Prof. mr. J.J.C. Kabel[*]*, drs. E.E.M. Sips MSc*[**] *en mr. dr. E.P.M. Thole*[***]

Klokkenluiders, interne meldregelingen, anonimiteit en privacy

150

Trefwoorden:
klokkenluiders, interne meldregelingen, anonimiteit

Van oudsher domineren de Amerikanen de markt van de 'whistleblowing'-meldlijnen. In de Verenigde Staten worden callcenters gebruikt om meldingen te ontvangen over een veilige werkomgeving. In navolging van de Corporate Sentencing Guidelines uit 1991 worden deze callcenters in het bedrijfsleven ingezet voor medewerkers om integiteitsmeldingen te ontvangen. In 2002, met de komst van Sarbanes Oxley, waarin het hebben van een anonieme meldmogelijkheid verplicht werd gesteld voor de beursgenoteerde bedrijven, groeide het gebruik van de callcenters. Toen de eerste Europese bedrijven – meestal onder externe druk – een klokkenluidersmeldlijn introduceerden, werd dit dan ook meestal geregeld bij één van de Amerikaanse callcenters.

Sinds 2005 bestaat er in Nederland een andersoortige oplossing ter inrichting van de meldregeling. Het in Amsterdam gevestigde bedrijf People Intouch B.V. verzorgt het SpeakUp-systeem, bestaande uit een geïntegreerd telefoon- en websysteem, dat organisaties in staat stelt om met de (anonieme) melder te communiceren over vermoedens van ernstige misstanden in de organisatie van de melder. Grote ondernemingen, zoals KPN, Randstad, HEMA, Deutsche Post en Hoffmann-La Roche, maken gebruik van het SpeakUp-systeem.

Evita Sips heeft een achtergrond in culturele antropologie en criminologie, en is sinds 2007 werkzaam bij People Intouch als managing consultant. Jan Kabel en Elisabeth Thole, respectievelijk redactieraadlid en redactielid van P&I, zijn in gesprek met Evita over hoe zo een interne meldregeling in de praktijk werkt en welke privacyaspecten daarmee gemoeid zijn.

Inleiding

Klokkenluiders als Bos, Schaap De Kwaadsteniet en Van Buitenen hebben maatschappelijke aandacht gevraagd voor ernstige misstanden in de publieke en de private sector. Bouwfraudes, haarscheurtjes in het reactorvat van de atoomcentrale in Petten, ondeugdelijk modelonderzoek door het RIVM of declaratiefraude bij Europese organen zouden zonder hen niet of veel later aan het licht zijn gekomen. Dat het met hen niet altijd even goed is afgelopen, om het maar zachtjes te zeggen, is wellicht een symptoom van het problematische karakter van het klokkenluiden. Het aan de grote klok hangen van interne misstanden bij bedrijven of de overheid wordt niet altijd gemakkelijk geaccepteerd. Binnen bedrijven of bij de overheid wordt eerder uitgegaan van de norm dat misstanden intern moeten worden gemeld en opgelost. De nadere wettelijke regeling van het klokkenluidenverschijnsel in de overheidssector,[1] hanteert dat uitgangspunt. Daarop is overigens weer kritiek uitgeoefend vanuit een oogpunt van vrijheid van meningsuiting die de klokkenluidende ambtenaar zou moeten toekomen.[2] De Meij en Schuijt zien daarin en in de perspublicaties die daaruit voortvloeien dé oplossing voor de gesignaleerde misstanden. Verhulp is daar niet zo van overtuigd en constateert aan de hand van de RIVM-affaire dat de media een geheel eigen belang hebben bij publicaties over deze en soortgelijke affaires, een belang dat verstorend kan werken op het oplossen van misstanden. In die laatste benadering heeft interne melding een hoge prioriteit. Dergelijke meldingen gaan vaak, hoewel niet altijd, gepaard met anonimiteit van de melder. Die anonimiteit dient de privacybelangen van de melder, maar maakt tegelijkertijd inbreuk op privacy- en procedurele belangen van de aangeklaagde omdat die anonimiteit het moeilijk maakt de herkomst en voor een belangrijk deel ook de juistheid van de aanklachten vast te stellen. De Artikel 29-Werkgroep heeft in haar opinie over klokkenluiders de rechten van de aangeklaagde op informatie, toegang, rectificatie en vernietiging met betrekking tot zijn persoonsgegevens benadrukt. Restricties op die rechten zouden steeds op noodzaak en proportionaliteit

---

* **Jan Kabel is emeritus hoogleraar informatierecht bij het Instituut voor Informatierecht van de Universiteit van Amsterdam en Of Counsel bij DLA Piper te Amsterdam.**

** **Evita Sips is managing consultant bij People Intouch te Amsterdam. Op 2 juli 2010 heeft Evita voor haar scriptie 'Condemn Silence. Honour the Whistleblower?' de NvK (Nederlandse Vereniging voor Kriminologie) scriptieprijs 2009-2010 gewonnen.**

*** **Elisabeth Thole is advocaat bij Van Doorne te Amsterdam en hoofd van het Van Doorne Privacyteam.**

1 Wet van 23 januari 2003, *Stb*. 2003, nr. 60 tot wijziging van de Ambtenarenwet in verband met de integriteit. Het gaat daarbij in het bijzonder om artikel 125 Ambtenarenwet.

2 Zie voor die discussie onder meer Gerard Schuijt, 'Laat de klok maar luiden', *Mediaforum* 2001-6, p.185; J.M. de Meij, 'Klokkenluiden bij de overheid in Nederland en in Zweden', *NJB* 2003-9, p. 418-425; Evert Verhulp, 'Zoals de klokkenluider thuis luidt…', in: *Van Ontvanger naar Zender, Opstellen aangeboden aan prof. mr. J.M. de Meij*, Amsterdam: Otto Cramwinkel Uitgever 2003, p. 357-371; zie voor bescherming door art. 10 EVRM van de klokkenluider EHRM 12 februari 2008 (*Guja/Moldavia*).

moeten worden onderzocht.[3] Het systeem dat in dit interview aan de orde komt, zou die toets kunnen doorstaan.

Vraag 1
Wat is het verschil tussen een klokkenluidersregeling en een intern meldsysteem zoals dat van People Intouch?

Een interne meldregeling in de betekenis van de verschillende governancecodes is er in ieder geval *niet* op gericht om de klok te laten luiden. Klokkenluiden is aan de orde op het moment dat het eigenlijk al te laat is – een werknemer voelt zich genoodzaakt om naar buiten te treden met de informatie. Interne meldregeling is dan ook een betere term dan klokkenluidersregeling. Zij beoogt het vroegtijdig signaleren van misstanden om zo de schade aan bedrijf, melder, en ander personeel te voorkomen, dan wel te minimaliseren. Een technische oplossing zoals het SpeakUp-systeem kan door bedrijven worden ingezet als laagdrempelig communicatie-instrument binnen de meldregeling. Ons bedrijf is dan een doorgeefluik en in privacyrechtelijke zin een bewerker en geen verantwoordelijke.

Vraag 2
Waarom zouden bedrijven kiezen voor het SpeakUp-systeem?

Optreden als je iets waarneemt als niet-betrokken omstander, is allesbehalve vanzelfsprekend. Deze problematiek is van alle tijden en culturen: het is een instinct om de andere kant op te kijken in plaats van het eigen bestaan op het spel te zetten. Bij de getuige op de werkvloer is dit net zo. Sterker nog, naast dit instinctief wegkijken spelen hier ook logische rationele overwegingen een rol die de werknemer ervan zullen weerhouden om aan de bel te trekken. De voornaamste daarvan is de – gegronde – angst voor repercussies. In tegenstelling tot slachtoffers, hebben getuigen geen enkele drijfveer om te melden, eerder een motief om *niet* te melden. Een verstandige getuige gaat niet melden als dit niet voor 100% veilig kan en hij of zij niet *in control* is. Een interne meldregeling opstellen zonder goed doordrongen te zijn van deze problematiek en deze mee te nemen in de opzet ervan, is bij voorbaat kansloos: er zal geen melding binnenkomen. Bedrijven die zich hiervan bewust zijn, zijn doordrongen van het nut van het implementeren van een effectieve interne meldregeling.

Vraag 3
Hoe gaan de meldingen via het SpeakUp-systeem?

De medewerker van een organisatie die zich heeft aangesloten bij SpeakUp heeft toegang tot SpeakUp middels een gratis telefoonnummer of een website, en is continu bereikbaar. SpeakUp is vanaf elke locatie te bereiken – we hebben gratis telefoonlijnen in alle landen waar dit technisch mogelijk is. Het SpeakUp-systeem wordt per land opgezet in de talen die de organisatie wenst. Momenteel draait het systeem in meer dan 65 talen. De melder draait het nummer, toetst de toegangscode van de organisatie in, ontvangt een organisatiespecifieke welkomsttekst en instructies in zijn of haar haar eigen taal en spreekt de boodschap in – dit kán anoniem. Meestal heeft de melder de boodschap vooraf opgeschreven, zodat die nauwkeurig kan worden gedaan. De melder ontvangt een uniek meldingsnummer en wordt verzocht binnen een week terug te bellen. Zodra de melder ophangt, vertaalt SpeakUp de melding, en wordt het tweetalig transscript beschikbaar gesteld aan de verantwoordelijke functionaris binnen de organisatie – vaak is dit de Group Compliance Officer. De ontvanger van de melding formuleert een eerste antwoordboodschap, meestal een bevestiging en vervolgvragen, en plaatst deze op het SpeakUp-systeem. SpeakUp spreekt die, indien nodig vertaald, in op het SpeakUp-systeem. De melder belt weer in en kan weer reageren op de boodschap van de compliance officer. Deze cyclus kan onbeperkt herhaald worden. Voor het websysteem werkt het ongeveer hetzelfde. Kenmerkend aan het SpeakUp-systeem is, dat het zo is ontworpen dat er directe – kwalitatieve en nauwkeurige – communicatie ontstaat tussen de melder en de organisatie; er zit geen verstorende schakel tussen. Bovendien hebben beide partijen de tijd om hun bericht nauwkeurig te formuleren, eventueel met behulp van advies van anderen: gedurende het proces zijn beide partijen *in control*.

Vraag 4
Wat is jullie visie op anoniem melden?

Met het oog op de meldproblematiek zoals zojuist besproken, is anonimiteit een minimale voorwaarde om getuigen te laten spreken; getuigen steken niet zo maar hun nek uit. Met anonimiteit heb je echter wel te maken met het veelgehoorde argument dat daarmee het risico op valse meldingen wordt verhoogd. In tegenstelling tot de ouderwetse anonieme brief, is het bij het SpeakUp-systeem mogelijk om te communiceren met de anonieme melder. Door het stellen van de juiste verificatievragen, kunnen valse meldingen worden uitgefilterd en onmiddellijk worden vernietigd. Wat we overigens ook zien, is dat anonieme melders zich na een eerste of tweede cyclus alsnog bekend maken. Anonimiteit kan dus ook slechts een fase zijn, die voorafgaat aan vertrouwelijkheid.

Vraag 5
Hoe zorgen jullie dat de privacy van de betrokkenen (slachtoffers, getuigen, daders) wordt gewaarborgd?

Bij een interne meldregeling gaat het voornamelijk om de rechten van twee groepen: de melders en de aange-

3 Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime, WP 117. Zie verder Christan Runtel e.a., 'Anonymous Hotlines for Whistleblowers. The U.S. Sarbanes Oxley Act and European Compliance Issues', *CRi* 2005-5, p. 135-140.

klaagden. Voor beide partijen geldt als belangrijkste waarborg dat ons systeem zo ontworpen is dat alle data zorgvuldig worden verwerkt. Alle boodschappen worden woord voor woord neergezet zonder verstoring door een operator of een tolk. Bovendien staat de organisatie in direct contact met de melder, waardoor uitsluitend die vragen worden gesteld die relevant zijn voor het doel waartoe de meldlijn dient. Specifiek voor de melder wordt de privacy verder gewaarborgd door de mogelijkheid om anoniem te melden. Voor de beschuldigde wordt de gegrondheid en de kwaliteit van de melding verder gegarandeerd doordat communicatie met de (anonieme) melder mogelijk is – valse meldingen of meldingen die niet thuishoren op een meldlijn kunnen zo worden uitgefilterd.

Vraag 6
Hoe gaan jullie om met het CBP en privacytoezichthouders van andere landen?

Wij adviseren onze klanten een melding te verrichten of anderszins een autorisatie te vragen in de landen waar dit moet. We helpen hen met alle informatie die wij hebben. Deze is meestal gebaseerd op de praktijkervaring van andere klanten, die hun kennis graag delen. Onze klanten vragen vaak advies van interne of externe juristen. Het is echter niet eenvoudig om het volgens de regels te doen. In 2006 heeft de Artikel 29-Werkgroep een opinie opgesteld, die elke lidstaat anders interpreteert.[4] In de praktijk blijkt verder dat de lokale toezichthouders zelf ook niet goed op de hoogte zijn – waardoor het voor de organisatie bijna onmogelijk wordt om zich aan de wet te houden. Bovendien ontmoedigt de Artikel 29-Werkgroep anonieme meldingen omdat zij ervan uitgaat dat communicatie met de anonieme melder niet mogelijk is. Ze zijn niet op de hoogte van de nieuwe technieken. Kortom: hier is zeker ruimte voor verbetering.

Vraag 7
Wie zijn jullie concurrenten en wat zijn de belangrijkste verschillen?

Zoals aangegeven, beheren de Amerikanen van oudsher de markt van de 'whistleblowing'-meldlijnen. De grootste aanbieders zijn*: Global Compliance* en *Ethics Line*: zij bieden een oplossing aan waarbij de medewerker 24/7 kan bellen met een Amerikaans callcenter en live wordt bevraagd, indien nodig met behulp van een tolk. Ook zijn inmiddels in Engeland meerdere callcenters actief, waaronder *Expolink*, tevens werkend vanuit het Anglosaksische perspectief. In Duitsland werkt een aantal bedrijven met het ombudsman-model: de medewerker die meldt, doet dit direct bij een externe partij die zich inhoudelijk en juridisch buigt over de zaak. In Nederland wordt de oplossing van een (interne of externe) vertrouwenspersoon, die persoonlijk en tijdens vaste uren te benaderen is, nog veel gebruikt. Hoffmann Bedrijfsrecherche biedt een andere oplossing voor Nederlandse bedrijven: ze bieden een telefoonnummer waar de werknemers naartoe kunnen bellen voor een live telefoongesprek.

De grootste concurrenten van People Intouch zijn daarmee de Amerikaanse callcenters, zoals Global Compliance en Ethics Line die al decennia lang in de Verenigde Staten klaaglijnen voor Amerikaanse medewerkers faciliteren. Ons inziens is deze oplossing niet geschikt voor de Europese omgeving. In Europa willen we geen klaagcultuur, maar veeleer een omgeving waar mensen elkaar eerst direct aanspreken op gedrag en waar oplossingen gezocht worden met behulp van normale rapportagelijnen. Uitsluitend als *laatste redmiddel* – voor de meldingen die anders niet gedaan zouden worden – dient een meldlijn te worden gebruikt. Een ander belangrijk verschil is dat er bij callcenters geen sprake is van directie communicatie tussen de melder en het bedrijf. Een operator probeert tijdens het eenmalig telefoongesprek zo veel mogelijk informatie uit de melder te halen – hij bepaalt welke informatie voor het bedrijf en het onderzoek belangrijk is. Wij denken dat een operator deze inschatting niet zou moeten kunnen maken. Er wordt zo onzorgvuldig met de data omgesprongen. Belangrijk, ook voor de privacywetgeving, is dat er bij ons geen persoonsgegevens naar de USA gaan.

Vraag 8
Welke soorten organisaties maken gebruik van een interne meldregeling, zoals het SpeakUp-systeem?

Dit is zeer divers, en kan variëren van hele grote ondernemingen tot ook de wat kleinere organisaties, met bijvoorbeeld maar twaalf werknemers. In sommige gevallen geldt een wettelijke verplichting tot het invoeren van een interne meldregeling. In andere gevallen is het een eigen keuze van de organisatie.

Vraag 9
Welke tips zijn er te geven bij het opzetten van een klokkenluidersregeling?

Ten eerste: noem het geen klokkenluidersregeling – de term is allesbehalve uitnodigend en bovendien incorrect in dit verband. Verder, wees ervan doordrongen dat het opzetten van een effectieve meldregeling makkelijker gezegd is dan gedaan. Wees bewust van de meldproblematiek – zorg daarom voor laagdrempeligheid – en ook van het belang van de bedrijfscultuur, de beleving van de gedragscode en de juiste signalen vanuit het management. Werk de regeling ook uit in wat past bij de eigen organisatie; dus geen regeling van het net plukken en die kopiëren. Verder: houd rekening met nationale privacyregelgeving en met medezeggenschapskwesties. Zorg voor één centraal ontvangstpunt van de meldingen, waarna de meest geëquipeerde persoon de melding onderzoekt. Gebruik anonimiteit op de juiste manier: alleen als laatste redmiddel en wanneer communicatie met de anonieme melder mogelijk is.

4 Opinion 1/2006, zie noot 4.

Vraag 10
Kun je een top vijf van soorten meldingen noemen?

Ongeveer 50% van de meldingen die binnenkomen zijn serieuze HR-gerelateerde zaken – denk aan *mobbing* of seksuele intimidatie – en ook onveilige arbeidsomstandigheden. 40% zijn zaken als fraude en corruptie, 10% overig. Opvallend is dat ongeveer 50% van de meldingen anoniem gedaan wordt.