan te nemen dat melding of openbaarmaking nodig was voor het onthullen van een inbreuk op grond van deze richtlijn. De klokkenluider mag dus geen overbodige informatie kenbaar maken.

gesproken geen gebruik van maken, door het nemen van foto's van de bedrijfsruimten of door het betreden van plaatsen waartoe zij doorgaans geen toegang hebben. Halverwege § 92 lijkt de richtlijn zich evenwel te bedenken wanneer ze bepaalt dat:

“Indien de melders toegang tot de relevante informatie of documenten hebben verworven of verkregen door het plegen van een strafbaar feit, zoals het fysiek betreden van verboden terreinen of hacking, moet hun strafrechtelijke aansprakelijkheid blijven vallen onder het toepasselijk nationaal recht, onverminderd de overeenkomstig artikel 21, lid 7, van onderhavige richtlijn verleende bescherming. (...)”

De richtlijn bevestigt dit laatste ook in artikel 21.²⁸ Naast het strafprocesrecht, blijft dus ook het strafrecht het exclusieve domein van de respectievelijke lidstaat.

Meteen rijst dan ook de vraag wat naar Belgisch recht kwalificeert als een strafrechtelijke klokkenluidersinbreuk, welke gronden van verweer er zijn voor die klokkenluider en wat de impact is voor het navolgend onderzoek van een eventuele strafrechtelijke inbreuk begaan door een klokkenluider. Deze vragen worden hierna verder besproken.

B. Kwalificatie handelingen klokkenluiders

1. Algemeen

De voorbeelden die worden aangehaald in § 92 van de richtlijn wijzen op een klokkenluider die zich toegang verschaft tot informatie waartoe hij in feite of in rechte geen toegang had dan wel informatie die hij “meeneemt” uit een onderneming om deze te voegen aan een toekomstige melding. Voor dergelijke feiten zijn meerdere strafrechtelijke kwalificaties denkbaar. Deze kunnen enerzijds opgedeeld worden in feiten gepleegd in een fysieke dan wel digitale context en anderzijds naar gelang gepleegd tegen personen of eigendommen.

2. Offline-misdrijven gepleegd door klokkenluiders

a. Tegen personen

In een fysieke/offline context valt bij bovenstaande feitelijke omschrijving in de eerste plaats te denken aan misdrijven tegen personen zoals het briefgeheim (art. 460 Sw.) of huisvredebreuk (art. 439 Sw.). Dit eerste misdrijf lijkt gezien de digitalisering van onze maatschappij voorbestemd te zijn nog verder in onbruik te raken. Mocht een klokkenluider er zich in feite toch schuldig aan maken, hoeft dit evenwel niet tot een strafrechtelijke kwalificatie te leiden. Een particulier die kennisneemt van een niet (meer) aan de post toevertrouwde brief, is niet strafbaar.²⁹ Het tweede misdrijf (huisvredebreuk) heeft specifiek betrekking op de plaats waar iemand verblijft en daardoor recht heeft op de bescherming van zijn privéleven. Dit laatste is niet het geval voor bedrijfsruimtes³⁰ waardoor de relevantie beperkt blijft voor klokkenluiders. De zaken die zij melden zullen zij, in het merendeel van de gevallen, vernemen in een professionele en/of werk gerelateerde context.

Veel relevanter lijkt dan weer een inbreuk op het beroepsgeheim (art. 458 Sw.). Voor zover daar twijfel over bestaat, meldt de richtlijn (*cf. supra*) expliciet dat zij geen beperking inhoudt op het medisch beroepsgeheim of dat van advocaten. Een klokkenluider die beroepsmatig of als gevolg van zijn staat noodzakelijkerwijze³¹ de vertrouwenspersoon is van de persoon/de onderneming waarover hij wil melden³², riskeert hiervoor vervolgd te worden. Elkeen moet zich tot de houder van een beroepsgeheim kunnen wenden in het volste vertrouwen en dus zonder de vrees dat hierover de klok zal worden geluid. Men moet zonder op enige wijze afgeschrikt te worden een beroep kunnen doen op de (kwaliteitsvolle) medische of juridische hulp waar men recht op heeft.³³ Er is geen bedrieglijk opzet vereist. Een algemeen opzet volstaat³⁴, hetgeen klokkenluiders gehouden tot een beroepsgeheim dus verhindert te melden (ook al menen zij een alge-

²⁸ “3. Melders kunnen niet aansprakelijk worden gesteld voor de verwerving van of de toegang tot de informatie die wordt gemeld of openbaar wordt gemaakt, tenzij die verwerving of die toegang op zichzelf een strafbaar feit vormde. In het geval de verwerving of de toegang een op zichzelf staand strafbaar feit uitmaakt, blijft voor de strafrechtelijke aansprakelijkheid het toepasselijk nationaal recht gelden.”

²⁹ Cf. Antwerpen 25 januari 2001, *Limb.Rechtsl.* 2001, 156 en P. DE HERT, “Bedrijf mag post werknemers niet zomaar openmaken”, *Juristenkrant* 2001, afl. 21, 1. Een brief die door de postdiensten is bezorgd bij de bestemming, is niet meer aan de postdiensten toevertrouwd. Dit lijkt de regel te zijn voor klokkenluiders. Zij zullen geen melding doen op basis van informatie uit briefwisseling die nog niet is bezorgd bij de bestemming.

³⁰ Cf. F. VAN VOLSEM, “De strafrechtelijke bescherming van de onschendbaarheid van de woning: voor echte woningen, niet voor bedrijfsgebouwen” (noot onder Gent 5 januari 2011), *RABG* 2012, afl. 8, 525-533.

³¹ P. LAMBERT, *Le secret professionnel*, Brussel, Bruylant, 2005, 149-150; H. Nys, *Geneeskunde – Recht en Medisch Handelen*, Mechelen, Kuwer, 2016, 482 en A. DE NAUW en F. DERUYCK, *Inleiding tot het bijzonder strafrecht*, Mechelen, Kluwer, 2019, 401.

³² Of werkzaam is voor een persoon/een onderneming die kwalificeert als een dergelijke vertrouwenspersoon. Voor hen geldt immers het afgeleid beroepsgeheim (R. VERSTRAETEN, “De granaataanslag, het beroepsgeheim en Antigoon”, *NC* 2021, afl. 1, 63).

³³ F. VERBRUGGEN en S. ROYER, “Komt een terrorist, met zijn advocaat bij de dokter ... Mogen of moeten beroepsgeheimhouders spreken”, *NC* 2017, afl. 1, 25-26 en R. VERSTRAETEN, “De granaataanslag, het beroepsgeheim en Antigoon”, *NC* 2021, afl. 1, 62.

³⁴ Zo veroordeelde het Bergense hof van beroep een politieagent die een lijst met politie-interventies online (op Facebook) zette (Bergen 13 maart 2018, *JLMB* 2018, afl. 41, 1950-1951). Het hof erkende expliciet dat de politieagent geen kwaadaardige intenties had (“*Le prévenu, qui a posté volontairement la photo de la liste des interventions policières, même sans intention malveillante, ce qui semble être le cas en l'espèce, est donc coupable des faits à lui reprochés.*”). Niettemin besloot het hem te veroordelen voor een inbreuk op art. 458 Sw. Een gelijkaardig geluid klom bij de correctionele rechtbank van Luik (Corr. Luik 28 april 2011, *JLMB* 2012, afl. 32, 1538-1539). De drijfveer van de persoon die zijn beroepsgeheim schendt, is niet relevant.

meen belang te vrijwaren) tenzij wanneer zij als houders van het beroepsgeheim in rechte (of in een parlementaire onderzoekscommissie) moeten getuigen dan wel wettelijk verplicht zijn zaken bekend te maken.³⁵ Het beroepsgeheim is ten slotte te onderscheiden van de loutere discretieplicht. Deze laatste is een professionele verplichting om van cliënten vernomen geheimen die geen belangrijk en als dusdanig maatschappelijk erkende aangelegenheden betreffen, in principe niet bekend te maken.³⁶ Hierover zou dus wel de klok geluid kunnen worden (voor zover dit geen andere strafrechtelijke inbreuk uitmaakt).

In de context van het beroepsgeheim rijst nog een klokkenluidersvraag vanuit een ander perspectief. Hoe dient een klachtenbehandelaar (die als interne of externe medewerker van een onderneming het klokkenluidersplatform beheert en bij wie de meldingen in een eerste fase binnenkomen) zich te positioneren? Zijn hun adviezen naar aanleiding van ontvangen meldingen eveneens gedekt en is hun spreekrecht beperkt door het beroepsgeheim of niet? Op heden is er weliswaar eensgezindheid dat (naast advocaten) ook andere financieel-juridische adviseurs zoals bedrijfsjuristen³⁷, accountants³⁸ en revisoren³⁹ gehouden zijn tot het beroepsgeheim overeenkomstig artikel 458 Sw. Maar talrijk zijn eveneens de discussies omtrent de exacte draagwijdte van deze beroepsgeheimen en de consequenties ervan voor andere regelgeving.⁴⁰ Deze discussies blijven niet beperkt tot meldingen in de financieel-juridische sfeer. Zij spelen (cf. *infra*) ook bij interpersoonlijke meldingen rond bijvoorbeeld grensoverschrijdend gedrag.

Dit is niet onbelangrijk omdat (overeenkomstig de richtlijn) het beheer van een klokkenluidersplatform intern kan opge-

volgd worden door bijvoorbeeld een jurist of directeur audit (§ 56 preambule), maar ook kan uitbesteed worden (art. 8, 6.). Is de communicatie die in het bijzonder deze interne of externe medewerkers aldus bereikt en de adviezen die ze hierover geven ten aanzien van klokkenluider of de onderneming waarbinnen de klok wordt geluid bijgevolg gedekt door het beroepsgeheim?

Terugkoppeland naar bovenvermelde beroepsgeheimen in combinatie met de wetgeving rond het voorkomen van witwassen van geld, lijkt het antwoord op die vraag positief althans voor externe klachtenbehandelaars dewelke ook accountant of revisor zijn. Wanneer zij kennis nemen van gemelde informatie bepalen zij onvermijdelijk de rechtspositie van hun cliënt (de onderneming die het beheer van het klokkenluidersplatform uitbesteedde).⁴¹ Vanuit die optiek kunnen zij als klachtenbehandelaar moeilijk gehouden zijn tot het openbaren van hetgeen ze via deze weg vernemen.

Ook buiten de specifieke context van het voorkomen van witwassen van geld lijkt het beroepsgeheim van accountants- of revisoren-klachtenbehandelaars van toepassing op de informatie die ze aldus vernemen. Huybrechts omschreef het beroepsgeheim van deze cijferberoepen die als externe diensten verlenen immers als een waarborg voor de vertrouwelijkheid van de zakengeheimen tot dewelke deze cijferberoepers toegang hebben omdat een onderneming een beroep op hen moet doen. Deze zakengeheimen omschreef hij dan weer als “*elke vertrouwelijke waardevolle informatie van commerciële, financiële of administratieve aard van of betreffende de onderneming (...) die ze niet openbaar wil maken noch maakt en waarvan de bekendmaking haar ernstig schade zou kunnen toebrengen*”.⁴² Een dergelijke

³⁵ Cf. o.a. L. HUYBRECHTS, “Het beroepsgeheim van de cijferberoepen”, *NC* 2015, afl. 3, 171-172. Een formele wet is wel noodzakelijk zoals bv. art. 29 Sw. (de aangifteplicht voor ambtenaren) en fiscaal-financieel geïnspireerde meldingsplichten in het kader van het voorkomen van het witwassen van geld en de DAC6-richtlijn (cf. *infra* en A. DE NAUW en F. DERUYCK, *Inleiding tot het bijzonder strafrecht*, Mechelen, Kluwer, 2019, 401). Deze laatste maakt op heden nog het voorwerp uit van prejudiciële vraagstellingen bij het Grondwettelijk Hof en het Hof van Justitie. Daarbij geldt ook nog de regel dat “beroepsmisdrijf het beroepsgeheim uitsluit” (L. HUYBRECHTS, “Het beroepsgeheim van de cijferberoepen”, *NC* 2015, afl. 3, 180). Een houder van het beroepsgeheim die zelf formeel in verdenking wordt gesteld, is gerechtigd zijn beroepsgeheim te doorbreken. Zie hierover met terechte bedenkingen in dit verband: P. HENRY, “Secret professionnel: condamnation de la technique de l’ouvre-boîte” (noot onder Luik 18 januari 2021), *JLMB* 2021, afl. 19, 854-863.

³⁶ L. HUYBRECHTS, “Het beroepsgeheim van de cijferberoepen”, *NC* 2015, afl. 3, 168-169. Financiële instellingen zijn aan een dergelijke discretieplicht gebonden en niet aan het beroepsgeheim in de zin van art. 458 Sw.

³⁷ Cf. o.a. J. BOCKEN, “Adviezen bedrijfsjuristen beschermd tegen Belgische mededingingsautoriteit” *Juristenkrant* 2013, afl. 267, 1; F. KONING, “Embargo sur les avis des juristes d’entreprise et chinese wall vis-à-vis des réviseurs agréés et des compliance officers”, *T. Verz.* 2015, afl. 3, 283-288 en J. STEVENS, “Geen beroepsgeheim maar Legal Professional Privilege voor bedrijfsjuristen: the final curtain?”, *RW* 2016-17, 883-894. Een klokkenluidersplatform kan ook door interne juristen en/of compliance-medewerkers beheerd worden (§ 56 preambule).

³⁸ Cf. art. 120 wet van 17 maart 2019 betreffende de beroepen van accountant en belastingadviseur (BS 27 maart 2019). De omstandigheid dat een accountant gegevens verstrekt die hem niet werden bezorgd door zijn cliënt (zoals bij klokkenluiders het geval), volstaat niet om een toepassing van art. 458 Sw. uit te sluiten (Cass. 22 februari 2001, P.10.1386.N). Een redenering die men *a fortiori* kan toepassen op informatie afkomstig van een klokkenluider.

³⁹ Cf. art. 86 wet van 7 december 2016 tot organisatie van het beroep van en het publiek toezicht op de bedrijfsrevisoren.

⁴⁰ Zoals onder meer in de context van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten (BS 6 oktober 2017). Art. 53 van deze wet verbiedt (onder meer) accountants en revisoren om (net als advocaten) vermoedens van witwassen te melden indien zij hun cliënt bijstaan bij het bepalen van diens rechtspositie.

⁴¹ Het Grondwettelijk Hof omschreef dit begrip op 24 september 2020 (nr. 114/220) en koppelde hierbij terug naar een eerder arrest van 23 januari 2008: “Daarenboven heeft het Hof gepreciseerd dat het begrip ‘bepaling van de rechtspositie’ van de cliënt het begrip ‘juridische advisering’ omvat (B.9.4.). Het heeft geoordeeld dat de activiteit bestaande in het verstrekken van juridisch advies ertoe strekt ‘de cliënt te informeren over de staat van de wetgeving die van toepassing is op zijn persoonlijke situatie of de verrichting die hij overweegt, of hem te adviseren over de wijze waarop die verrichting binnen het wettelijk kader kan worden uitgevoerd’ en ‘altijd tot doel [heeft] het de cliënt mogelijk te maken een rechtsgeding met betrekking tot die verrichting te vermijden.’ (B.9.5.)”.

⁴² L. HUYBRECHTS, “Het beroepsgeheim van de cijferberoepen”, *NC* 2015, afl. 3, 168-169.

omschrijving lijkt aan de via een klokkenluidersplatform bekomen informatie te beantwoorden.

Een parlementaire bevestiging en/of verfijning in dit verband blijft evenwel zonder meer opportuun, al was het maar omdat accountants en revisoren niet de enige externe klachtenbehandelaars zijn.⁴³ In zoverre die er niet komt, kan de bestaande rechtspraak in de context van meldingen rond psychosociale problemen desgevallend als inspiratiebron dienen.⁴⁴ Bij dergelijke meldingen is het beroepsgeheim gevrijwaard gezien de persoon die zich tot de klachtenbehandelaar wendt ervan mag uitgaan dat die melding vertrouwelijk blijft.⁴⁵ Dit beroepsgeheim is volgens de Belgische rechtspraak wel niet absoluut. De betrokkene waarover wordt gemeld en tegen wie mogelijk een procedure wordt ingeleid, heeft onder bepaalde voorwaarden en indien nodig na anonimiseren of selectie door een rechter het recht om kennis te nemen van het aanvankelijke dossier.⁴⁶ Deze rechtspraak gaat wel uit van de min of meer rechtstreekse werkgever-werknemerrelatie. De richtlijn breidt de mogelijkheid te melden ook uit naar derden (zoals leveranciers) die in principe vreemd zijn aan de regelgeving rond deze psychosociale problematieken. In dit verband aanvaardde de Antwerpse KI alvast dat het beroepsgeheim van een preventieadviseur zich ook kan uitstrekken tot meldingen gedaan door externe personen zonder rechtstreekse link met de onderneming waarbinnen de preventieadviseur was aangesteld.⁴⁷ Of deze redenering zonder meer kan worden doorgetrokken naar meldingen in het kader van de richtlijn is vandaag (nog) geen uitgemaakte zaak. Een argument dat ervoor pleit dat dit wel het geval zou moeten zijn, is de focus van de richtlijn op vertrouwelijkheid (*cf. supra*).

Een laatste meldenswaardig misdrijf (in een fysieke/offline context) tegen personen is het misbruik van inzagerecht (art. 460ter Sw.). In een recent en opmerkelijk vonnis veroordeelde de Brugse correctionele rechtbank een VRT-journalist die een reportage bracht omtrent de zgn. “Kasteelmoord”. De journalist in kwestie werd veroordeeld als deelnemer aan het misbruik van inzagerecht door één van de beklaagden (art. 460ter Sw.).⁴⁸ Klokkenluiders (en de journalisten bij wie ze de klok luiden) die wantoestanden aankaarten aan de hand van een via het inzagerecht in het strafdossier bekomen informatie en zo een onderzoek verhinderen dan wel de integriteit van betrokken personen in het gedrang brengen, riskeren dus een veroordeling.⁴⁹

b. Tegen eigendommen

Naast de misdrijven tegen personen in een fysieke/offline context, is er eveneens een ruim arsenaal aan klokkenluidersmisdrijven in diezelfde context tegen eigendommen.

Een klokkenluider die informatie meeneemt uit het bedrijf zou zich schuldig kunnen maken aan (huis)diefstal (art. 464 Sw.) of misbruik van vertrouwen (art. 491 Sw.). Zo veroordeelde de correctionele rechtbank van Ieper een bankbediende die vertrouwelijke informatie over cliënteel “ontvreemde” (door ze te mailen naar zijn privé-e-mailadres en bepaalde informatie nadien te wissen) voor deze misdrijven alsook voor informaticabedrog (art. 504quater Sw.). De dubbele kwalificatie van het kopiëren en wissen van deze gegevens als (huis)diefstal én informaticabedrog bestempelde de rechtsleer wel als merkwaardig.⁵⁰ Dit duidt alleszins op de complexiteit van het klokkenluidersperspectief. Elke mededeling van informatie (waaraan per definitie een

⁴³ Cf. ook K. JANSSENS, “Witwaswet: is gewoon boekhouden ook ‘bepalen van rechtspositie cliënt’?”, *Fisc.Act.* 2010, afl. 7, 9-10. Zo wordt een dergelijke (fundamentele) afweging niet (of minstens minder) overgelaten aan de cijferberoepen zelf en hebben zij een meer concrete houvast.

⁴⁴ Op heden kan men hierover de klok luiden bij de preventieadviseurs en vertrouwenspersonen bedoeld in de welzijnswet (wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk (*BS* 18 september 2017)) en de Codex Welzijn op het werk (Codex van 28 april 2017 over het welzijn op het werk (*BS* 2 juni 2017)). De Richtlijn erkent dergelijke bestaande kaders en laat de mogelijkheid open om interpersoonlijke conflicten via deze bestaande procedures te blijven behandelen (preambule § 22). Hoewel een op die manier opgedeeld klokkenluidersplatform de voorkeur lijkt uit te dragen van de (toenmalige) Privacycommissie, lijkt ze m.i. toch niet de meest logische aanpak. Een goede klokkenluidersregeling is namelijk duidelijk en laagdrempelig. Klokkenluiders vervolgens zelf laten analyseren welke de exacte aard is van hun melding, werkt in die zin niet drempelverlagend. Zie uitgebreider: J. LAMBRECHTS, “Europese Richtlijn ter bescherming van klokkenluiders: analyse van een (r)evolutie”, *NJW* 2021, afl. 435, 57-58.

⁴⁵ Cf. o.a. § 60 van de preambule: “Doeltreffende opsporing en preventie van inbreuken op het Unierecht vereist dat potentiële klokkenluiders gemakkelijk en onder strikte vertrouwelijkheid de informatie waarover zij beschikken onder de aandacht kunnen brengen van de bevoegde autoriteiten die in staat zijn om het probleem te onderzoeken en aan te pakken, indien mogelijk.”

⁴⁶ GwH 23 januari 2019, nr. 2/2019. Cf. ook V. DOOMS, “Over het vertrouwelijk karakter van de informatie bij een vertrouwenspersoon en preventieadviseur bij feiten tot staving van een dringende reden” (noot onder Cass. 14 december 2015), *RABG* 2017, afl. 3, 197-212 en S. HEYNDRICKX, “Het beroepsgeheim van de preventieadviseur: absoluut of niet” (noot onder Gent 19 september 2019), *RABG* 2020, afl. 2, 167-176.

⁴⁷ KI Antwerpen 17 mei 2019, nr. K/1050/2015, *onuitg.*

⁴⁸ Hiertegen werd evenwel beroep aangetekend en ook meteen kritiek geuit (*cf.* D. VOORHOOF, “Veroordeling VRT-journalist voor misbruik inzagerecht is verontrustend”, *Juristenkrant* 2021, afl. 430, 12-13).

⁴⁹ Cf. ook Cass. 7 december 2004, P.04.1006.N. Art. 10 EVRM en het recht op vrije meningsuiting is geen absolute andersluidende garantie. Wel geldt sinds 2005 een specifieke wettelijke bescherming op het journalistieke bronnengeheim (wet van 7 april 2005 tot bescherming van journalistieke bronnen (*BS* 27 april 2005)). Deze wet houdt onderzoekers niet noodzakelijk tegen over te gaan tot inbeslagname van gegevens bij journalisten die met behulp van klokkenluiders zaken aankaarten. Zie in het algemeen over het journalistieke bronnengeheim, de Europese rechtspraak hieromtrent en de recente casus waarbij onderzoekers niet noodzakelijk geremd lijken door deze bijzondere wetgeving: S. LAMBERIGTS en S. ROYER, “Over een bezoek aan een drugdealer en het journalistiek bronnengeheim” (noot onder EHRM 6 oktober 2020), *T.Strafr.* 2021, afl. 2 en J. LAMBRECHTS, “Commotie over te snelle spuit ook aanzet voor spoedige omzetting Europese klokkenluidersrichtlijn?”, *Juristenkrant* 2021, afl. 430, 16.

⁵⁰ S. ROYER, “Na bijna 20 jaar nog onduidelijkheid over kwalificatie diefstal, misbruik van vertrouwen en informaticabedrog” (noot onder Corr. Ieper 27 juli 2018), *NJW* 2018, afl. 389, 753-754. Cf. ook Cass. 5 januari 2011, P.10.1094.F en Cass. 23 november 2011, P.11.1092.F: software, studies, rapporten, klantenlijsten, ... in een IT-systeem kunnen voorwerp zijn van een misbruik van vertrouwen.

meenemen/ontvreemding voorafgaat) riskeert – zelfs in een louter fysieke/offline context – onder meerdere en tegelijk bediscussieerbare kwalificaties te vallen. Men kan, vertrekkende van het legaliteitsbeginsel, moeilijk verwachten dat de gemiddelde klokkenluider de strafrechtelijke draagwijdte van diens handelen correct kan inschatten indien er onduidelijkheid blijft bestaan⁵¹ over enkele van de voor hen meest significante strafrechtelijke kwalificaties. Ook in dat opzicht lijkt een parlementaire reflectie niet overbodig in afwachting van de (hopelijk fundamentele) herdenking van ons Strafwetboek.⁵²

c. Online-misdrijven gepleegd door klokkenluiders

Hoewel het misdrijvenarsenaal in een fysieke/offline context ruim is, is het niet waarschijnlijk dat de door klokkenluiders gepleegde feiten frequent aanleiding riskeren te geven of zullen geven tot vervolging op die basis. In een samenleving die meer en meer digitaliseert, met sinds de recente COVID 19-crisis een digitale tussenversnelling, is de kans klein dat in de toekomst via fysiek gelekte documentatie de klok wordt geluid.⁵³ Meer nog dan offline-misdrijven (met uitzondering van het beroepsgeheim) zullen hun online-varianten het debat bepalen.

Het online-misdrijf waarvoor de klokkenluider zich het meeste moet hoeden is hacking. Artikel 550bis Sw. bestraft in al haar specifieke vormen de integriteitsschending van een informaticasysteem. Buitenstaanders verschaffen zich (per definitie onbevoegd) toegang tot een informaticasysteem (externe hacking cf. art. 550bis, § 1 Sw.) of bevoegde personen (insiders) overschrijden die bevoegdheid binnen, opnieuw, een informaticasysteem (interne hacking cf. art. 550bis, § 2, Sw.). De persoon die vervolgens de gehackte gegevens onder zich houdt, onthult, verspreidt of er enig gebruik van maakt is evenzeer strafbaar (art. 550bis, § 7 Sw.).⁵⁴ Indien dit informaticasysteem op zichzelf elektroni-

sche communicatie is, dan speelt artikel 124, 1° WEC.⁵⁵ Dit artikel stelt eenieder strafbaar die zonder toestemming met opzet kennis neemt van het bestaan van informatie van alle aard die via elektronische weg werd verstuurd en die niet persoonlijk voor hem/haar bestemd is.⁵⁶

Bij beide misdrijven (hacking en art. 124 WEC) speelt de mate waarin contractuele afspraken werden gemaakt een belangrijke rol om de exacte draagwijdte van de misdrijven te bepalen.⁵⁷ Ondernemingen die een klokkenluidersregeling implementeren, doen er dan ook goed aan hun algemene computer-, e-mail- en internetpolities nog eens van nabij te bekijken. Dit om duidelijk de manoeuvreerruimte van eventuele klokkenluiders te bepalen en meteen ook voor hun eigen *investigative readiness*.⁵⁸ Een melding door een klokkenluider geeft immers niet zelden aanleiding tot een interne (fraude) audit. Indien private fraude onderzoekers tijdens zo'n interne audit niet terug kunnen vallen op duidelijke afspraken bestaat de kans dat zij zich geen toegang kunnen verschaffen tot cruciale informatie zoals e-mailverkeer.⁵⁹

C. Gronden van verweer voor de klokkenluider

1. De mensenrechtelijke principes

In 2008 zette het Europees Hof voor de Rechten van de Mens (EHRM) de bakens uiteen voor de bescherming van klokkenluiders die een inbreuk plegen. Sindsdien kunnen zij zich (trachten te) beroepen op hun recht op vrije meningsuiting (art. 10 EVRM). Het EHRM lijstte toen⁶⁰ een zesvoudige toets op die een (publieke) melding moet doorstaan om binnen het toepassingsgebied van artikel 10 EVRM te vallen. Het vertrok hierbij eerst van de algemene overwegingen dat een beperking van de vrije meningsuiting een wettelijke grondslag dient te hebben en een legitieme doelstelling. Daarnaast moet ze ook noodzakelijk zijn in een democrati-

⁵¹ In die zin dat er ook binnen rechtspraak en rechtsleer geen eensgezindheid bestaat onder welke strafrechtelijke kwalificaties dit soort handelen valt.

⁵² Zie in dit verband: *Parl.St.* Kamer 2018-19, nr. 3651/001.

⁵³ Cf. ook E. COBBAUT, "L'encadrement de l'alerte et la protection du lanceur d'alerte (whistleblower): l'affaire Luxleaks à l'aune d'un cadre européen en construction", *RDTI* 2019, afl. 75, 54.

⁵⁴ Cf. ook O. LEROUX, "Criminalité informatique" in H.D. BOSLY en C. DE VALKENNEER (eds.), *Les infractions contre les biens*, Brussel, Larcier, 2016, 476-490 en K. DE SCHEPPER, "Materieel ICT-strafrecht" in P. WAETERINCKX, F. DERUYCK en F. VAN VOLSEM (eds.), *Strafrecht in de onderneming*, Antwerpen, Intersentia, 2016, 430-450.

⁵⁵ Wet van 13 juni 2005 betreffende de elektronische communicatie (BS 20 juni 2005).

⁵⁶ Daar waar § 92 van de preambule er net voor pleit klokkenluiders te vrijwaren van aansprakelijkheid in dit geval: "De melders moeten ook worden vrijgesteld van aansprakelijkheid in gevallen waarin de verwerving van of de toegang tot de relevante informatie of documenten burgerrechtelijke, bestuursrechtelijke of arbeidsrechtelijke aansprakelijkheid in het geding brengt. Voorbeelden zijn gevallen waarin de melders de informatie hebben verworven door het raadplegen van het e-mailverkeer van een collega of dossiers waar zij normaal gesproken geen gebruik van maken bij hun werk (...)"

⁵⁷ In het kader van (interne) hacking: Cass. 24 januari 2017, P.16.0048.N. In het kader van art. 124 WEC: Cass. 20 mei 2019, S.17.0089.F en Brussel 8 februari 2019, www.juridat.be.

⁵⁸ Hiermee wordt de algemene paraatheid bedoeld van een organisatie om een fraude-incident of -vermoeden te onderzoeken. Het draait om het uitstippen van een algemeen beleid rond onderzoeken en onderzoeksbevoegdheden waardoor de uitkomst ervan wordt gemaximaliseerd en de kost zoveel als mogelijk beperkt. Cf. ook R. ROWLINGSON, "A ten step process for forensic readiness", *International Journal of digital evidence* 2004, afl. 2, 1.

⁵⁹ Opnieuw cf. Cass. 20 mei 2019, S.17.0086.F: een werkgever die zich onrechtmatig toegang verschafft tot een mailbox, kan zich ook zelf schuldig maken aan een inbreuk op art. 124 WEC. Overeenkomstig art. 17 van de richtlijn moet elke verwerking van persoonsgegevens in het kader van de richtlijn worden verricht overeenkomstig de GDPR.

⁶⁰ EHRM 12 februari 2008, *Guja / Moldavië*. Deze principes werden bevestigd in navolgende arresten zoals onder meer EHRM 21 juli 2011, *Heinisch / Duitsland* en EHRM 8 januari 2013, *Bucur en Toma / Roemenië*.

sche samenleving. Hiervoor geldt de volgende zesvoudige toets⁶¹:

- dat de klokkenluider niet terecht kon bij zijn leidinggevende(n) of een andere instantie⁶²;
- dat de melding betrekking heeft op zaken van algemeen belang⁶³;
- dat de gemelde informatie authentiek, betrouwbaar en accuraat is, hetgeen niet zozeer een resultaatsverbintenis tot verificatie impliceert in hoofde van de klokkenluider, maar eerder een redelijke inspanningsverbintenis (de melding moet dus niet per definitie aanleiding geven tot vervolging)⁶⁴;
- dat de schade zoals veroorzaakt door de klokkenluider in verhouding staat tot het belang van zijn melding⁶⁵;
- dat de klokkenluider niet handelt vanuit een (zuiver) individueel, maar vanuit een algemeen belang en dus te goeder trouw is⁶⁶;
- de impact die een sanctie voor de klokkenluider heeft en wat daarvan de gevolgen waren.⁶⁷

Een zeer recent Luxemburgs en een navolgend Straatsburgs arrest⁶⁸ vertalen deze criteria specifiek in het kader van de directe aanleiding van de richtlijn, één van de *LuxLeaks*-klokkenluiders. Die was werkzaam bij een Big 4-consultancykantoor en begeleidde er (samen met zijn teamleden) fiscale rulings. Nadat vele hiervan lekten in de media, bleek uit intern onderzoek bij het consultancykantoor dat de klokkenluider i.c. (weliswaar niet als enige) informatie had bezorgd aan de media. Hij luidde de klok als reactie op de eerste bekendmakingen ten gevolge van door andere klokkenluiders gedane meldingen. Het consultancykantoor legde hierop klacht neer tegen de klokkenluider. Dit leidde finaal (overeenkomstig Luxemburgs recht) tot een veroordeling

voor feiten die (naar Belgisch recht) onder meer gekwalificeerd zouden kunnen worden als (huis)diefstal, hacking en schending van het beroepsgeheim.

De klokkenluider bepleitte hierop zijn zaak voor het EHRM. Dat oordeelde aan de hand van de zes voormelde criteria en verwees ook naar het oordeel van het Luxemburgse hof van beroep. Deels omdat over vier criteria geen discussie bestond. Het EHRM erkende (net als de betrokken partijen en het Luxemburgse hof van beroep) dat de klokkenluider geen alternatief zag voor zijn publieke bekendmaking, zaken van algemeen belang aankaarte, zijn informatie authentiek was en hij te goeder trouw handelde.⁶⁹ De discussie die het EHRM diende te beslechten had betrekking op de laatste twee criteria, zijnde enerzijds de evenredigheid tussen het beschermde algemeen belang en de schade voor de betrokkene waarover werd gemeld en anderzijds de sanctie die de klokkenluider werd opgelegd.

Bij dit laatste herinnerde het EHRM eerst aan zijn relatieve rol wat strafrechtelijke beoordelingen betreft.⁷⁰ Vervolgens oordeelde het EHRM dat – niettegenstaande het feit dat er aan het consultancykantoor slechts 1 EUR symbolische schadevergoeding was toegekend⁷¹ – ook rekening moet gehouden worden met de meerwaarde van de gemelde informatie voor het publieke debat. Dit impliceert m.a.w. dat een klokkenluider zich er niet alleen voor moet hoeden onnodige informatie te onthullen⁷², maar er tegelijk op moet letten effectief met nieuwe elementen naar buiten te komen.⁷³ In dit specifieke dossier droegen de onthullingen van de klokkenluider weinig nieuws bij. Wel schaadden ze het consultancykantoor. Daarom woog de bekendmaking niet op tegen de geleden schade.⁷⁴ Omdat ook de opgelegde sanctie rela-

61. Zoals ook besproken in o.a. D. VOORHOOF, “Europees Hof neemt klokkenluider in bescherming”, *Juristenkrant* 2008, afl. 167, 1-3 en V. JUNOD, “La liberté d’expression du whistleblower” (noot onder EHRM 12 februari 2008), *Rev.trim.DH* 2009, afl. 77, 227-260.

62. EHRM 12 februari 2008, *Guja / Moldavië*, § 73; EHRM 21 juli 2011, *Heinisch / Duitsland*, § 72-76 en EHRM 8 januari 2013, *Bucur en Toma / Roemenië*, § 95-100.

63. EHRM 12 februari 2008, *Guja / Moldavië*, § 74; EHRM 21 juli 2011, *Heinisch / Duitsland*, § 71 en EHRM 8 januari 2013, *Bucur en Toma / Roemenië*, § 101-104.

64. EHRM 12 februari 2008, *Guja / Moldavië*, § 75; EHRM 21 juli 2011, *Heinisch / Duitsland*, § 77-81 en EHRM 8 januari 2013, *Bucur en Toma / Roemenië*, § 105-113.

65. EHRM 12 februari 2008, *Guja / Moldavië*, § 76; EHRM 21 juli 2011, *Heinisch / Duitsland*, § 88-90 en EHRM 8 januari 2013, *Bucur en Toma / Roemenië*, § 114-115.

66. EHRM 12 februari 2008, *Guja / Moldavië*, § 77; EHRM 21 juli 2011, *Heinisch / Duitsland*, § 82-87 en EHRM 8 januari 2013, *Bucur en Toma / Roemenië*, § 116-118. Voor een meer uitgebreide analyse van wat een algemeen belang kan inhouden met verwijzing naar diverse Europese rechtspraak: E. COBBAUT, “L’encadrement de l’alerte et la protection du lanceur d’alerte (whistleblower): l’affaire *LuxLeaks* à l’aune d’un cadre européen en construction”, *RDTT* 2019, afl. 75, 61-62.

67. EHRM 12 februari 2008, *Guja / Moldavië*, § 78; EHRM 21 juli 2011, *Heinisch / Duitsland*, § 91-92 en EHRM 8 januari 2013, *Bucur en Toma / Roemenië*, § 119.

68. EHRM 11 mei 2021, *Halet / Luxemburg*.

69. EHRM 11 mei 2021, *Halet / Luxemburg*, § 21-24.

70. EHRM 11 mei 2021, *Halet / Luxemburg*, § 91: “La Cour estime qu’il ne lui appartient pas de donner son avis sur la question de savoir si l’élément légal de l’infraction reprochée au requérant était à neutraliser ou non, pareil examen relevant du seul droit national.”

71. Het EHRM bevestigde expliciet dat het symbolische karakter hiervan er niet aan in de weg staat de schade van het consultancykantoor toch als ernstig moet worden beschouwd (EHRM 11 mei 2021, *Halet / Luxemburg*, § 99).

72. Cf. § 91 van de preambule: de klokkenluider mag geen overbodige informatie kenbaar maken.

73. De richtlijn bevat trouwens een gelijkaardige beperking in § 43 van de preambule: “(...) Bescherming is echter niet nodig voor personen die informatie melden die reeds ten volle tot het publieke domein behoort of van onbewezen geruchten en verhalen.” Zie hierover uitgebreider: A. LACHAPPELLE, “L’encadrement juridique du lancement d’alerte au sein de l’Union européenne”, *RDTT* 2020, afl. 78-79, 29-30.

74. EHRM 11 mei 2021, *Halet / Luxemburg*, § 104-110.

tief beperkt was⁷⁵, besloot het EHRM (opnieuw verwijzend naar de appreciatiemarge waarover lidstaten beschikken) dat er geen schending voorlag van artikel 10 EVRM.⁷⁶

De toekomstige klokkenluider die zich wenst te beroepen op artikel 10 EVRM, doet er bijgevolg goed aan te evalueren in welke mate de door hem/haar te openbaren informatie nieuw is en iets fundamenteel extra bijdraagt aan het – misschien reeds bestaande – maatschappelijk debat.⁷⁷ Tegelijk heeft de aandachtige lezer de koppeling gemaakt tussen de richtlijn zelf en het eerste criterium van het EHRM. Het antwoord op de vraag of een klokkenluider terecht kan bij zijn hiërarchisch overste of een andere instantie heeft consequenties voor het verbod/de mogelijkheid de klok te luiden en dus de noodzakelijkheid van de inperking van het recht op vrije meningsuiting. Anders geformuleerd, een onderneming die zich kwijt van haar toekomstige verplichtingen onder de richtlijn en een effectieve klokkenluidersregeling implementeert, ontnemt (minstens deels) een eventuele klokkenluider het recht (op basis van art. 10 EVRM) om meteen voor een externe melding of publieke bekendmaking te opteren.⁷⁸

Hierin schuilt opnieuw⁷⁹ de paradox van het implementatieproces van een klokkenluidersregeling. Sociaal gezien kan een goed geïmplementeerde klokkenluidersregeling op lange termijn een organisatie creëren met een dermate hoge graad van integriteit waarbij medewerkers worden gevormd tot zelfdenkende en kritische individuen. Hierdoor spreken zij collega's of managers rechtstreeks aan op afwijkend gedrag (in plaats van zich te wenden tot het meer formele

klokkenluidersplatform).⁸⁰ Dus net zoals sociaal draagvlak voor een klokkenluidersregeling het gebruik ervan *de facto* doet afnemen, ontnemt de correcte implementatie ervan de juridische steun om voluit voor het alternatief (het recht op vrije meningsuiting) te kunnen (of beter gezegd: moeten⁸¹) gaan.

2. De noodtoestand

De noodtoestand is een jurisprudentieel ontwikkelde strafrechtelijke rechtvaardigingsgrond.⁸² Zij neutraliseert een bepaalde gedraging in het algemeen en maakt haar zo (strafrechtelijk) aanvaardbaar. De aanwezigheid van de noodtoestand betekent dat iemand om het ene (hoger ingeschatte) rechtsgoed te vrijwaren het andere (per definitie lager ingeschatte) rechtsgoed schendt. Sinds het zgn. “*onthulde-boevenschuilplaats*”-arrest van het Hof van Cassatie is het mogelijk dat een arts zijn beroepsgeheim schendt wanneer hij (*cf.* de benaming van het arrest) de schuilplaats van personen onthult die mogelijk nieuwe en (zeer) ernstige feiten kunnen plegen.⁸³ Deze strafrechtelijke inbreuk op het beroepsgeheim geldt dan als een soort *ultimum remedium* ten aanzien van het ernstigere alternatief (de nieuwe feiten).

Hoewel de noodtoestand in eerste instantie werd toegepast op het medische beroepsgeheim en niet op dat van advocaten, wordt inmiddels aanvaard dat de noodtoestand ook als dusdanig op advocaten kan toegepast worden.⁸⁴ Niet onlogisch heeft de praktische toepassing van dit principe tot op heden voornamelijk betrekking gehad op het terzijde schui-

⁷⁵. EHRM 11 mei 2021, *Halet / Luxemburg*, § 111.

⁷⁶. EHRM 11 mei 2021, *Halet / Luxemburg*, § 112.

⁷⁷. Hetgeen allerminst een evidentie is (*cf.* ook E. COBBAUT, “L’encadrement de l’alerte et la protection du lanceur d’alerte (whistleblower): l’affaire *Lux-leaks* à l’aune d’un cadre européen en construction”, *RDTI* 2019, afl. 75, 64).

⁷⁸. *Cf.* ook A. LACHAPPELLE, “L’encadrement juridique du lancement d’alerte au sein de l’Union européenne”, *RDTI* 2020, afl. 78-79, 41. Dit betekent niet noodzakelijk dat de afwezigheid van een formele klokkenluidersregeling ertoe leidt dat de klok zomaar mag geluid worden. Ook dan is het mogelijk dat men (zonder formele regeling) bij zijn leidinggevende terecht kan (A. LACHAPPELLE, *La dénonciation à l’ère des lanceurs d’alerte fiscale*, Brussel, Larcier, 2021, 1027).

⁷⁹. Zie hierover uitgebreider: J. LAMBRECHTS, “Europese Richtlijn ter bescherming van klokkenluiders: analyse van een (r)evolutie”, *NJW* 2021, afl. 435, 61.

⁸⁰. *Cf.* ook K. LOYENS, “Interne meldprocedures: een kwestie van maatwerk?”, *Orde dag* 2015, afl. 72, 41 en L. GROENEWALD, *Whistleblowing Management Handbook*, Pretoria, The Ethics Institute, 2020, 7.

⁸¹. Uit onderzoek blijkt immers dat klokkenluiders niet spontaan voor de meer ingrijpende optie kiezen (melding via het externe kanaal of een publieke bekendmaking). Klokkenluiders verkiezen een interne melding en gaan pas voor de externe piste als die niet het gewenste of verwachte resultaat oplevert (*cf.* G. VYNCKIER en B. DE BIE, “Een held vertelt. De meldingsbeleving: voor, tijdens en na”, *Orde dag* 2015, afl. 72, 20; W. VANDEKERCKHOVE, “Antwoorden is belangrijker dan melden”, *Orde dag* 2015, afl. 72, 26 en A.J. BROWN *et al.*, *Clean as a whistle: a five step guide to better whistleblowing policy and practice in business and government*, Brisbane, Griffith University, 2019, 21).

⁸². *Cf.* o.a. D. VAN GERVEN, “De noodtoestand als uitzondering op het beroepsgeheim van de advocaat, en de ongrondwettigheid van de uitbreiding die hieraan wordt gegeven door artikel 458bis Sw.” (noot onder GwH 26 september 2013), *RW* 2013-14, afl. 32, 1257; L. HUYBRECHTS, “Het beroepsgeheim van de cijferberoepen”, *NC* 2015, afl. 3, 172-173; F. VERBRUGGEN en S. ROYER, “Komt een terrorist, met zijn advocaat bij de dokter ... Mogen of moeten beroepsgeheimhouders spreken”, *NC* 2017, afl. 1, 32 en R. VERSTRAETEN, “De granaataanslag, het beroepsgeheim en Antigoon”, *NC* 2021, afl. 1, 66.

⁸³. Cass. 13 mei 1987, *RCJB* 1986-87, 588-630, noot A. DE NAUW. Er moet sprake zijn van een dreigend en ernstig gevaar, de inbreuk is noodzakelijk en de proportionaliteit blijft gevrijwaard tussen het beschermde belang en het belang dat door de geschonden bepaling wordt beschermd.

⁸⁴. *Cf.* o.a. GwH 3 mei 2000, nr. 46/2000. De aanvaarding van de noodtoestand is genuanceerd. Hoewel zij principieel kan ingeroepen worden, kan ze allerminst als een automatisme worden beschouwd en/of toegepast. De noodtoestand vereist dat een advocaat het bestaan aantoonde van een daadwerkelijk en ernstig gevaar dat onmogelijk op een andere wijze kon worden vermeden dan door het meedelen, desnoods in laatste instantie, van een door zijn cliënt gepleegd misdrijf (GwH 26 september 2013, nr. 127/2013).

ven van een beroepsgeheim van advocaten teneinde de fysieke integriteit van derden te vrijwaren.⁸⁵

In recente rechtsleer⁸⁶ wordt het idee geopperd de noodtoestand ook te aanvaarden voor klokkenluiders. Indien zij van mening zijn dat de vraag naar transparantie de noodzaak tot beroepsmatige geheimhouding overstijgt, kunnen zij (dan wel in eer en geweten en weloverwogen⁸⁷) de vraag naar transparantie laten doorwegen en de klok luiden. Een dergelijke toepassing van de noodtoestand lijkt mij echter te verregaand. Hoewel de noodtoestand vanuit haar aard een *ad hoc* beoordeling vraagt en op zich ook betrekking kan hebben op materiële⁸⁸ belangen, is de toepassing ervan in een financieel-economische klokkenluiderscontext niet (minstens: niet altijd⁸⁹) opportuun om een schending van het beroepsgeheim te rechtvaardigen. Een dergelijke invulling gaat immers voorbij aan het wezen zelf van dit beroepsgeheim, dat evengoed een algemeen maatschappelijk belang dient.⁹⁰

Deze inschatting is per definitie individueel en gekleurd door eenieders maatschappijbeeld.⁹¹ Net daarom is het cruciaal dat de al uitvoerig vermelde parlementaire reflectie plaatsvindt. De wetgevende macht zou zulke fundamentele maatschappelijke kwesties niet mogen laten beslechten door rechtspraak of rechtsleer en evenmin door haar uitvoerende

tegenhanger.⁹² Beter neemt ze zelf het heft in handen en bepaalt ze – idealiter binnen een duidelijk wetgevend kader gezien het legaliteitsbeginsel⁹³ – de contouren van het beroepsgeheim en de uitzonderingen erop.⁹⁴

3. Het algemeen of bedrieglijk opzet

De algemene filosofie achter de richtlijn is dat klokkenluiders handelen te goeder trouw⁹⁵ en ter vrijwaring van een algemeen belang.⁹⁶ Een laatste mogelijke piste van verweer voor klokkenluiders zou dus betrekking kunnen hebben op het moreel bestanddeel. Is het vereiste opzet wel aanwezig voor het misdrijf waaraan zij zich materieel gezien schuldig maken?

Het Belgisch strafrecht maakt principieel een onderscheid tussen opzettelijke en onopzettelijke misdrijven. Deze laatste lijken niet relevant in een klokkenluiderscontext.⁹⁷ De eerste (opzettelijke) misdrijven moeten dan weer onderscheiden worden naargelang zij een algemeen opzet, bijzonder opzet of soms zelfs een gans bijzonder opzet vereisen. Bij het algemeen opzet volstaat het dat de dader van een misdrijf een bepaalde gedraging wil stellen, ongeacht of deze verboden is. De zuivere goede trouw (in hoofde van de klok-

85. D. VAN GERVEN, “De noodtoestand als uitzondering op het beroepsgeheim van de advocaat, en de ongrondwettigheid van de uitbreiding die hieraan wordt gegeven door artikel 458bis Sw.” (noot onder GwH 26 september 2013), *RW* 2013-14, afl. 32, 1263. In die zin kan de invoering van art. 458bis Sw. – zoals Van Gerven schrijft – gezien worden als een wettelijk (naar een fysieke integriteit) verankerde toepassing van de noodtoestand. Cf. ook F. VERBRUGGEN en S. ROYER, “Komt een terrorist, met zijn advocaat bij de dokter ... Mogen of moeten beroepsgeheimhouders spreken”, *NC* 2017, afl. 1, 33.

86. A. LACHAPPELLE, *La dénonciation à l'ère des lanceurs d'alerte fiscale*, Brussel, Larcier, 2021, 733-734.

87. Cf. R. VERSTRAETEN, “De granaataanslag, het beroepsgeheim en Antigoon”, *NC* 2021, afl. 1, 66.

88. F. VERBRUGGEN en S. ROYER, “Komt een terrorist, met zijn advocaat bij de dokter ... Mogen of moeten beroepsgeheimhouders spreken”, *NC* 2017, afl. 1, 33.

89. Zo haalde Huybrechts in 2015 het hypothetische voorbeeld aan van een revisor of accountant die oordeelt een ernstig financieel misdrijf te moeten bekend maken. Dit om rampscenario's te vermijden waarbij duizenden beleggers riskeren hun gespaarde vermogen te verliezen (L. HUYBRECHTS, “Het beroepsgeheim van de cijferberoepen”, *NC* 2015, afl. 3, 173). Een dergelijke invulling van de noodtoestand gaat evenwel uit van het particuliere financieel belang, daar waar de klokkenluiders-casussen tot op heden eerder het algemene belang van de overheid en belastingbetaler vooropstelden (cf. de schandalen rond *LuxLeaks* die de directe aanleiding waren voor de richtlijn).

90. Cf. o.a. T. BONTINCK, “Le secret professionnel de l'avocat ne peut être levé que dans des circonstances exceptionnelles” (noot onder Cass. 3 oktober 2018), *JLMB* 2019, afl. 6761, 145-146.

91. Cf. ook M. JADOUL, “La désobéissance civile dans le contexte de l'urgence écologique: l'état de nécessité et la liberté d'expression ont le vent en poupe”, *Rev.dr.pén.* 2021, afl. 6, 643. Jadoul bespreekt de noodtoestand in een ecologische context en verwijst naar buitenlandse rechtspraak.

92. In dit verband maakt Kutty ook terechte bedenkingen in het kader van de rechtspraak van het Gentse hof van beroep omtrent de acties van burgerlijke ongehoorzaamheid ten aanzien van genetisch gemodificeerde gewassen (F. KUTTY, “La désobéissance civile peut-elle être constitutive d'une cause justification déduite de l'état de nécessité?” (noot onder Gent 23 december 2014), *JLMB* 2018, afl. 30, 1411-1421).

93. Cf. ook GwH 14 maart 2019, nr. 44/2019 en hierover: S. ROYER en W. YPERMAN, “Horen zien, en (moeten) spreken: Grondwettelijk Hof vernietigt actieve meldplicht OCMW's”, *Juristenkrant* 2019, afl. 386, 1-2. Een wetgever kan van rechtzoekenden niet verwachten telkens bepaalde fundamentele elementen in al hun juridische complexiteit te moeten beoordelen indien daar in hoofde van die rechtzoekende strafrechtelijke consequenties aan gekoppeld worden.

94. Cf. ook F. VERBRUGGEN en S. ROYER, “Komt een terrorist, met zijn advocaat bij de dokter ... Mogen of moeten beroepsgeheimhouders spreken”, *NC* 2017, afl. 1, 23 en 30. Beide auteurs vinden het betreurenswaardig dat wetgeving en rechtspraak geen duidelijkheid scheppen over de precieze spreekrechten en -plichten van beroepsgeheimhouders. Net omdat het beroepsgeheim een dergelijke belangrijke maatschappelijke functie heeft. Zij maken ook een terechte bedenking in verband met het beschikkingsrecht van het beroepsgeheim voor de persoon die erdoor wordt beschermd. Indien de wetgever deze laatste effectief de mogelijkheid had willen geven om de beroepsgeheimhouder van zijn beroepsgeheim te ontheffen, dan had die dat expliciet in de wet moeten inschrijven. Op eenzelfde manier lijkt het continu uitbreiden van de noodtoestand mij niet opportuun. Het is aan de wetgever om uitzonderingen op de regel te bepalen.

95. Cf. § 32 van de preambule.

96. Cf. o.a. § 1, 3, 5, 14, 31, 33, 42 en 80 van de preambule.

97. Een melding door een klokkenluider kan moeilijk vanuit een zekere onachtzaamheid gebeuren. Net integendeel, de klokkenluider overweegt doelbewust bepaalde zaken aan te kaarten en gaat hierbij meestal niet over één nacht ijs.

kenluider) sluit het opzet dan niet uit.⁹⁸ Bij een bijzonder (of gans bijzonder) opzet is een specifieke ingesteldheid noodzakelijk om de dader te kunnen veroordelen. Louter wetens en willens handelen volstaat niet. Voor een bijzonder opzet wordt wél aangenomen dat goede trouw het opzet en dus de veroordeling van de dader uitsluit.⁹⁹

In deze omstandigheden is het voorspelbaar dat bij een schending van het beroepsgeheim de goede trouw een klokkenluider niet zal vrijpleiten, vermits de schending van het beroepsgeheim “slechts” een gewoon opzet vereist. Hetzelfde geldt voor de klokkenluider die kennisneemt van e-mails die niet voor hem/haar zijn bestemd (inbreuk art. 124 WEC). Een merkwaardige situatie ontstaat echter bij hacking. De insider die zijn toegangsbevoegdheid overschrijdt (interne hacking *cf.* art. 550bis, § 2 Sw.) zou als klokkenluider te goeder trouw vrijuit kunnen gaan. Een bedrieglijk opzet is namelijk vereist.¹⁰⁰ De externe hacker (art. 550bis, § 1 Sw.) of de persoon die de gehackte gegevens onthult of verspreidt (zoals een journalist¹⁰¹ of eventueel zelfs de zgn. “facilitator” van de klokkenluider) riskeren een veroordeling. Want voor hen volstaat een algemeen opzet.¹⁰² Hoewel theoretisch mogelijk correct lijkt het er zo wel op dat naar gelang de tenlastelegging waarvoor wordt vervolgd¹⁰³, de kans op een strafrechtelijke vrijspraak voor de klokkenluider vergroot of verkleint.

Ook nu schuilt een mogelijke oplossing voor bovenstaande discussies in het innemen van een proactief standpunt door ondernemingen onderworpen aan de richtlijn. Hierbij valt inspiratie te halen uit de discussies rond zgn. “ethisch hacken”. Ethische hackers testen informaticasystemen en gaan op zoek naar veiligheidslekken. Zij melden deze vervolgens aan de onderneming die het informaticasysteem beheert. Zo helpen ze in de strijd tegen cybercriminaliteit. Niettegenstaande hun oprechte intenties, blijven zij als externe

hackers strafbaar.¹⁰⁴ Door het Centrum voor Cybersecurity werd evenwel het standpunt ingenomen dat bij een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden, de ethische hacker zou toetreden tot een overeenkomst waarbij het gehackte bedrijf vooraf toestemming verleent haar IT-omgeving op kwetsbaarheden te testen en hierover geïnformeerd te worden.¹⁰⁵ In eenzelfde zin zou een klokkenluidersregeling publiek (door publicatie op de website) de rechten en plichten kunnen schetsen van eventuele klokkenluiders, en dit alvorens een melding zelfs maar wordt overwogen. Bij het luiden van de klok gaan zij dan in op de expliciete uitnodiging van een onderneming om intern zaken te onderzoeken en te rapporteren. Deze oplossing geldt natuurlijk maar in de mate die onderneming zelf ook ten aanzien van haar medewerkers correct heeft gedocumenteerd waaraan zij zich kunnen verwachten (*cf. supra* en de *investigative readiness*).

§ 2. Vrijwaring van de resultaten van het onderzoek na het luiden van de klok: wat met Antigoon?

Zodra de klokkenluider een melding doet waarbij één of meerdere strafrechtelijke inbreuken worden gepleegd, rijst meteen de vraag omtrent de bruikbaarheid van dergelijk onrechtmatig verkregen bewijs. Sinds het *Antigoon*-arrest van het Antwerpse hof van beroep¹⁰⁶ en de navolgende bevestiging van deze principes door het Hof van Cassatie¹⁰⁷, heeft een onrechtmatigheid bij de verkrijging van bewijs slechts tot gevolg dat een rechter dit bewijs niet in aanmerking mag nemen:

- hetzij wanneer de naleving van bepaalde vormvoorwaarden voorgeschreven wordt op straffe van nietigheid¹⁰⁸;

⁹⁸ D. VANDERMEERSCH, *Éléments de droit pénal et de procédure pénale*, Brugge, die Keure, 2009, 161; C. VAN DE WYNGAERT, S. VANDROMME en P. TRAEST, *Strafrecht en strafprocesrecht*, Oud-Turnhout, Gompel & Svacina, 2019, 325 en F. DERUYCK, *Overzicht van het Belgisch algemeen strafrecht*, Brugge, die Keure, 39. *Cf.* ook Corr. Brugge 11 maart 2009, *Jaarboek Handelspraktijken & Mededinging* 2009, 265.

⁹⁹ F. KUTY, *Principes généraux du droit pénal belge*, vol. I, Brussel, Larcier, 2009, 274 en C. VAN DE WYNGAERT, S. VANDROMME en P. TRAEST, *Strafrecht en strafprocesrecht*, Oud-Turnhout, Gompel & Svacina, 2019, 329.

¹⁰⁰ *Contra*: I. DELBROUCK, “Informaticacriminaliteit” in X, *Postal Memorialis – Strafrecht, strafvordering en bijzondere wetten*, Mechelen, Kluwer, 2010, 220-223. Delbrouck haalt onder het misdrijf interne hacking (dat een bedrieglijk opzet vereist) het voorbeeld aan van de medewerker die gegevens bemachtigt om ze aan de pers mee te delen.

¹⁰¹ Journalisten kunnen overeenkomstig art. 6 van de wet van 7 april 2005 tot bescherming van het journalistiek bronnengeheim niet vervolgd worden op basis van art. 505 Sw. wanneer zij het recht uitoefenen om hun informatiebronnen te verzwijgen. Deze beperking heeft echter geen betrekking op de heling van gehackte gegevens (art. 550bis, § 7 Sw.) (O. LEROUX, “Criminalité informatique” in H.D. BOSLY en C. DE VALKENEEER (eds.), *Les infractions contre les biens*, Brussel, Larcier, 497).

¹⁰² *Cf.* ook J. KERKHOFS en P. VAN LINTHOUT, *Cybercrime 3.0*, Brussel, Politea, 2019. Een hackerscollectief dat IP-adressen en persoonsgegevens publiceert van bezoekers van fora voor zedendelinquenten, is strafbaar gezien een algemeen opzet volstaat (indien die gegevens verkregen werden via hacking van die fora).

¹⁰³ Dit natuurlijk onder het voorbehoud van een herkwalficatie door de strafrechter. Deze kan – voor de feiten waarvoor hij wordt geadieerd door de akte van aanhangigmaking – onder de toepasselijke voorwaarden steeds beslissen de volgens hem juiste kwalificatie in aanmerking te nemen.

¹⁰⁴ F. MOLS en J. KEUSTERMANS, “Informaticacriminaliteit” in A. VANDEPLAS, P. ARNOU, S. VAN OVERBEKE en S. VANDROMME (eds.), *Strafrecht en strafvordering. Commentaar met overzicht van rechtspraak en rechtsleer*, Mechelen, Kluwer, 2020, 25.

¹⁰⁵ Zie hiervoor: www.ccb.belgium.be en de aldaar gepubliceerde FAQ rond het beleid voor de gecoördineerde bekendmaking van kwetsbaarheden.

¹⁰⁶ Antwerpen 11 april 2003, *T.Strafr.* 2004, afl. 2, 147-148.

¹⁰⁷ Cass. 14 oktober 2003, P.03.0762.N

¹⁰⁸ De nietigheden in het Belgisch strafprocesrecht zijn op heden eerder beperkt. Het betreft inbreuken op art. 86bis-86ter Sv. (anonieme getuigenissen), art. 112duodecies Sv. (gebruik van de polygraaf of leugendetector) en art. 463 WIB 1992/art. 74bis WTB (het verhoor van fiscale ambtenaren als getuige).

- hetzij wanneer de begane onrechtmatigheid de betrouwbaarheid van het bewijs heeft aangetast¹⁰⁹;
- hetzij wanneer het gebruik van het bewijs in strijd is met het recht op een eerlijk proces.¹¹⁰

Het EHRM bevestigde dat deze rechtspraak geen schending inhoudt van artikel 6 EVRM¹¹¹ en finaal verleende ook de wetgever deze aanvankelijk louter jurisprudentiële zienswijze democratische legitimiteit. Dit door in 2013 artikel 32 VT Sv. in te voegen dat voormelde gedachtestrepen quasi letterlijk herneemt.

Voor de klokkenluider die zich door of voorafgaand aan de melding schuldig maakt aan een misdrijf, lijkt de *Antigoon*-toets een quasi-vrijgeleide vanuit bewijsrechtelijk standpunt. De *Antigoon*-criteria nemen op zich het plegen van een misdrijf niet in aanmerking als reden om het hierdoor verkregen bewijs uit te sluiten. Het Hof van Cassatie bevestigde deze zienswijze ook al in een klokkenluiderscontext. Zo luidde het in een arrest van 28 februari 2017¹¹² dat het gebruik van onrechtmatig verkregen inlichtingen¹¹³ die niet dienen als bewijs, maar louter worden aangewend ter oriëntering van een onderzoek¹¹⁴, niet leidt tot de ontvankelijkheid van de strafvordering. De bodemrechter die nagaat of het gebruik van dergelijke inlichtingen het eerlijk proces in zijn geheel niet aantast, doorstaat de cassatietoets. Ook in een fiscale procedure werden dergelijke principes al toegepast ten aanzien van klokkenluiders uit de financiële sector.¹¹⁵ Anders

dan in het *KB Lux*-dossier¹¹⁶ doen onderzoekers er op heden dus beter aan de eventuele onregelmatigheid gepleegd door een klokkenluider voor of tijdens een melding, te aanvaarden en niet onnodig zaken te ensceneren. Dat lijkt immers nergens (meer) voor nodig.¹¹⁷

Specifiek voor bewijs verkregen door een schending van het beroepsgeheim geldt sinds de wettelijke erkenning van *Antigoon* bovendien dat het niet per definitie moet worden geweerd. Daar waar *Antigoon* in zijn louter jurisprudentiële invulling nog enige flexibiliteit kende om het beroepsgeheim en andere fundamentele rechten te vrijwaren, is dit sinds 2013 niet noodzakelijk meer het geval.¹¹⁸ Opnieuw bevestigde het Hof van Cassatie dit in een relatief recent arrest. Op 18 januari 2018¹¹⁹ besliste het dat vergaring van bewijs met miskennis van het beroepsgeheim de aanwending ervan niet onmogelijk maakt. Hiermee lijkt niet gezegd dat het beroepsgeheim indirect geen wering rechtvaardigt.¹²⁰ Langs de kant van de verdediging moet men er dan wel een punt van maken en dit kaderen in (waarschijnlijk) een schending van het recht op een eerlijk proces.¹²¹ Meteen wordt wel het laatste punt van parlementaire reflectie duidelijk waartoe deze bijdrage oproept. Wat moet wel of niet worden geweerd na een inbreuk op het beroepsgeheim. Een wetgevend debat hierover is (zelfs los van de richtlijn) niet alleen opportuun, het is zonder meer noodzakelijk.¹²²

¹⁰⁹ Bv. Cass. 25 mei 2005, P.05.0672.N: wanneer DNA-bewijs wordt verkregen in strijd met de hiervoor geldende regelgeving.

¹¹⁰ Bv. EHRM 27 november 2008, *Salduz / Turkije* (verhoor van een verdachte zonder bijstand van diens advocaat) en EHRM 25 september 2012 of *El Haki / België* (gebruik van verklaringen afgelegd in Marokko zonder *ad hoc*-verificatie dat deze niet werden verkregen in strijd met art. 3 EVRM (het verbod op foltering, onmenselijke of vernederende behandeling)).

¹¹¹ EHRM 28 juli 2009, *Lee Davies / België*.

¹¹² Cass. 28 februari 2017, P.16.0261.N.

¹¹³ I.c. betrof het gegevens van cliënten die een bediende bij een Liechtensteinse bank zich illegaal had toegeëigend. Deze gegevens werden nadien verkocht aan de Duitse overheid die ze op haar beurt aan de Belgische autoriteiten bezorgde.

¹¹⁴ Wat exact de situatie is van een melding door een klokkenluider. Ook deze dient als start voor verder onderzoek.

¹¹⁵ Deze casus had betrekking op een informaticus van een financiële instelling die op onrechtmatige wijze gegevens van cliënten had bekomen, deze overhandigde aan de Franse overheid waarna die ze weer bezorgde aan de Belgische autoriteiten in het kader van een rechtshulpverzoek. Hierdoor werd deze informatie (aldus de rechtbank) rechtmatig bekomen (Rb. Antwerpen 10 juni 2019, *TFR* 2019, afl. 557, 246).

¹¹⁶ Cass. 31 mei 2011, P.10.2037.N.

¹¹⁷ In dit dossier werden opnieuw gegevens van cliënten gestolen door bedienden van een bank (Kredietbank Luxemburg). Zij hoopten ze te kunnen gebruiken om een hogere opzegvergoeding te onderhandelen. Vervolgens boden ze die gegevens onder meer aan bij de Brusselse gerechtelijke politie. Deze zou echter, met medeweten van de toenmalige onderzoeksrechter, de wederrechtelijke oorsprong van de gegevens hebben willen verdoezelen en ze “toevallig” ergens hebben proberen aantreffen. Sinds *Antigoon* zouden diezelfde Brusselse speurders en onderzoeksrechter de gegevens gewoon hebben kunnen gebruiken als oriënterend voor hun onderzoek (cf. L. KELL, “Klokkenluider of dief: fiscaal bruikbaar gerief”, *Fisc.Koer.* 2019, afl. 6, 84).

¹¹⁸ A. DE NAUW, “Na de jurisprudentiële, een bijkomende wettelijke verenging van de sanctie van de bewijstuitsluiting” (noot onder Cass. 10 juni 2014), *RW* 2014-15, afl. 30, 1190-1193 en R. VERSTRAETEN, “De granaataanslag, het beroepsgeheim en Antigoon”, *NC* 2021, afl. 1, 66-67.

¹¹⁹ Cass. 18 januari 2018, P.16.0031.N.

¹²⁰ Cf. o.a. P. RENIER en L. CASSIMON, “Antigoon vs. beroepsgeheim: beschermt cassatie onze grondrechten?” (noot onder Cass. 18 januari 2018), *Fisc.Act.* 2018, afl. 1-5 en G. VAEL en Y.L. ZHENG, “Nouvel arrêt de la Cour de cassation en matière d’utilisation de preuves obtenue de manière irrégulière: confirmation de la jurisprudence Antigone ou rendez-vous manqué” (noot onder Cass. 18 januari 2018), *Act.Fisc.* 2018, afl. 22, 5.

¹²¹ Hierbij volstaat het niet dat de bodemrechter vaststelt dat er alsnog tegenspraak kon gevoerd worden over het verkregen bewijs om een schending van het recht op een eerlijk proces te weerleggen. Hij kan bv. één of meer van volgende omstandigheden in aanmerking nemen: (1) de onregelmatigheid werd al dan niet opzettelijk of ingevolge een niet te verontschuldigen onachtzaamheid begaan; (2) de ernst van het misdrijf overstijgt veruit de begane onregelmatigheid; (3) de onregelmatigheid betreft alleen een materieel element van het bestaan van het misdrijf; (4) de onregelmatigheid heeft een louter formeel karakter; (5) de onregelmatigheid heeft geen weerslag op het recht of de vrijheid die door de overschreden norm wordt beschermd (Cass. 5 mei 2020, P.19.1272.N). Of en in welke mate deze criteria een prominente rol zullen innemen in een klokkenluiderscontext zal de tijd uitwijzen.

¹²² Cf. ook F. BLOCKX, “Medisch beroepsgeheim en strafvervolgning: laat de granaat geen boemerang worden”, *Juristenkrant* 2019, afl. 398, 11.

IV. CONCLUSIE

Uit hetgeen voorafgaat blijkt dat alleen al vanuit straf(proces)rechtelijke invalshoek diverse vragen rijzen omtrent de impact en implementatie van de richtlijn. Niettegenstaande het straf(proces)recht het exclusieve domein is en blijft van de lidstaten zijn er in dit verband verschillende (ook voorheen al) onopgeloste vraagstukken. Deze zijn niet zuiver juridisch getint of werk voor specialisten. Het zijn fundamentele overwegingen die de richting bepalen waarin we als maatschappij willen evolueren. De richtlijn is een absolute meerwaarde en zonder meer een noodzakelijke stap richting een meer transparante samenleving. Maar even cruciaal is een vrijwaring van het beroepsgeheim en tegelijk een duidelijke en consequente afbakening van de mate waarin ondernemingseigen informatie vertrouwelijk is en moet blijven.

Die mate van vertrouwelijkheid is zoals hoger geschetst het domein bij uitstek waarop individuele ondernemingen zelf initiatief kunnen en moeten nemen. De daadwerkelijke implementatie van een klokkenluidersregeling kan dan weer zo'n formele regeling op termijn feitelijk overbodig maken. Minstens weet op die manier iedereen goed waar de grenzen liggen bij het luiden van de klok.

Afwegingen in verband met het beroepsgeheim spelen dan weer ruimer. In welke mate willen en moeten we dit vrijwaren. Niet zozeer in een individueel, maar wel in een algemeen maatschappelijk belang. En liefst niet uitsluitend afgebakend door rechtsleer of rechtspraak, maar bepaald door en gestuurd vanuit een zo ruim mogelijke parlementaire meerderheid. Ten behoeve van deze parlementaire denkoefening past het wel de intussen al wat oudere overwegingen te citeren van advocaat-generaal Damien VANDERMEERSCH. Die schreef omtrent de *Antigoon*-principes in een conclusie bij het arrest van het Hof van Cassatie van 2 maart 2005:

“Il est cependant des libertés et des droits fondamentaux dont on ne peut pas relativiser les violations sous peines de les banaliser: dans ces hypothèses, seule l'exclusion de la preuve peut venir sanctionner adéquatement l'irrégularité commise.

Je songe ici notamment à la preuve recueillie à la suite d'une perquisition ou d'une écoute illégale, à la preuve obtenue en violation du secret professionnel, du droit au silence ou des droits de la défense et à la preuve qui n'a pas été soumise au principe du contradictoire.

Comme la protection de ces droits ne s'identifie pas nécessairement au droit à un procès équitable, il me paraît essentiel de poser ici une balise supplémentaire: la preuve devrait être exclue en cas de violation des libertés et droits fondamentaux lorsque la valeur protégée (secret professionnel, inviolabilité du domicile, ...) représente, dans une société démocratique, une valeur supérieure à celle de l'efficacité de la justice pénale.”¹²³

Beroepsgeheim en bescherming van klokkenluiders zijn elk een essentieel onderdeel van een goed functionerende democratische samenleving. Zij verdienen beide een volwaardig parlementair debat. De relativisering van het beroepsgeheim ten voordele van de klokkenluider riskeert dit eerste alledaags (banaal) te maken. Net dat zou een fundamentele vergissing zijn. Het is dus aan de wetgever om duidelijk af te bakenen wat kan en wat niet. Enkel zo kan de omzetting van de richtlijn de meerwaarde bieden waarvoor ze bedoeld is. Het creëren van een meer transparante en duurzame maatschappij die tegelijk haar juridische principes zoals het beroepsgeheim vrijwaart.

¹²³. Cass. 2 maart 2005, *JT* 2005, 213.