tekst Erwin Gevers | **foto's** Frank Visschedijk

Schending van privacy ligt gevoelig

SNUFFELEN IN DE MAIL?

Porno kijken op een bedrijfscomputer in de baas z'n tijd. Of urenlang chatten met je vriend(in) op een zakelijk mobieltje. Privaat misbruik van bedrijfsmiddelen, zoals computers, email en internet, en werktijd komt steeds vaker voor en wordt urgenter. In hoeverre mag een baas snuffelen in het mailverkeer van werknemers en wanneer schuurt dat met de privacy? En net zo interessant: hoe kun je het misbruik voorkomen?

Recente onderzoeken van rechtsbijstandsbureau ARAG, Intermediair en OfficeTime.net (leverancier van timetrack-systemen) leveren een onthutsend beeld op. Ruim twee uur per werkdag besteedt de werknemer aan online surfen en chatten op een zakelijke account voor privédoeleinden. In 2007 kwam EY met nog schokkender cijfers naar buiten: bijna vijf uur per dag bleken managers uit het bedrijfsleven en van de overheid onder werktijd bezig met privézaken. Opmerkelijk daarbij is dat één op drie werkgevers de bedrijfscomputers monitoren om te zien of ze wel bedrijfsmatig worden ingezet.

Dagelijks porno downloaden

Conflicten over privégebruik komen niet vaak voor de rechter. Meestal lossen werkgever en de beklaagde werknemer het onderling op door middel van ontslag of een berisping. Het is dus

Directeur Herbert Krabbe van onderzoeksbureau RJ Safety & Security: “Sinds de komst van internet en social media zien we een stijging van het aantal zaken.”

ook lastig om een exact statistisch beeld te krijgen. Werkgevers en werknemers zijn uiteraard niet openhartig over misbruik van bedrijfsmiddelen en werktijd. Volgens directeur Herbert Krabbe van het particuliere onderzoeksbureau RJ Safety & Security zien we nu nog maar een topje van de ijsberg. Het Enschedese bureau doet in opdracht van bedrijven en organisaties rechercheonderzoek bij verdenking van misbruik van bedrijfsmiddelen. “Sinds de komst van internet en social media zien we een stijging van het aantal zaken. Wij krijgen gemiddeld tien keer per jaar een dergelijk verzoek van een bedrijf. In alle gevallen is de situatie dan al behoorlijk uit de hand gelopen. Neem bijvoorbeeld werknemers die dagelijks porno downloaden of betaalde seks-sites bekijken of concurrentiegevoelige informatie tegen betaling doorverkopen aan de concurrent. Het is geen uitzondering dat werkgevers opgezadeld worden met facturen van 800 tot 900 euro per maand omdat werknemers betaalde sex-sites hebben bezocht.” Krabbe heeft een zaak bij de hand gehad die hem nog raakt. “Een werknemer had kinderporno gedownload op de computer van de zaak. Toen we de werknemer met het bewijs confronteerden, bekende hij meteen. Hij stortte volledig in elkaar en ik heb hem dringend verzocht om professionele hulp te zoeken. Toen hij dat deed was dat voor mij een soort morele genoegdoening”.

Onrust en onduidelijkheid

Ook mr. Saskia van de Griek van het in Almelo gevestigde advocatenkantoor Corporate Law, bedrijfsadvies en advocatuur signaleert een toenemende belangstelling van werkgevers voor deze materie. Haar kantoor is gespecialiseerd in onder meer arbeidsrecht, ict-recht en privacyrecht. Zij geeft onder anderen juridische adviezen over hoe misbruik van bedrijfsmiddelen >>

“Werkgevers mogen **niet zomaar snuffelen in mailverkeer”**

te voorkomen en conflicten met de werknemer op te lossen. “Er komen veel vragen over de aangescherpte privacywetgeving. Werkgevers mogen niet zomaar rondsnuffelen in bijvoorbeeld mailverkeer van werknemers. Diverse waarborgen zijn noodzakelijk. Daar heerst bij werkgevers onrust en onduidelijkheid over.”

Onderling ‘schikken’

Twentse rechtszaken over privé-misbruik van bedrijfsmiddelen zijn echter niet voorhanden. Meestal worden deze arbeidsconflicten onderling ‘geschikt’. “Veel werkgevers doen geen aangifte bij de politie, maar komen eerst bij ons”, zegt Krabbe van RJ Safety & Security. “We gaan direct met de werkgever in gesprek en adviseren over de aanpak en de in te zetten middelen.” Deze instrumenten variëren van de inzet van een camera, peilzenders, track-en-trace systemen in de (zakelijke) email en het internetaccount van de werknemer of het schoontrekken van een laptop of smartphone tot het opvragen van een Verklaring van Goed Gedrag of een BKR-registratie. We moeten de werknemer na het onderzoek altijd vertellen dat we hem of haar hebben nagetrokken. Onze onderzoeksresultaten kunnen dienen als bewijslast in een eventueel politieonderzoek. Maar meestal komt het tot een vaststellingsovereenkomst tussen werkgever en werknemer dat resulteert in ontslag”.

Cameratoezicht op de werkvloer. Wat moet u doen?

Privacytoets uitvoeren:

- Is de inzet van camera’s echt noodzakelijk?
- Kan opsporing van misbruik ook via een ander middel worden bereikt?
- Is het bedrijfsbelang zwaarder dan het privacybelang van de werknemers?
- Meld heimelijk cameratoezicht vooraf bij de Autoriteit Persoonsgegevens.
- Vraag vooraf toestemming aan de OR.
- Informeer werknemers en personeel over gebruik van camera’s.
- Camerabeelden niet gebruiken voor functioneringsbeoordelingen.
- Inbreuk op privacy zo klein mogelijk houden.
- Gebruik van verborgen camera alleen in bijzondere omstandigheden, dus bij verdenking van fraude of diefstal.
- Permanent gebruik van verborgen camera is niet toegestaan.
- Informeer de betrokken werknemer(s) altijd achteraf over controle via verborgen camera.
- Deze stappen gelden ook voor monitoring van o.a. computers en emailverkeer.

Hoge boete voor schending privacy

Privacy schending ligt gevoelig zodra de baas zijn werknemer gaat bespieden wegens vermeend misbruik van bedrijfsmiddelen. Advocate Saskia van de Griek is kristalhelder: “Een werkgever moet de Autoriteit Persoonsgegevens vooraf informeren dat hij het mail- of internetverkeer van zijn werknemer heimelijk laat monitoren of een verborgen camera wil inzetten. Ook zal hij moeten uitleggen waarom een minder ingrijpende manier niet mogelijk is. De Autoriteit Persoonsgegevens (voorheen: College Bescherming Persoonsgegevens, red.) zal vervolgens de monitoring toetsen. Daarnaast dient de werkgever aan de Autoriteit duidelijk te maken hoe hij de beelden of andere data beveiligt zodat deze bijvoorbeeld niet kunnen weglekken naar derden. Onder de nieuwe Meldplicht datalekken sinds januari kan een boete oplopen tot 810.000 euro!”

Informatie- en meldplicht

Verder zijn werkgevers verplicht om hun personeel in te lichten over het monitoren van de bedrijfsmiddelen - computers, maar ook vervoersmiddelen - om te zien of ze bedrijfsmatig worden ingezet. “Dat is mogelijk via een personeelsreglement dat als aanhangsel dient van een arbeidsovereenkomst. Aanvullend kan een algemeen bericht aan het personeel worden gestuurd. Kortom:

Mr. Saskia van de Griek van advocatenkantoor Corporate Law: “Er komen veel vragen over de aangescherpte privacywetgeving.”

een werkgever kan niet lukraak in iemands mailbox gaan snuffelen, maar moet eerst voldoen aan de meld- en informatieplicht. Al deze waarborgen worden ook genoemd in de recente uitspraak van het Europese Hof voor de Rechten van de Mens, waar zoveel ophef over is de laatste tijd. Deze uitspraak geeft werkgevers dus niet ineens het recht om zonder meer te ‘snuffelen’ in email- of chatverkeer van werknemers”, aldus Van de Griek.

Van de Griek en Krabbe ervaren dat veel bedrijven niet op de hoogte zijn van dit soort richtlijnen en wettelijke regels. “Werkgevers denken over het algemeen te makkelijk over deze kwesties. Zo van: dit gebeurt mij niet. Totdat ze van een concullega horen wat hun is overkomen: weglekken van bedrijfsgevoelige informatie of hoge facturen moeten betalen. Daarna nemen ze maatregelen”, aldus Krabbe. Het is volgens hem van belang dat alle lopende en nieuwe arbeidscontracten worden aangepast aan het voorkomen van misbruik van bedrijfsmiddelen. “We zien regelmatig dat vooral de oude arbeidsovereenkomsten niets hierover bevatten, terwijl dit juist werknemers betreft die op cruciale functies zitten en vaak weinig ervaring hebben met het verantwoord omgaan met social media.”

Tips en aanbevelingen

- Stel een duidelijk protocol op dat privé misbruik van bedrijfsmiddelen niet is toegestaan en benoem de middelen: bijvoorbeeld e-mail en internet. Laat alle werknemers hiervoor tekenen.
- Monitor bedrijfsmiddelen op bedrijfsmatig gebruik en meld dit aan het personeel.
- Bouw een zorgvuldig dossier op bij vermoeden van misbruik en grijp tijdig in.