

Internet monitoren, wat mag er juridisch?

Vrijwel ieder bedrijf doet het, of overweegt het op zijn minst: het monitoren van het internetverkeer van medewerkers. Vaak worden bijvoorbeeld de websites bijgehouden die het personeel bezoekt, maar inspectie van hun mailboxen, laptops of e-mails en chatgesprekken is zeker ook mogelijk. Echter, op grond van de privacywet mag een werkgever niet zomaar privé-gebruik van internet volledig verbieden, laat staan zomaar controles uitoefenen op naleving van zo'n verbod. Op zijn minst dient de werkgever een protocol te hanteren waarin staat wat wel en niet mag en onder welke omstandigheden er gemonitord of geïnspecteerd kan worden.

Privacyregels op het werk

Werkgevers kunnen niet zomaar het internetgebruik van hun werknemers controleren. De privacy van de werknemer gaat onder normale omstandigheden boven het bedrijfsbelang bij monitoren of loggen van internetgebruik. Een werknemer mag een redelijk niveau van privacy verwachten op de werkplek en dus ook bij internetgebruik. Pas bij een redelijk vermoeden van wangedrag mag de werkgever gaan observeren of bijhouden wat individuele werknemers doen met de internetverbinding.

De vuistregel daarbij is dat monitoren en loggen zo veel mogelijk anoniem moet gebeuren. Pas als daarna wangedrag boven tafel komt, is het toegestaan uit te zoeken wie daar voor verantwoordelijk is. Wel moet de werkgever daarbij uitkijken dat andere werknemers niet onnodig ook gemonitord worden. Het monitoren en loggen van wat werknemers doen, valt namelijk onder de *Wet Bescherming Persoonsgegevens* ("de privacywet"). Op grond van deze wet moet elk monitoren een legitiem doel dienen en niet verder gaan dan absoluut noodzakelijk voor dat doel. Veel genoemde doelen zijn:

- Kosten: internetverkeer kost geld, en privégebruik van internet kan het bedrijf dus op hoge kosten jagen.
- Beveiligingsrisico's: een werknemer kan virussen downloaden of juist gevoelige bedrijfsgegevens verspreiden, bijvoorbeeld via filesharing.
- Public relations: het bedrijf kan worden aangekeken op wangedrag op een website vanaf een zakelijk IP-adres.
- Arbeidsconflicten: het downloaden of rondsturen van pornografie of racistisch beeldmateriaal kan de sfeer negatief beïnvloeden, net als iemand die zijn werk niet doet omdat hij de hele dag internetspelletjes speelt.

Een bedrijf met meer dan 50 medewerkers is wettelijk verplicht een ondernemingsraad (OR) in te stellen. Eén van de taken van die OR is toezien op de privacy van medewerkers. Omdat een internet/e-mailprotocol over privacygevoelige zaken gaat, is instemming van de OR verplicht bij het invoeren van zo'n protocol (art. 27 lid 1(k) en (l) van de Wet op de OR). Los daarvan moet het protocol natuurlijk altijd aan alle medewerkers beschikbaar worden gesteld.

Invoeren van een internetprotocol

Een werkgever moet werknemers informeren over hoe en wanneer er gemonitord wordt. Dit gebeurt meestal door invoering van een internetprotocol. Hierin worden algemene regels gegeven over wat wel en niet mag met de bedrijfspc, e-mail, internetverbinding en (mobiele) telefoon. Zo kan een protocol het verbieden om een abonnement te nemen op premium SMS-diensten, of voorschrijven dat in het buitenland een belkaart wordt gebruikt in plaats van de mobiele telefoon.

Een protocol mag privégebruik van ICT-faciliteren niet volledig verbieden, maar mag er wel (redelijke) grenzen aan stellen. Vaak wordt de formulering “mits dit niet storend is voor de dagelijkse werkzaamheden” gehanteerd. De situaties waarin de werkgever gericht mag kijken of deze grenzen worden overschreden, moeten expliciet worden genoemd. Zo kan meelezen van e-mail gerechtvaardigd zijn als er klachten komen over beledigende mails of reclamespam.

Verder moet het protocol aan iedereen bekend worden gemaakt. Uitreiken op papier of per e-mail is een goede mogelijkheid. Daarnaast bevelen wij aan deze op het intranet te publiceren en in het handboek voor medewerkers op te nemen.

Blokken en filteren van ongewenste inhoud

Een werkgever kan internetgebruik beperken, sites ontoegankelijk maken of het installeren van ongewenste software bemoeilijken. Dat is in principe toegestaan, en vanuit privacyoogpunt zelfs gewenst. Natuurlijk is zo'n blokkade te omzeilen. Door een proxy of een “anonymizer” te gebruiken, kan men sites bezoeken ondanks het filter. En door het administrator-wachtwoord te kraken, kun je software installeren terwijl dat niet de bedoeling was. Dergelijke handelingen zijn echter meestal illegaal. Bovendien kunnen ze in het bedrijfsreglement over internetgebruik verboden zijn. Wie een dergelijke regel overtreedt, hoeft bij de rechter op weinig sympathie te rekenen.

Doorzoeken van de bedrijfspc

Medewerkers kunnen ziek worden, op staande voet ontslag nemen of om andere redenen niet beschikbaar zijn. Omdat het werk door moet, is het dan vaak nodig toegang te krijgen tot zijn PC omdat alleen daar de benodigde bestanden te vinden zijn. Om de privacy van de werknemer te beschermen, is het aan te bevelen dat hierbij nooit één persoon het doorzoeken uitvoert, maar twee. Dit zouden bijvoorbeeld de beoogde ontvanger en de privacy officer van het bedrijf kunnen zijn, of de afdelingschef en een lid van de OR. Bij twee personen is de kans klein dat zij gaan snuffelen in evident niet relevante bestanden.

Een verbod op privégebruik van de bedrijfspc zal hier weinig aan helpen. Enig privégebruik is altijd te verwachten. Een werknemer die veel onderweg of in het buitenland is, kan en mag chats of mails met het thuisfront uitwisselen of vrijdagavond in de trein de nieuwsbrief van zijn sportclub afmaken. Omdat internet zo'n belangrijk deel van onze maatschappij is geworden, moet een werkgever dit soort privégebruik dan ook tolereren - binnen redelijke grenzen.

Bloggen of Hyven op het werk

Steeds meer mensen bloggen of gebruiken sociale netwerken zoals Hyves, LinkedIn, Myspace en Facebook. De meeste daarvan zijn puur voor privé: berichtjes uitwisselen met vrienden, foto's delen enzovoorts. Toch worden die sites vooral onder werktijd gebruikt.

Ook deze vorm van privégebruik van internet valt onder de al genoemde hoofdregel en is dus in principe toegestaan. Wel geldt er hier een extra regel: als men blogt, twittert of krabbelt over het werk, dan mag de werkgever eerder optreden. Zulke uitlatingen kunnen negatief uitstralen op het bedrijf of zaken onthullen die nog niet publiek mogen worden. Een goed internetprotocol bevat dan ook een paragraaf over de grenzen van bloggen, Hyven of Twitteren door werknemers.