# Rechtmatig operationeel handelen in ICT

## *Handreikingen voor HBO- en universitaire instellingen*

Bert-Jaap Koops, Colette Cuijpers, Paul de Hert (Universiteit van Tilburg, TILT - Centrum voor Recht, Technologie en Samenleving)

Versienummer 1.0, mei 2011

# Inhoudsopgave

# Afkortingen

| | |
|---|---|
| Awb | Algemene wet bestuursrecht |
| BW | Burgerlijk Wetboek |
| CBP | College Bescherming Persoonsgegevens |
| EHRM | Europees Hof voor de Rechten van de Mens |
| EVRM | Europees Verdrag voor de Rechten van de Mens |
| FIOD | Fiscale Inlichtingen- en Opsporingsdienst |
| HR | Hoge Raad |
| ICT | informatie- en communicatietechnologie |
| Ktr. | kantonrechter |
| NJ | Nederlandse Jurisprudentie |
| NMa | Nederlande Mededingingsautoriteit |
| OPTA | Onafhankelijke Post- en Telecommunicatie Autoriteit |
| Rb. | rechtbank |
| SIOD | Sociale Inlichtingen- en Opsporingsdienst |
| Wbp | Wet bescherming persoonsgegevens |
| WHW | Wet op het hoger onderwijs en wetenschappelijk onderzoek |
| Wiv 2002 | Wet op de inlichtingen- en veiligheidsdiensten 2002 |
| Wor | Wet op de ondernemingsraden |
| WvSr | Wetboek van Strafrecht |
| WvSv | Wetboek van Strafvordering |

# Samenvatting

Dit rapport brengt de juridische aspecten in kaart van rechtmatig operationeel handelen, dat wil zeggen handelingen met betrekking tot ICT-systemen, gegevens en communicatie, door (hoger)onderwijsinstellingen. Behandeld worden algemene rechten en plichten van ICT-medewerkers en gebruikers en de belangrijkste wet- en regelgeving, zoals de Wet bescherming persoonsgegevens. Vervolgens worden drie typen van operationeel handelen besproken vanuit het perspectief van een ICT-medewerker bij een (hoger)onderwijsinstelling: autorisatie- en systeembeheer, het loggen en monitoren van systemen, en het verstrekken van gegevens.

De onderwijsinstelling is verantwoordelijk voor het handelen van haar ICT-medewerkers en de omgang met persoonsgegevens. Voor de bevoegdheden en taakafbakening van ICT-medewerkers geldt vaak een reglement, bijvoorbeeld op basis van de model-integriteitscode van SURF. De belangrijkste – open – normen voor wat er mag en niet mag bij operationeel handelen zijn het goed werkgeverschap en het goed werknemerschap.

Werknemers en studenten mogen gebruik maken van ICT-faciliteiten van de onderwijsinstelling, ook enigermate voor privédoeleinden, waarbij zij kunnen verwachten dat hun privacy redelijkerwijs wordt beschermd. De onderwijsinstelling mag wel toezicht houden op het ICT-verkeer, maar gebruikers moeten weten waar ze aan toe zijn; daarom is het belangrijk dat de instelling een gedragscode ICT-gebruik heeft, waarin zowel de grenzen van gebruik als de vorm van toezicht door de instelling specifiek worden beschreven. Wanneer bij het operationeel handelen persoonsgegevens worden verwerkt – en dat zal snel het geval zijn – is de Wet bescherming persoonsgegevens van toepassing; dat mag alleen voor welomschreven doelen met een legitieme grondslag (zoals toestemming of een wettelijke plicht) en de verwerking moet zich tot het aangegeven doel beperken. Persoonsgegevens moeten ook adequaat worden beveiligd, en gebruikers hebben inzage- en correctierechten.

Voor specifieke vormen van rechtmatig operationeel handelen zijn de belangrijkste juridische voorwaarden als volgt:

1. *aanpassen van wachtwoorden*: dit moet vooral zorgvuldig gebeuren, verder zijn er geen juridische vereisten;

2. *afsluiten van een account of faciliteiten*: de voorwaarden en procedure hiervoor moeten kenbaar moeten zijn, bij voorkeur door opname van bepalingen in het arbeids- of onderwijscontract dan wel de gedragscode;

3. *beveiligen van (persoons)gegevens*: dit moet naar de stand van de techniek op basis van een afweging van de risico's en financiële kosten; ICT-medewerkers moeten geheimhouding betrachten als zij kennisnemen van persoonsgegevens;

4. *algemene controle op email- en Internetverkeer*: hierbij mag nooit kennis worden genomen van communicatie-inhoud (gesprekken, email); toestemming voor controlesystemen is nodig van de ondernemings- of medezeggenschapsraad; de controle moet proportioneel zijn; waar mogelijk moeten gegevens worden geanonimiseerd; de voorwaarden en procedure moeten vooraf kenbaar zijn voor alle gebruikers en dus goed vindbaar zijn op het intranet;

5. *specifieke controle op email- en Internetverkeer bij verdenking van misbruik*: hiervoor gelden dezelfde voorwaarden als bij algemene controle, zoals een proportionele en kenbare procedure, maar in principe mag er meer bij concrete, incidentele gevallen; inzage in de inhoud van gesprekken of email is toegestaan als dit strikt noodzakelijk is en het misbruik niet op een

andere manier kan worden bestreden;  ook privécommunicatie mag in zwaarwegende gevallen worden gecontroleerd; de sancties op misbruik moeten in de gedragscode zijn vermeld;

6. *verstrekken van gegevens aan collega's of leidinggevende*: het is raadzaam om regels over het verstrekken van persoonsgegevens aan derden, voor zover al niet geregeld in de arbeidsovereenkomst, vast te leggen in een gedragscode of privacyreglement; verder gelden de regels van de Wet bescherming persoonsgegevens: er is een legitieme grondslag nodig (toestemming van de medewerker, een contractuele verplichting of een zwaarwegend instellingsbelang) en de verstrekking moet nodig en proportioneel zijn; voor zakelijke belangen mogen in beginsel geen privégegevens, zoals persoonlijke mails of bestanden, worden verstrekt;

7. *verstrekken van gegevens aan familie*: op basis van de Wet bescherming persoonsgegevens zal dit zelden toegestaan zijn, tenzij de betrokkene toestemming heeft gegeven of is overleden, maar ook in die gevallen moet de instelling een zorgvuldige afweging maken;

8. *verstrekken van gegevens aan derden, zoals auteursrechtorganisaties*: dit is alleen toegestaan als de derde aantoonbaar een duidelijk belang heeft bij de gegevens, deze niet op andere wijze kan verkrijgen, en het belang van de derde zwaarder weegt dan dat van de gebruiker; bij gerede twijfel kan de instelling weigeren en afwachten of de derde via de rechter toegang tot de gegevens eist;

9. *verstrekken van gegevens aan politie en justitie*: bij een (schriftelijk) bevel tot verstrekking moet de instelling meewerken, waarbij alleen gelet kan worden op evidente fouten in het bevel, zoals het ontbreken van voldoende autorisatie (van een officier van justitie voor andere dan identificerende gegevens, en van de rechter-commissaris voor gevoelige gegevens);

10. *verstrekken van gegevens aan andere overheidsdiensten*: bijzondere opsporingsdiensten en toezichthouders hebben ruime bevoegdheden om inlichtingen en gegevens op te vragen, voor zover deze redelijkerwijs nodig zijn voor de uitoefening van hun taak, waarbij de instelling verplicht is mee te werken; inlichtingen- en veiligheidsdiensten kunnen alleen op vrijwillige basis gegevens opvragen.

# Inleiding

## Achtergrond en doelstelling

Dit rapport brengt de juridische aspecten in kaart van rechtmatig operationeel handelen door (hoger)onderwijsinstellingen. Onder **rechtmatig operationeel handelen** verstaan we in dit rapport:

> het in de praktijk uitvoeren van handelingen met betrekking tot het ICT-systeem van de organisatie, vooral de verwerking, opslag of transport van gegevens- en/of communicatie, zowel dagelijkse standaardhandelingen als bijzondere verrichtingen in uitzonderingssituaties.

Dit rapport beoogt op hoofdlijnen een overzicht te geven van relevante vragen en de juridische stand van zaken rond rechtmatig operationeel handelen in ICT door (hoger)onderwijsinstellingen. We hebben op basis van een kleine inventarisatie onder ICT-medewerkers van onderwijsinstellingen een keuze gemaakt voor de vormen van operationeel handelen in ICT die in juridisch opzicht het meest relevant zijn voor (hoger)onderwijsinstellingen. Voor die vormen brengen we in kaart wat welke wetgeving relevant is, wat de juridische voorwaarden en grenzen zijn voor deze vormen, en welke juridische aandachtspunten en mogelijke onduidelijkheden er spelen.

Het onderzoek voor dit rapport is uitgevoerd in de periode november 2010-maart 2011. De rapportage is afgerond op 2 mei 2011. Het onderzoek is vertrokken vanuit een inventarisatie van vormen van operationeel handelen en daarbij spelende vragen onder ICT-medewerkers van onderwijsinstellingen. Op basis van deze inventarisatie is literatuur-, wetgevings- en jurisprudentieonderzoek uitgevoerd om de meest relevante vragen te beantwoorden.

## Betrokken partijen

Dit rapport is geschreven door TILT in opdracht van SURFnet in afstemming met SURFdirect in het kader van het BIS!-programma (**B**eveiliging, **I**dentity Management, **S**ecurity Incident Management). Binnen dit programma worden de verschillende activiteiten van SURFfoundation en SURFnet op het gebied van Informatiemanagement en –beveiliging afgestemd.

### SURFfoundation

SURFfoundation initieert, regisseert en stimuleert ICT-vernieuwingen in het hoger onderwijs en onderzoek via kennisdeling, stimuleringsprogramma's en partnerschappen. SURFfoundation voert het management voor het BIS!-programma.

### SURFnet

SURFnet, motor voor ICT-innovatie, maakt samenwerking in het hoger onderwijs en onderzoek mogelijk. Via een geavanceerde netwerkinfrastructuur, SURFnet6, zijn 160 instellingen in hoger onderwijs en onderzoek met elkaar verbonden. Om veilig en efficiënt toegang te hebben tot allerlei diensten op dat netwerk, ontwikkelt SURFnet authenticatie- en autorisatiediensten. Voor het samenwerken over de grenzen van instellingen heen, biedt SURFnet innovatieve omgevingen waarbinnen docenten, onderzoekers en studenten data uitwisselen, online overleggen en mediabestanden delen. Bij al deze activiteiten staat beveiliging hoog in het vaandel. Door de pioniersrol ontwikkelt SURFnet continu kennis over en ervaring met nieuwe technologieën. SURFnet vindt het belangrijk deze kennis te delen met de internationale netwerkgemeenschap en de SURFnet gebruikers.

Binnen het expertisedomein ‘Collaboration Infrastructure’ wil SURFnet stimulerend optreden op het gebied van online applicaties en unified communications. Daarnaast werkt SURFnet aan een actieve community van gebruikers van online applicaties.

### SURFdirect

SURFdirect, de digitale rechten expertise community van SURF, identificeert de juridische aspecten die spelen bij diverse thema’s in e-learning en e-science. SURFdirect richt zich binnen de missie van SURF (innovatie, samenwerking en ICT) op het ondersteunen van het hoger onderwijs en onderzoek bij juridische kwesties rond toegang en hergebruik van tekst, beeld en geluid. Privacy is een van de gebieden waar SURFdirect haar kennis wil vergroten en wil publiceren ten behoeve van de doelgroep hoger onderwijs en onderzoek.

### TILT – Centrum voor Recht, Technologie en Samenleving, Universiteit van Tilburg

Het onderzoek is uitgevoerd door onderzoekers van het Centrum voor Recht, Technologie en Samenleving (TILT) van de Universiteit van Tilburg. TILT is een onderdeel van de rechtenfaculteit van de Universiteit van Tilburg. TILT heeft circa 25 onderzoekers en is een van de belangrijkste en meest ervaren Nederlandse onderzoek- en onderwijsinstituten op het gebied van regulering van technologie. Het specialisme van TILT bestrijkt een breed aantal onderwerpen rond ontwikkelingen in ICT, biotechnologie en andere technologieën. Deze ontwikkelingen worden bestudeerd in de context van de belangrijke domeinen in de kennismaatschappij, zoals e-overheid, e-handel, e-zorg, bio- en nanotechnologie, privacy, identiteitsmanagement, elektronische handtekeningen, biometrie, computercriminaliteit, veiligheid en intellectuele-eigendomrechten. Het onderzoek en onderwijs van TILT zijn gericht op de interactie tussen juridische, bestuurskundige en ethische expertise, tussen recht, regulering en bestuur, en tussen juridische, technische en maatschappelijke invalshoeken.

## Leeswijzer

Hoofdstuk 2 bevat een algemene uiteenzetting van de partijen betrokken bij operationeel handelen en de belangrijkste wet- en regelgeving die hierbij van belang is. Een korte bespreking van de betrokken partijen is van belang om de rolverdeling en algemene richtlijnen voor operationeel handelen te verduidelijken. Daarbij wordt ook de belangrijkste wet, de Wet bescherming persoonsgegevens, algemeen besproken.

Vervolgens behandelen we drie typen van operationeel handelen. Daarbij hanteren we het perspectief van een ICT-medewerker bij een (hoger)onderwijsinstelling. In hoofdstuk 3 wordt gekeken naar het autorisatie- en systeembeheer. Daarna wordt in hoofdstuk 4 het loggen en monitoren van systemen juridisch in kaart gebracht. Hierbij ligt de nadruk op het controleren of gebruikers de ICT-faciliteiten (on)rechtmatig gebruiken. Vervolgens wordt het juridische kader voor het verstrekken van gegevens aan derden behandeld, waaronder we ook verstaan – vanuit het perspectief van de ICT-medewerker – het verstrekken van gegevens van medewerkers aan collega’s of leidinggevenden. Een belangrijk onderscheid is of de gegevens worden verstrekt aan private partijen (hoofdstuk 5) of aan de overheid (hoofdstuk 6).

De wetgeving waarnaar dit rapport verwijst, is integraal en in de meest actuele versie te vinden op http://wetten.overheid.nl. Rechtspraak met een LJN-nummer is te vinden op http://www.rechtspraak.nl.

# Algemeen

## Algemene richtlijnen

Er bestaat een verschil tussen de onderwijsinstelling die opdracht geeft tot bepaald operationeel handelen, en de persoon die dit handelen daadwerkelijk uitvoert. Juridisch kan het onderscheid tussen de verantwoordelijke instelling en de handelende persoon (mede) bepalend zijn voor de rechtmatigheid van het handelen. Ook kan operationeel handelen zowel docenten en onderzoekers als studenten, gasten en tijdelijke medewerkers betreffen. De rechtsverhouding tussen de instelling en de medewerker (een arbeidsverhouding), die tussen instelling en student (dienstverlening) en die tussen instelling en gasten (geen directe rechtsverhouding) is anders, en ook deze onderliggende rechtsverhoudingen zijn van belang in het licht van de juridische kwalificatie van operationeel handelen.

### Wat mag de ICT-medewerker?

De ICT-medewerker heeft een arbeidsrelatie met de onderwijsinstelling. Wanneer de ICT-medewerker handelt als een goed werknemer, voert zij de taken uit die zij krijgt opgedragen vanuit de onderwijsinstelling en gaat zij niet verder dan haar bevoegdheden strekken. De handelingen die de ICT-medewerker verricht, verricht zij onder gezag van de onderwijsinstelling; er is sprake van een hiërarchische relatie. Voor zover schade veroorzaakt door de ICT-medewerker niet een gevolg is van haar opzet of bewuste roekeloosheid, is de werkgever (de onderwijsinstelling) op grond van artikel 6:170 BW aansprakelijk:

> Voor schade, aan een derde toegebracht door een fout van een ondergeschikte, is degene in wiens dienst de ondergeschikte zijn taak vervult aansprakelijk, indien de kans op de fout door de opdracht tot het verrichten van deze taak is vergroot en degene in wiens dienst hij stond, uit hoofde van hun desbetreffende rechtsbetrekking zeggenschap had over de gedragingen waarin de fout was gelegen.

Ook in het kader van de Wet bescherming persoonsgegevens (Wbp) geldt dat de onderwijsinstelling verantwoordelijk is voor de verwerking van persoonsgegevens, voor zover de ICT-medewerker verwerkingen uitvoert onder gezag van of in een hiërarchische verhouding tot de instelling. Dit wordt intern beheer genoemd. Alleen wanneer de ICT-medewerker op eigen gelegenheid persoonsgegevens verwerkt, waarbij zij zelf doel en middelen van de verwerking van persoonsgegevens vaststelt, is zij als verantwoordelijke in de zin van de Wbp aan te merken. De verplichtingen van de Wbp (zie onder, Wet bescherming persoonsgegevens) gelden dus voor de instelling in wiens naam de ICT-medewerker in haar taakuitoefening handelt, of voor de medewerker zelf als zij op eigen gezag doel en middelen van de verwerking van gegevens vaststelt; dat laatste zal vaak alleen gelden voor zaken die niet de functie van de medewerker betreffen (zoals het organiseren van een zaalvoetbaltoernooi voor collega's).

Voor de bevoegdheden en de grenzen van de uitoefening van de functie van ICT-medewerkers geldt vaak een reglement, waarin in aanvulling op het algemene recht – en vaak ter invulling van de meer abstracte grenzen van het recht – bepaald wordt wat de medewerker onder welke omstandigheden mag doen. SURF heeft een goed bruikbare model-integriteitscode ontwikkeld.[1] Een voorbeeld van een uitgewerkt reglement is de *Integriteitscode ICT-personeel* van de Universiteit van Tilburg (opvraagbaar bij de auteurs).

---

[1] SurfIBO, Leidraad Integriteitcode, juni 2010, beschikbaar op http://www.surffoundation.nl/nl/publicaties/Documents/SurfIBO%20Leidraad%20integriteitcode%20definitief.pdf.

## Wat mag de werkgever?

De gezagsverhouding tussen de werkgever en de werknemer beperkt de handelingsvrijheid van de werknemer. De werkgever mag instructies geven en maatregelen nemen ter bevordering van de goede werking van de onderneming (art. 7: 660 BW). Hierbij geldt evenwel dat de werkgever zich dient te gedragen als een goed werkgever (art. 7:611 BW).[2] Wanneer de werkgever gegevens over zijn werknemers verwerkt, is hij gehouden aan de bepalingen die zijn neergelegd in de Wbp, wat erop neerkomt dat er een legitieme verwerkingsgrond aanwezig moet zijn, er sprake moet zijn van doelbinding, proportionaliteit en subsidiariteit. De werkgever moet aantonen waarom gegevens worden verzameld en opgeslagen, dat de gegevens relevant zijn voor het beoogde doel en dat er geen andere minder ingrijpende mogelijkheid is om dat doel te bereiken. Inzage in en het verstrekken van gegevens kan dus zijn toegestaan, voor zover dit geschiedt in overeenstemming met de geldende wet- en regelgeving, met name de Wet bescherming persoonsgegevens (zie onder, Wet bescherming persoonsgegevens).

Deze uitleg van het goed werkgeverschap impliceert dat in uitzonderlijke omstandigheden controle op (de inhoud van) communicatie gerechtvaardigd is (zie verder hfd. 4). Permanente controle is echter alleen bij hoge uitzondering toegestaan (Hof 's-Hertogenbosch 2 juli 1986, NJ 1987, 451, *Koma*). Dit arrest had weliswaar betrekking op cameratoezicht, maar is in het algemeen van belang voor de toelaatbaarheid van controlesystemen.

## Wat mag de werknemer of de student?

In het kader van dit rapport wordt uitgegaan van de situatie dat een medewerker of student in het kader van haar werk respectievelijk studie, de ICT-systemen gebruikt van de onderwijsinstelling. De werknemers en studenten duiden we in het rapport ook wel kortheidshalve aan als gebruikers.

Voor werknemers gelden specifieke bepalingen die voortvloeien uit de arbeidsrelatie, maar ook uit het recht. In de wet is vastgelegd dat werknemers zich moeten gedragen als goed werknemer (art. 7: 611 BW). Daarnaast, of wanneer er geen arbeidsrelatie is, bijvoorbeeld omdat de gebruiker een studentgebruiker is, geldt de algemene bepaling van art. 6:162 BW over de onrechtmatige daad. Uit dit artikel volgt de algemene norm dat men moet handelen volgens de wet en volgens 'hetgeen in het maatschappelijke verkeer betaamt', ofwel een plicht tot zorgvuldig handelen naar de maatstaven van wat in de situatie gebruikelijk en gepast is.

Naast de plicht tot zorgvuldig handelen, gelden voor gebruikers ook rechten, zoals het recht op privacy en het recht op communicatievrijheid. Controle op email raakt het communicatiegeheim (art. 13 Grondwet). Hoewel er discussie is over de vraag of artikel 13 van de Grondwet ook email omvat, aangezien deze Nederlandse grondrechtelijke bepaling strikt genomen alleen het brief-, telefoon- en telegraafgeheim beschermt, erkent rechtspraak soms wel de toepassing van de Grondwet op email (Ktr. Utrecht 16 september 1998; Rb. Rotterdam 29 maart 2001). Sowieso is artikel 8 EVRM, dat de privacy beschermt, van toepassing op 'correspondentie', wat heel ruim wordt geïnterpreteerd om alle vormen van communicatie te beschermen. Een werkgever kan wel bepalen dat email en telefoon hoofdzakelijk voor werkdoeleinden mogen worden gebruikt, maar hij mag niet volledig alle niet-zakelijke communicatie verbieden (Ktr. Amsterdam 26 april 2001). Ook mag de werkgever niet compleet Internetgebruik afsluiten; het recht op informatievergaring van art. 10 EVRM bepaalt dat enige toegang tot externe informatiekanalen voor werknemers/studenten mogelijk moet zijn.

---

[2] Zie algemeen Mark Diebels e.a., *Goed werkgeverschap. Handvatten voor redelijkheid*, Alphen aan den Rijn: Kluwer 2006.

Dat het recht op privacy in het Europees Verdrag voor de Rechten van de Mens (EVRM) zich ook uitstrekt tot de werkvloer blijkt uitdrukkelijk uit Europese jurisprudentie. Werknemers hebben een zekere mate van privacy op de werkplek en ook de zakelijke correspondentie is tot op zekere hoogte beschermd (EHRM 16 december 1992, NJ 1993, 400; zie ook EHRM 25 juni 1997, NJ 1998, 506, *Halford*). Hoewel artikel 8 EVRM geen melding maakt van telefoongesprekken, heeft het EHRM beslist dat het telefoonverkeer ook onder de bescherming van het privéleven en de correspondentie valt (EHRM 6 september 1976, *Klass*). Ondertussen kan ook het emailverkeer en Internetgebruik op de werkplaats bescherming genieten van artikel 8 EVRM (EHRM 3 april 2007, *Copland*). In dit arrest werd gezegd dat, indien de werknemer een bepaalde vrijheid inzake privégebruik van de bedrijfsmiddelen geniet, hij een redelijke verwachting heeft dat hij die beperkte vrijheid onbelemmerd kan uitoefenen.

De Europese rechtspraak hecht veel belang aan voorzienbaarheid en kenbaarheid van controlemaatregelen. In *Halford* had een werkneemster een redelijke privacyverwachting omdat zij niet gewaarschuwd was dat gesprekken werden opgenomen (EHRM 25 juni 1997, NJ 1998, 506, *Halford*).

Voor studenten gelden grotendeels dezelfde richtlijnen, met dien verstande dat de rechten van de studenten en de plichten van de onderwijsinstelling hier niet voortvloeien uit het goed werkgever/werknemerschap maar uit de eisen die aan een goed dienstverlener/dienstafnemer in het maatschappelijk verkeer worden gesteld.

Samenvattend: uit de wetgeving en de jurisprudentie blijkt dat werknemers en studenten gebruik mogen maken van faciliteiten van de onderwijsinstelling, waarbij geldt dat dit gebruik in beginsel privacybescherming geniet, zeker als er geen expliciete afspraken zijn gemaakt of waarschuwingen zijn gegeven die de redelijke privacyverwachting ondermijnen.

## Wat mag de tijdelijke of incidentele gebruiker?

### *lkj;lkjj*

Naast werknemers en studenten maken ook anderen gebruik van ICT-faciliteiten. Wanneer deze derden een min of meer vergelijkbare juridische relatie hebben als werknemers of studenten – bijvoorbeeld inhuurkrachten of contractstudent met wie ook een overeenkomst is afgesloten – gelden daarvoor dezelfde richtlijnen als onder het vorige kopje behandeld. Het is dan wel belangrijk dat de overeenkomst verwijst naar geldende voorschriften en gedragscodes, en dat omgekeerd de op de instelling geldende reglementen en gedragscodes ook een clausule bevatten die aangeven dat de regels voor ICT-gebruik ook voor dit type tijdelijke of incidentele medewerkers of studenten gelden.

Maar er zijn ook tijdelijke of incidentele gebruikers met wie er geen contractuele relatie bestaat, zoals een gastdocent die een gastcollege verzorgt, een gastonderzoeker die twee weken lang een bureau bij een onderzoeksgroep heeft, of congresbezoekers die via WiFi in de congreszaal van Internet gebruik maken. Maakt dat verschil voor hun gebruiksrechten vanuit juridisch oogpunt?

Over dit onderwerp bestaat nauwelijks jurisprudentie. Hoewel het goed werkgeverschap en goed werknemerschap hier niet opgaan, lijkt ons dat over het algemeen dezelfde normen zullen gelden voor incidentele gebruikers als voor vaste gebruikers, op basis van de algemene norm van art. 6:162 BW (onrechtmatige daad, die een algemene norm stelt van wat in het maatschappelijk verkeer betaamt). Alleen als er uit de aard van het ICT-gebruik relevante verschillen zijn, zal een verschil in behandeling gerechtvaardigd zijn. Bijvoorbeeld als gastonderzoekers een algemene computer delen met een gezamenlijk gastaccount, dan is wellicht een zwaardere vorm van monitoren van internetverkeer of het blokkeren van bepaalde faciliteiten toegestaan die bij vaste

medewerkers niet proportioneel zou zijn. Maar meestal zal er niet zoveel verschil bestaan in het operationeel handelen tussen incidentele en reguliere gebruikers.

Een belangrijk punt van aandacht is wel de kenbaarheid van geldende regels en gedragscodes voor tijdelijke en incidentele gebruikers. Het moet kenbaar zijn voor de gebruikers wat zij wel en niet mogen doen (zie ook het volgende kopje over privégebruik van faciliteiten) en ook of en hoe de instelling het ICT-gebruik monitort (zie hfd. 4). Als het beleid aan de vaste gebruikers kenbaar wordt gemaakt bij indiensttreding of het begin van de studie en via een verwijzing op de webpagina (het intranet) van de instelling, dan zal dit veelal langs gastdocenten, gastonderzoekers en congresbezoekers heen gaan. Zij moeten dan op een andere manier op het beleid worden gewezen, bijvoorbeeld door bij het begin van hun bezoek of in de congresmap een informatievel aan te bieden waarin staat dat de gasten gebruik mogen maken van de aangeboden ICT-faciliteiten en dat daarop de gedragscode van toepassing is, die is bijgevoegd of die te vinden is op de URL www.instelling.nl/regelingen/ICT-gedragscode. Daarnaast moet dan ook in de gedragscode worden vermeld dat de regeling ook van toepassing is op incidentele gebruikers. Als er ook buitenlandse gasten op de instelling komen, dan is het natuurlijk raadzaam – en er regelmatig buitenlandse bezoekers komen noodzakelijk – om het informatievel en de gedragscode ook in het Engels aan te bieden.

Aangezien er volgens ons, buiten de kenbaarheid, weinig relevante verschillen zijn tussen reguliere en tijdelijke gebruikers, zullen we in dit rapport verder uitgaan van de reguliere gebruikers, oftewel medewerkers en studenten.

## Privégebruik van werkfaciliteiten

Als het privégebruik van door de onderwijsinstelling ter beschikking gestelde middelen wordt gedoogd, mag de werknemer of de student een redelijke privacybeleving veronderstellen (EHRM 25 juni 1997, NJ 1998, 506, *Halford*). In elk geval moet de werkgever een zekere mate van het gebruik van ICT-faciliteiten voor privégebruik aanvaarden (Ktr. Amsterdam 26 april 2001). Maar de werknemer moet wel beseffen dat buitensporig privégebruik niet wordt getolereerd (Ktr. Emmen 29 november 2000). Aan de andere kant mag het privégebruik ook niet louter afhankelijk worden gemaakt van de voorafgaande en arbitraire beslissing van een leidinggevend persoon (Registratiekamer 27 december 1999). Met andere woorden: de werkgever mag zeker grenzen stellen aan privégebruik, maar dat moet kenbaar zijn en de grenzen mogen niet willekeurig door verschillende leidinggevenden op de werkvloer worden bepaald – er moet dus een helder instellingsbeleid zijn. Dat gebeurt bij voorkeur in de vorm van een gedragscode waarin wordt bepaald hoe medewerkers en studenten de ICT-faciliteiten mogen gebruiken en hoe de werkgever daarop toezicht uitoefent.[3]

Aan de aanwezigheid van een gedragscode lijkt in de Nederlandse rechtspraak steeds meer gewicht te worden toegekend. Maar een duidelijke afgetekende lijn is er niet. In sommige rechterlijke uitspraken heeft de afwezigheid van een privacybeleid geen of weinig invloed gehad op de uitspraak (Ktr. Haarlem 26 juni 2000; Ktr. Utrecht 20 november 2000; Ktr Apeldoorn 6 september 2000; Rb Rotterdam 29 maart 2001). Andere rechtspraak kent wel gewicht toe aan het bestaan van een gedragscode (Ktr. Utrecht 13 juli 2000; Ktr. Sittard 21 december 2001; Ktr. 's-Gravenhage 3 oktober 2002). Bovendien kan de aanwezigheid van een gedragscode niet bepalen

[3] SurfIBO heeft een handleiding voor het opstellen van een gedragscode gemaakt: *Leidraad voor het opstellen van een Acceptable Use Policy*, november 2005 beschikbaar op http://www.surffoundation.nl/nl/publicaties/Documents/SURF-IBO%20Leidraad%20voor%20het%20opstellen%20van%20een%20acceptable%20use%20policy%20definitief.pdf. Zie verder hfd. 4 onder 'Algemeen' voor meer voorbeelden van gedragscodes.

dat een werknemer geen enkele vorm van privécommunicatie mag voeren (Ktr. Amsterdam 26 april 2001). Volgens Europese rechtspraak moet de medewerker of student haar handelen kunnen afstemmen op vooraf kenbare regels. Hierbij is het volgens diezelfde rechtspraak niet voldoende dat de werknemer bekend is met de *mogelijkheid* van de controle; volgens *Halford* is daarnaast ook een voorafgaande waarschuwing nodig. In de nationale rechtspraak bestaat hierover echter geen volledige duidelijkheid. Al lijkt er een tendens aanwezig dat het kenbaarheidsprincipe gestaag veld wint.

## Wet bescherming persoonsgegevens (Wbp)

Omdat er bij rechtmatig operationeel handelen, voor zover het raakt aan juridische vraagstukken, bijna altijd persoonsgegevens (van werknemers of studenten) in het spel zijn, is de Wet bescherming persoonsgegevens (Wbp) van bijzonder belang. Bij de inzage, het verstrekken, het loggen en het monitoren van communicatie, gaat het in essentie allemaal om de verwerking van persoonsgegevens. Daarom behandelen we hier in het algemeen het juridisch kader dat de Wbp geeft voor het verwerken van persoonsgegevens. De Wbp vormt een uitwerking van één van de dimensies van het overkoepelende grondrecht op privacy, namelijk de informationele privacy, ofwel het recht op bescherming van persoonsgegevens. Op basis van de Wbp is de verwerking van persoonsgegevens alleen toegestaan wanneer dit op een behoorlijke en zorgvuldige wijze gebeurt. Wat behoorlijk en zorgvuldige gegevensverwerking is volgt uit de rechten en plichten vastgelegd in de Wbp.

De naleving van de regels van deze wet staat onder toezicht van het College Bescherming Persoonsgegevens. Bij twijfel over de interpretatie of toepassing van deze wet kan dan ook contact worden opgenomen met het CBP. Ook biedt de webpagina van het CBP tal van adviezen en voorbeelden van hoe de wet in bepaalde situaties moet worden uitgelegd.[4]

### Gelaagd systeem

De Wet bescherming persoonsgegevens is een algemene regeling die de minimumvoorwaarden voor het verwerken van persoonsgegevens bevat. De Wbp vormt de implementatie van Europees recht. Artikel 7 van het Handvest van de Grondrechten van de EU betreft een algemene omschrijving van het recht op gegevensbescherming, welk recht nader is uitgewerkt in verschillende Richtlijnen. Deze richtlijnen zijn Richtlijn 95/46/EG welke de algemene richtlijn betreffende gegevensverwerking is, Richtlijn 2002/58 EG betreffende de verwerking van persoonsgegevens in de elektronische communicatie sector, en Richtlijn 2006/24/EG betreffende het bewaren van gegevens. Voor deze studie is de algemene richtlijn, welke in Nederland is omgezet in de Wbp, het meest van belang. De richtlijnen zijn onderdeel van een gelaagd systeem van gegevensbescherming dat in de EU tot stand is gebracht. De eerste drie lagen van dit systeem zijn opgenomen in Richtlijn 95/46/EG, en omgezet in de Wbp:

1. algemene regels voor de rechtmatigheid van de verwerking van persoonsgegevens;
2. regels voor de verwerking van bijzondere (gevoelige) gegevens;
3. regels betreffende de doorgifte van gegevens naar derde landen (landen buiten de EU).

Daarnaast zijn de volgende twee lagen van belang: http://www.janm.nl

1. sectorspecifieke wet- en regelgeving (o.a. Richtlijn 202/58 en 2006/24, maar bijvoorbeeld ook in Nederland de Wet geneeskundige behandelingsovereenkomst met daarin bijzondere

[4] http://www.cbpweb.nl/.

bepalingen betreffende verwerking van persoonsgegevens in een medische behandelingsrelatie);

2. onderliggende (contractuele) rechtsverhoudingen.

Er wordt gesproken van een gelaagd systeem omdat de verschillende lagen van regels elkaar cumulatief aanvullen. Dit houdt in dat de eerste laag altijd van toepassing is indien persoonsgegevens worden verwerkt en geen van de in de Wbp opgenomen uitzonderingen van toepassing is. Indien bijzondere persoonsgegevens (zoals gegevens over etnische afkomst of lidmaatschap van een vakbond) verwerkt worden, dan zijn zowel de bepalingen uit de eerste laag, als die uit de tweede laag van toepassing. Als deze bijzondere gegevens vervolgens ook nog doorgegeven worden aan een derde land, dan is bovendien ook nog laag 3 van toepassing.

Per geval moet beoordeeld worden of naast de in de Wbp opgenomen regels tevens sectorspecifieke wetgeving van toepassing is en of er wellicht binnen de rechtsverhouding contractuele afspraken zijn gemaakt die van invloed zijn op de wijze waarop gegevens al dan niet rechtmatig verwerkt mogen worden. Voor onderwijsinstellingen en hun medewerkers en studenten kan in dit verband niet alleen gewezen worden op arbeidscontracten en contracten tussen de onderwijsinstelling en de studenten, maar bijvoorbeeld ook op geldende gedragscodes en privacypolicies, die, al dan niet expliciet, onderdeel uit kunnen maken van de contractuele relatie.

## Verwerking en persoonsgegeven

Bij de vraag of de Wbp van toepassing is staan de begrippen persoonsgegeven en verwerking centraal. De Wbp regelt immers onder welke voorwaarden persoonsgegevens mogen worden verwerkt en wat daarbij de regels zijn. De definitie van 'persoonsgegeven' en 'verwerking van persoonsgegevens' is te vinden in artikel1 sub a en b van de Wbp:

a. persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;

b. verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Het begrip 'verwerking' wordt ruim uitgelegd en omvat alles van het aanmaken tot het vernietigen van gegevens. Ook het begrip persoonsgegeven wordt zeer ruim uitgelegd, maar daarover bestaat wel de nodige discussie.[5] De artikel 29 Werkgroep[6] heeft het begrip verduidelijkt en aangegeven dat het uit vier elementen bestaat, te weten:

- "iedere informatie" (of, zoals opgenomen in de Wbp, 'elk gegeven')
- "betreffende"

---

[5] Zie Groep gegevensbescherming artikel 29 (2007) *Advies 4/2007 over het begrip persoonsgegeven*. 01248/07/NL, WP 136. Toegankelijk via: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_nl.pdf. De Richtlijn 95/46/EG wordt momenteel herzien; in dat kader staat ook de uitleg van het begrip persoonsgegeven ter discussie.

[6] De artikel 29 Werkgroep is in het leven geroepen door artikel 29 van de Richtlijn bescherming persoonsgegevens (95/46/EG). De groep heeft als taak het adviseren van de Europese Commissie over de uniforme toepassing en interpretatie van de Richtlijn, en in het algemeen over het niveau van databescherming binnen de Europese Unie. Zie ook artikel 30 van de Richtlijn.

- “geïdentificeerd of identificeerbaar”
- “natuurlijke persoon”.

Identificatie kan direct en indirect plaatsvinden, met name met betrekking tot de indirecte identificatie heersen meningsverschillen betreffende de interpretatie. Bekend is de discussie omtrent IP-adressen, het is immers sterk van de context afhankelijk of IP-adressen leiden tot identificatie. IP-adressen die zijn toegewezen aan computers in een internetcafé waar geen legitimatie wordt verlangd zullen niet leiden tot identificatie, terwijl IP-adressen van consumenten die via een reguliere ISP worden verstrekt in veel gevallen wel ter herleiden zijn tot natuurlijke personen, en dus wel persoonsgegevens zijn. Aan de hand van de door de ISP bijgehouden verkeersgegevens is immers vast te stellen wie gebruik heeft gemaakt van het betreffende IP-adres op een bepaald tijdstip. In onderwijsinstellingen zullen in de regel IP-adressen te herleiden zijn tot medewerkers en studenten, en zijn dus te kwalificeren als persoonsgegevens in de zin van de Wbp. Hetzelfde geldt voor gegevens betreffende het gebruik van email en internet.

Hoewel de eerste vier artikelen betreffende het toepassingsgebied van de Wbp vragen kunnen oproepen omdat de toepasselijkheid van de Wbp gekoppeld is aan de vestigingsplaats van de verantwoordelijke, wat bij multinationale bedrijven tot erg complexe situaties kan leiden, is deze discussie voor het onderhavige rapport weinig relevant en wordt ervan uitgegaan dat het gaat om Nederlandse onderwijsinstellingen, gevestigd in Nederland, waarop de Wbp in beginsel van toepassing is.[7]

## Verantwoordelijke en bewerker

De verplichtingen in de Wbp gelden ten aanzien van de verantwoordelijke, in artikel 1 d van de Wbp gedefinieerd als:

> "de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt".

De verantwoordelijke kan een andere persoon inschakelen de gegevens daadwerkelijk te verwerken, er wordt dan gesproken van ´bewerken´. Artikel 1 e van de Wbp definieert ´bewerker´ als:

> "degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen." [8]

Het verschil hiertussen is dat de bewerker niet de doelen en middelen voor de verwerking van persoonsgegevens bepaalt, maar slechts in opdracht van de verantwoordelijke persoonsgegevens verwerkt.

Degene op wie een persoonsgegeven betrekking heeft, wordt ´betrokkene´ genoemd. In de Wbp is de relatie tussen verantwoordelijke, bewerker en derden nader toegelicht in artikel 12 dat bepaalt:

---

[7] Andere uitzonderingen betreffende toepasselijkheid van de Wbp zijn te vinden in artikel 2 en 3 Wbp, onder andere gebruik van puur huishoudelijke aard, voor uitsluitend journalistieke, artistieke of literaire doeleinden en het kader van bepaalde wetten zoals de Wet gemeentelijke basisadministratie persoonsgegevens, Wet justitiële en strafvorderlijke gegevens en de Kieswet. Bespreking blijft buiten beschouwing bij gebrek aan relevantie in het kader van dit rapport.

[8] Zoals eerder opgemerkt wordt gesproken van intern beheer indien de persoon die de verwerking uitvoert onder gezag van of in een hiërarchische verhouding tot de verantwoordelijke staat.

> "Een ieder die handelt onder het gezag van de verantwoordelijke of van de bewerker, alsmede de bewerker zelf, voor zover deze toegang hebben tot persoonsgegevens, verwerkt deze slechts in opdracht van de verantwoordelijke, behoudens afwijkende wettelijke verplichtingen."

Voor deze personen geldt een plicht tot geheimhouding van de gegevens waarvan zij kennis nemen, behalve wanneer een wettelijk voorschrift hen tot mededeling verplicht of het voor de uitoefening van hun taak noodzakelijk is om gegevens mee te delen.

## Algemene bepalingen

Het centrale artikel van de Wbp is artikel 6 dat bepaalt dat persoonsgegevens worden verwerkt in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze. De artikelen die volgen geven inhoud aan het begrippenpaar 'behoorlijke en zorgvuldig', want de verwerking van persoonsgegevens is pas behoorlijk en zorgvuldig als deze verwerking in overeenstemming is met de bepalingen uit de Wbp.

In de eerste plaats mogen persoonsgegevens alleen verzameld worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (Art. 7). Onderwijsinstellingen doen er verstandig aan de inzage in gegevens, het verstrekken van gegevens en het monitoren van gegevens uitdrukkelijk als doeleinden te beschrijven. Hierbij geldt dat de doelen expliciet, compleet en duidelijk beschreven moeten worden. Voor zover de verwerking van persoonsgegevens wordt uitbesteed aan een bewerker, zal de doelomschrijving in de overeenkomst tussen verantwoordelijke en bewerker opgenomen moeten worden. De verantwoordelijke moet niet alleen zorg dragen voor een deugdelijke vaststelling van het doel, maar zal tevens moeten garanderen dat gegevens niet worden verwerkt op een wijze die onverenigbaar is met de vastgestelde doeleinden (Art. 9). Ook bepaalt artikel 9 dat verwerking niet is toegestaan in geval van geheimhoudingsplichten op basis van ambt, beroep (bijv. arts) of wettelijk voorschrift. In het licht van onderwijsinstellingen kan deze bepaling relevant zijn omdat er bij bepaalde functies binnen het onderwijs sprake kan zijn van een geheimhoudingsplicht, dit is echter niet waarschijnlijk met betrekking tot systeembeheerders, maar meer met betrekking tot vertrouwenspersonen. Bij inzage, verstrekken en monitoren van gegevens van personen binnen de instelling met een dergelijke bijzondere positie, moeten dus mogelijk extra waarborgen in acht worden genomen.

Een tweede belangrijke voorwaarde voor de verwerking van persoonsgegevens is de aanwezigheid van een legitieme verwerkingsgrond. De mogelijke gronden voor verwerking zijn limitatief opgesomd in artikel 8 Wbp. De eerste rechtmatige verwerkingsgrond om gegevens te mogen verwerken (artikel 8 a Wbp) is 'toestemming van betrokkenen'. De Wbp definieert het begrip 'toestemming' in artikel 1 sub i als volgt: 'elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt'. Het vragen van toestemming heeft als nadeel dat het omslachtig is, omdat hiervan een registratie aangelegd moeten worden. Deze registratie is noodzakelijk omdat de verwerker moet kunnen aantonen dat hij toestemming heeft en omdat de toestemming altijd ingetrokken mag worden. Dit betekent voor de verantwoordelijke een administratieve last. Bovendien is de verwerkingsgrond toestemming in de parlementaire geschiedenis uitgelegd als betekenend dat wanneer toestemming eenmaal geweigerd of ingetrokken is, gegevens niet meer op een van de andere verwerkingsgronden (zie hieronder) gestoeld mogen worden.

De inzage, verstrekking en het monitoren van gegevens kan onderdeel uitmaken van verwerkingsgrond b):

> "de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst."

Andere mogelijke verwerkingsgronden zijn de nakoming van een wettelijke verplichting, het vitaal belang van de betrokkene (dat wil zeggen levensbedreigende situaties) en de vervulling van een publiekrechtelijke taak door een bestuursorgaan. Als restgrond wordt artikel 8 onder f beschouwd, dat bepaalt dat gegevens verwerkt mogen worden als de gegevensverwerking noodzakelijk is om het gerechtvaardigde belang van de verantwoordelijke of van een derde te behartigen, tenzij het privacybelang van de betrokkene zwaarder weegt. Het gaat hier dus om een belangenafweging tussen het belang van verwerking tegenover het privacybelang van de betrokkene.

Vervolgens stelt de Wbp eisen aan de kwaliteit van gegevens. Zo moeten gegevens toereikend, ter zake dienend, niet bovenmatig, juist en nauwkeurig zijn met het oog op de doeleinden waarvoor zij worden verzameld of waarvoor zij vervolgens worden verwerkt. Zolang ze identificeerbaar zijn, mogen gegevens niet langer worden bewaard dan nodig is voor het doel waarvoor ze verzameld zijn (Art. 10). Op grond van artikel 13 Wbp moeten gegevens deugdelijk beveiligd worden. Indien een bewerker wordt ingeschakeld, moet de verantwoordelijke zorg dragen dat deze voldoende waarborgen biedt qua technische en organisatorische beveiligingsmaatregelen voor de te verrichten verwerkingen.

Een andere belangrijke plicht voor verantwoordelijken betreft het verstrekken van informatie (33 en 34 Wbp). De verantwoordelijke moet de betrokkene informeren over zijn identiteit en de doeleinden van de verwerking waarvoor de gegevens zijn bestemd, alsmede nadere informatie verstrekken voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen. In uitzonderlijke gevallen geldt bovendien de plicht om de verwerking van persoonsgegevens te melden bij de bevoegde nationale toezichthoudende autoriteit, in Nederland het College Bescherming Persoonsgegevens (CBP) (Hoofdstuk 4 Wbp).

De Wbp bevat naast plichten voor verantwoordelijken ook rechten voor betrokkenen (de gebruikers). De belangrijkste rechten zijn het recht op toegang tot de eigen gegevens, een recht om gegevens te rectificeren, te wissen, af te schermen en het recht zich te verzetten tegen de verwerking van persoonsgegevens.

Tot slot is het met het oog op onderwijsinstellingen van belang te wijzen op artikel 5 van de Wbp betreffende minderjarigheid. Wanneer persoonsgegevens verwerkt worden van betrokkenen beneden de zestien jaar, is daarvoor steeds in plaats van toestemming van de betrokkene, toestemming van de wettelijk vertegenwoordiger (ouder of voogd) vereist (Art. 5 Wbp). Dit geldt ook wanneer de betrokkene onder curatele is gesteld of voor de betrokkene een juridisch mentorschap is ingesteld. Daarbij kan toestemming door de betrokkene of zijn wettelijk vertegenwoordiger te allen tijde worden ingetrokken.

## Bijzondere gegevens en doorgifte naar derde landen

Bij de in dit rapport besproken materie zal het zelden gaan om de doorgifte van persoonsgegevens naar derde landen. De derde laag in het systeem van gegevensverweking blijft in dit rapport dan ook buiten beschouwing (zie daarvoor de verwijzingen in de volgende paragraaf, Cloud-computing en toepasselijk recht). Voor die gevallen waarin toch gegevens worden doorgegeven naar landen buiten de EU, wijzen wij hier op artikelen 75-77 Wbp, die gelden als het desbetreffende land geen passend beschermingsniveau heeft, dat wil zeggen vergelijkbaar met het EU-systeem.[9]

[9] Zie voor een uitgebreide beschrijving van deze derde laag van gegevensverwerking over doorgifte naar derde landen het voor SURF geschreven rapport Colette Cuijpers e.a. (2011), *De wolk in het onderwijs. Privacy aspecten bij cloud computing services*, Tilburg: TILT, beschikbaar op

Wat wel aan de orde kan zijn bij monitoring, het inzien van gegevens en het verstrekken van gegevens is dat er zogeheten 'bijzondere persoonsgegevens' worden verwerkt. Bijzondere persoonsgegevens, ook wel gevoelige gegevens genoemd, zijn persoonlijke gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven en betreffende het lidmaatschap van een vakvereniging. Foto's en videobeelden kunnen zulke persoonsgegevens bevatten; een hoofddoek en huidskleur bieden immers informatie over godsdienst en mogelijk ras. Op grond van artikel 16 van de Wbp is verwerking van deze gegevens verboden, tenzij een van de uitzonderingen in de artikelen 17 -23 Wbp van toepassing is. Het voert te ver om in het kader van dit rapport uitgebreid bij deze materie stil te staan. Wij volstaan hier met te wijzen op de algemene uitzonderingsgrond in artikel 23. Op grond van dit artikel is het verwerkingsverbod onder andere niet van toepassing als de verwerking geschiedt met uitdrukkelijke toestemming van de betrokkene of als de gegevens door de betrokkene duidelijk openbaar zijn gemaakt, of als verwerking noodzakelijk is voor de vaststelling, de uitoefening of de verdediging van een recht in rechte. Bij het inzien en monitoren van gegevens om onrechtmatig gedrag vast te stellen kan mogelijk deze laatste grond uitkomst bieden wanneer bij het monitoren en inzien van communicatie, al dan niet verwacht, bijzondere persoonsgegevens worden aangetroffen.

## Cloud-computing en toepasselijk recht

De toepasselijkheid van wet- en regelgeving is normaliter gebonden aan een bepaald territorium: in Nederland geldt Nederlands recht, op de BES-eilanden geldt Antilliaans recht (en voor een deel Nederlands recht), in de Verenigde Staten geldt Amerikaans recht (dat weer onderverdeeld is in het recht van staten en het federale recht). Bij computernetwerken is het niet altijd duidelijk welk recht van toepassing is, maar meestal is dat nog wel goed te bepalen aan de hand van de plaats waar servers en computers staan waar een handeling op betrekking heeft.

Door *cloud-computing* wordt ook dat laatste moeilijk te bepalen: in de *cloud* maakt het immers niet meer uit waar een server precies staat, en vaak is het dan ook onduidelijk op welk territorium bijvoorbeeld gegevens zijn opgeslagen. Dan is het ook onduidelijk welk recht van toepassing is.

In dit rapport zijn we uitgegaan van dienstverlening op Nederlands grondgebied en we hebben dan ook alleen aan Nederlands recht aandacht besteed. Voor onderwijsinstellingen die diensten uitbesteden in de *cloud*, vergt het vraagstuk van toepasselijk recht bijzondere aandacht. Binnen het bestek van dit rapport kunnen we daarop niet nader ingaan. We verwijzen naar een ander rapport dat voor SURF is geschreven over de juridische aspecten van cloud-computing in de onderwijssector,[10] en in aanvulling daarop naar een recent advies van de Artikel 29 Werkgroep over toepasselijk recht.[11]

---

http://www.surfnetkennisnetproject.nl/attachments/session=cloud_mmbase+2320973/De_wolk_in_het_onderwijs_feb2011.pdf.

[10] Colette Cuijpers e.a. (2010), *De wolk in het onderwijs*, Tilburg: TILT.

[11] Article 29 Data Protection Working Party, *Opinion 8/2010 on applicable law*, te vinden op http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm.

# Autorisatie- en systeembeheer

## Aanpassen van wachtwoorden

### Omschrijving

Het aanpassen van wachtwoorden is relevant in twee verschillende situaties. In de eerste plaats kan een medewerker of student zelf vragen om het wachtwoord aan te passen (of een nieuw wachtwoord te krijgen omdat het oude vergeten is). In de tweede plaats kan derde vragen om (tijdelijk) een wachtwoord aan te passen. In deze tweede situatie kan bijvoorbeeld een collega of leidinggevende aan een ICT-medewerker verzoeken om het wachtwoord van een collega (tijdelijk) aan te passen, zodat zij toegang kunnen hebben tot het account van die collega, of wellicht om de toegang van de collega zelf (tijdelijk) te blokkeren. In die situatie gaat het niet om het aanpassen van het wachtwoord als zodanig, maar om inzage in gegevens of het afsluiten van accounts. In algemene voorwaarden of in een privacybeleid kunnen naast informatie over inzage ook procedures opgenomen worden over wachtwoordbeheer. Hiervoor gelden immers richtlijnen voor medewerkers en studenten (vertrouwelijk behandelen, niet afstaan aan derden etc.) die vanuit een oogpunt van kenbaarheid het beste hun weerslag kunnen vinden in een geschreven document. Het kan daarbij geen kwaad om ook de manier waarop het systeembeheer met wachtwoorden omgaat en de procedures en voorwaarden over het toekennen en aanpassen van wachtwoorden op schrift te stellen. Voor het overige gelden voor deze situatie dezelfde voorwaarden en aandachtspunten als voor het verstrekken van gegevens aan collega's of leidinggevenden (zie hfd. 5) en afsluiten van accounts (zie hieronder, Afsluiten van een account of bepaalde functionaliteiten).

In deze paragraaf beperken we ons verder tot de eerste situatie, waarbij persoon A zelf verzoekt om haar wachtwoord aan te passen, meestal omdat zij het vergeten is. Over het algemeen laat het systeem toe, en wordt het vaak zelfs vanuit de organisatie periodiek vereist om de beveiliging te verhogen, dat medewerkers zelf hun wachtwoord kunnen wijzigen. Soms kan hiervoor de hulp van ICT-medewerkers ingeroepen moeten worden. Dan is het belangrijk dat degene die het wachtwoord aanpast, zeker weet dat degene die om aanpassing van het wachtwoord verzoekt ook daadwerkelijk persoon A is, en niet een kwaadwillende derde op zoek naar toegang tot de gegevens van persoon A of tot het ICT-systeem van de onderwijsinstelling.

### Relevante wet- en regelgeving en jurisprudentie

- Grondwet, artikel 10, en Europees Verdrag voor de Rechten van de Mens, art. 8
- Wet bescherming persoonsgegevens
- Goed werknemerschap (art. 7:611 BW)
- Goed werkgeverschap (art. 7:611 BW)
- Onrechtmatige daad (art. 6:162 BW)
- Arbeidscontract
- Eventuele gedragscodes (Bijv. 'Gedragscode e-mail, internet- en telefoonfaciliteiten UvT')

### Juridische voorwaarden

Er zijn geen specifieke juridische voorwaarden van toepassing op het aanpassen van wachtwoorden op verzoek van de gebruiker. Wel gelden de regels van de Wbp (omdat er persoonsgegevens worden verwerkt, zie hfd. 2) en de algemene grens van de onrechtmatige daad (het aanpassen van

het wachtwoord mag niet in strijd zijn met ‘wat in het maatschappelijk verkeer betaamt’), wat betekent dat de ICT-medewerker zorgvuldigheid moet betrachten.

### Juridische aandachtspunten

Vanuit een oogpunt van veiligheid is het van belang dat wachtwoorden pas worden gewijzigd wanneer de ICT-mederwerker er voldoende zeker van is dat degene die om wijziging van het wachtwoord verzoekt echt degene is aan wie het wachtwoord is toegekend. Omwille van kenbaarheid is het voor medewerkers en studenten, maar zeker ook voor de ICT-medewerker, van belang dat de werkgever duidelijkheid verschaft in de voorwaarden waaronder de ICT-medewerker bevoegd is een wachtwoord te wijzigen. De ICT-medewerker zal zich, op basis van het goed werknemerschap, dan aan deze voorwaarden en procedures moeten houden.

Er kan daarbij een onderscheid tussen medewerkers en studenten gerechtvaardigd zijn. Ervan uitgaande dat de ICT-medewerker veel van haar collega’s kent, en dat verzoeken om wijziging via interne telefoonlijnen worden gedaan, kan voor medewerkers een telefonisch verzoek tot aanpassing van het wachtwoord wellicht afdoende zijn. Bij grote instellingen waarbij ICT-medewerkers de meeste van de collega’s echter niet in persoon kennen, is telefonische identificatie echter weinig betrouwbaar, ook niet als een interne lijn wordt gebruikt. Een verzoek per email (van een privéadres) of sms biedt waarschijnlijk ook te weinig identificatiezekerheid en zal dus mogelijk op die grond afgewezen moeten worden. Voor die situaties kan een extra identificatiemiddel nodig zijn, bijvoorbeeld dat de ICT-medewerker de verzoeker terugbelt op het interne nummer of op het thuisnummer.

Bij studenten, waarmee ICT-medewerkers minder (persoonlijk) contact hebben, kunnen wellicht zwaardere identificatie-eisen worden gesteld, bijvoorbeeld dat een student die om wachtwoord wijziging verzoekt zich in persoon met haar collegekaart moet melden bij de ICT-afdeling.

In enkele algemene voorwaarden van diensten op Internet kan worden teruggevonden dat de “eigenaar zich het recht voorbehoud het wachtwoord en de toegangscode te veranderen indien dit noodzakelijk is in het belang van het functioneren van de website”. Eventueel kan de onderwijsinstelling een dergelijk voorbehoud opnemen in het contract met medewerker of student of in een gedragscode. Als mogelijke sanctie op oneigenlijk (in strijd met wet, contract en/of gedragscode) zou daarbij vermeld kunnen worden het aanpassen van een wachtwoord (dus feitelijk de toegang blokkeren totdat de gebruiker het nieuwe wachtwoord krijgt, wellicht na een vermaning of boetedoening). In die gevallen ligt het afsluiten van een account of van bepaalde functionaliteiten echter meer voor de hand dan het aanpassen van een wachtwoord. Daarover gaat de volgende paragraaf.

## Afsluiten van een account of bepaalde functionaliteiten

### Omschrijving

Een onderwijsinstelling hanteert meestal een gedragscode voor het gebruik van ICT-faciliteiten. Bij overtreding van die gedragscode, of bij overtreding van wet- en regelgeving zoals auteursrechten of strafwetgeving, zal de instelling sancties willen hanteren. Een mogelijke sanctie – de meest vergaande buiten uitschrijving als student of ontslag van de medewerker – is het afsluiten van het account. Veel algemene voorwaarden en gedragscodes die in het kader van dit onderzoek geraadpleegd zijn, noemen bijvoorbeeld de schending van intellectuele-eigendomsrechten (zoals auteursrecht) uitdrukkelijk als grond voor het afsluiten of opschorten van een account. Iets minder ingrijpend is het afsluiten van bepaalde functionaliteiten, zoals het gebruiken van serverruimte of het kunnen versturen van MP3-bestanden.

Bij het sluiten van een account of van bepaalde functionaliteiten, gaat het erom dat de student of medewerker van een onderwijsinstelling niet langer gebruik kan maken van het account of van bepaalde functionaliteiten. Dit kan vergaande gevolgen hebben. Een student die niet langer toegang heeft tot Blackboard, of tot zijn mailadres van de onderwijsinstelling, zal belangrijke informatie over het lesprogramma missen, waardoor bijvoorbeeld inleverdata voor opdrachten en daarmee gehele vakken en studies niet gehaald worden. Voor medewerkers geldt hetzelfde voor wat betreft het kunnen uitoefenen van hun functie. Daarom vergt het afsluiten van een account of van bepaalde functionaliteiten een zorgvuldige procedure, die meestal zal samenhangen met een gedragscode. Zowel de gedragscode als de mogelijke gevolgen van overtreding daarvan, inclusief het afsluiten van een account, moeten voldoende kenbaar zijn voor alle medewerkers en studenten.

## Relevante wet- en regelgeving en jurisprudentie

- Arbeidscontract of contract tussen onderwijsinstelling en student
- Goed werkgeverschap (art. 7:611 BW)
- Goed werknemerschap (art. 7:611 BW)

## Juridische voorwaarden

Wij hebben geen relevante jurisprudentie kunnen vinden over het (on)rechtmatig sluiten van een account. De belangrijkste voorwaarden voor het rechtmatig afsluiten van een account of bepaalde functionaliteiten zijn dat:

1. De contracten en algemene voorwaarden dienen in orde zijn, dat wil zeggen dat daarin uitdrukkelijk moet blijken dat de instelling het account en de bijbehorende functionaliteiten aan studenten en medewerkers ter beschikking stelt onder voorwaarde dat zij zich houden aan wet- en regelgeving en de op de instelling geldende gedragscode(s);
2. De contracten en algemene voorwaarden een bepaling moeten bevatten dat schending van wet- en regelgeving of van de geldende gedragscode aanleiding kan zijn om een account te sluiten of bepaalde functionaliteiten op te schorten;
3. De regels en procedure voor het afsluiten van een account of bepaalde functionaliteiten voldoende kenbaar zijn voor de studenten en medewerkers; de algemene voorwaarden en de gedragscode moeten daarbij vermoedelijk actief onder de aandacht worden (of zijn) gebracht.

Deze voorwaarden zijn *voldoende* om een account of functionaliteiten rechtmatig te kunnen afsluiten. De voorwaarden zijn echter niet per se *noodzakelijk*: Ook zonder een expliciete regeling in contract, algemene voorwaarden of gedragscode kan een instelling in bepaalde omstandigheden iemands account afsluiten. Dat gebeurt dan op basis van de algemene regels van het goed werknemerschap en goed werkgeverschap: beiden moeten zich ‘behoorlijk’ gedragen. Dat betekent dat een werknemer die de wet overtreedt, bijvoorbeeld door op de werkcomputer kinderpornografie van Internet binnen te halen, door de werkgever bestraft kan worden met het (al dan niet tijdelijk) afsluiten van Internettoegang, ook als dat niet met zoveel woorden in het arbeidscontract, algemene voorwaarden of gedragscode staat. Het moet dan wel om tamelijk evidente gevallen van onrechtmatig handelen door de werknemer of student gaan; voor minder evidente gevallen is wel een expliciete basis nodig in een gedragscode.

## Juridische aandachtspunten

Met betrekking tot de vraag of het afsluiten of opschorten van een account of bepaalde functionaliteiten is toegestaan, spelen een paar vragen een belangrijke rol.

1. Zijn de bepalingen die in de gedragscode zijn opgenomen in overeenstemming met de wet?

2. In de tweede plaats, is de gedragscode *duidelijk kenbaar* gemaakt aan de medewerkers en studenten zodat zij weten wat op basis van de gedragscode al dan niet is toegestaan? Hierbij is ook van belang dat de gedragscode (of het arbeidscontract/contract met de student) duidelijk aangeeft wat de sancties zijn op het niet naleven van de gedragscode, inclusief wanneer dit kan leiden tot het afsluiten of opschorten van een account of bepaalde functionaliteiten.

3. *Door wie en hoe* wordt vastgesteld of er sprake is van een schending van de gedragscode? De instelling zal iemand moeten aanwijzen die bevoegd is om hierover te oordelen, bijvoorbeeld een security officer. Uit de gedragscode moet blijken dat de onderwijsinstelling (hierbij aangegeven welke functie precies binnen de onderwijsinstelling) bevoegd is deze vaststelling met welke middelen te doen, uiteraard binnen de grenzen die de wet stelt (bijvoorbeeld het respecteren van wetgeving voor privacy en de bescherming van persoonsgegevens) (zie nader hfd. 4). Enige discussie is mogelijk over de vraag of de onderwijsinstelling zelf voldoende bevoegdheid heeft om een schending vast te stellen of dat een derde (bijvoorbeeld een rechter) deze vaststelling moet bekrachtigen. Dat zal afhangen van de aard van de norm en de aard van de overtreding.

    a. Overtreding van een *norm uit de gedragscode* – bijvoorbeeld dat men geen pornografische webpagina's mag bezoeken – kan door de instelling zelf worden vastgesteld. Als er discussie is over de vraag of een bezochte pagina wel pornografie bevat (in plaats van bijvoorbeeld artistieke naaktfoto's), kan de beoordeling wellicht worden voorgelegd aan een onafhankelijke partij, zoals een commissie voor klachten en beroep of een ethische commissie van de instelling.
    b. Overtreding van *wet- en regelgeving* kan in sommige gevallen door de instelling zelf worden vastgesteld, met name als het gaat om onmiskenbaar onrechtmatige handelingen, zoals bezit van prepuberable kinderpornografie. Bij niet-evidente onrechtmatigheden zal, wanneer de student of medewerker bestrijdt dat er sprake is van overtreding, echter eerder een oordeel van de rechter aangewezen zijn, omdat het die instantie is die uiteindelijk bepaalt wat wel en niet mag volgens de wet. Het zal echter niet altijd praktisch of wenselijk zijn om een geschil voor te leggen aan de rechter. In dat geval kan wederom een beroep op een onafhankelijke partij – zoals een commissie voor klachten en beroep of een door beide partijen aanvaarde arbiter – uitkomst bieden.

4. Bij het vaststellen van een schending is het van belang dat hiervoor *voldoende bewijs* voorhanden is, en dat de betrokken accounthouder gehoord wordt om haar kant van het verhaal toe te lichten en eventuele gronden aan te dragen die de overtreding rechtvaardigen of verzachten, waardoor bijvoorbeeld een berisping een gepastere sanctie is dan het afsluiten van het account. Het bewijs zou zelfstandig beoordeeld moeten worden door de bevoegde functionaris (zie punt 3); het enkel afgaan op een klacht van een derde – zoals een instantie die beweert dat een medewerker auteursrechten heeft geschonden – is niet voldoende.

5. Tot slot is het van belang dat de *sanctie*, het afsluiten of opschorten van account of bepaalde functionaliteiten *in verhouding* staat tot de overtreding die begaan is. De beginselen van proportionaliteit en subsidiariteit zullen hierbij mee moeten wegen, zeker aangezien de sanctie van het afsluiten van een account of functionaliteiten vergaande consequenties kan hebben.

## Juridische problemen en onduidelijkheden

Een punt voor nader onderzoek is wat precies de voorwaarden en omstandigheden zijn die in de rechtspraak worden gehanteerd voor ontslag van medewerkers op basis van overtreding van

gedragscodes of wet- en regelgeving. Aangezien ontslag een nog ingrijpender sanctie is dan het afsluiten van een account, zullen die voorwaarden en omstandigheden die ontslag rechtvaardigen in elk geval ook het afsluiten van een account kunnen rechtvaardigen. De in jurisprudentie gehanteerde voorwaarden voor rechtmatig ontslag kunnen nog nader worden geïnventariseerd.

# Beveiligen van gegevens

## Omschrijving

Systeembeheerders dragen zorg voor een passende beveiliging van de informatie- en communicatiesystemen op een onderwijsinstelling. Beveiliging omvat de vertrouwelijkheid, de integriteit & authenticiteit en de beschikbaarheid van gegevens.

## Relevante wet- en regelgeving en jurisprudentie

- Wet bescherming persoonsgegevens, art. 12, 13 en 14
- goed werkgeverschap (art. 7:611 BW)
- Wetboek van Strafrecht, art. 161septies en 350b
- Code voor informatiebeveiliging (NEN ISO 27001, voorheen BS 7799-2, en ISO 27002)

## Juridische voorwaarden

1. Er bestaat geen algemeen of overkoepelend juridisch kader voor informatiebeveiliging. Van onderwijsinstellingen van enige omvang mag men echter verwachten dat zij, als een goed werkgever, zorgvuldig omgaan met informatiestromen van hun medewerkers en studenten en hun systemen naar redelijke maatstaven beveiligen tegen verlies, diefstal of lekken.

2. Voor de verwerking van persoonsgegevens bestaat wel een specifieke beveiligingsplicht. Artikel 13 Wbp legt een algemene beveiligingsplicht op aan de instelling voor de verwerking van persoonsgegevens:

   > De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

3. Wanneer de instelling de verwerking van persoonsgegevens, zoals emailverkeer of dataopslag, uitbesteedt aan een derde partij (een ‘bewerker’ in de terminologie van de Wbp), moet de instelling erop toezien dat deze derde voldoende waarborgen biedt voor informatiebeveiliging. De instelling ziet toe op de naleving daarvan (artikel 14 Wbp).

4. ICT-medewerkers die uit hoofde van hun functie kennisnemen van persoonsgegevens, zijn verplicht hierover geheimhouding te betrachten, tenzij zij wettelijk verplicht zijn of hun taak het noodzakelijk maakt om mededeling te doen aan iemand (art. 12 Wbp).

## Juridische aandachtspunten

1. De Wbp vraagt om een *passend niveau* van informatiebeveiliging. Maximale of ‘effectieve’ beveiliging wordt niet geëist. Er moet een risicoinschatting worden gemaakt van de risico’s van inbreuken op de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens en vervolgens een kosten-batenanalyse van de maatregelen die getroffen kunnen worden om deze risico’s te beheersen. Het niveau van informatiebeveiliging zal dus afhangen van bijvoorbeeld de soort

persoonsgegevens, de risico's van aantasting en de draagkracht van de instelling. Het College Bescherming Persoonsgegevens heeft een rapport uitgebracht met een nadere aanduiding van welk niveau in welke situaties passend is.[12] Een belangrijk hulpmiddel bij het maken van de risico- en kosten-batenanalyse is de Code voor informatiebeveiliging, een NEN-norm.[13]

2. Een onderdeel van het beveiligen van persoonsgegevens is het beginsel van *dataminimalisatie*: de maatregelen moeten onnodige verzameling en verdere verwerking van persoonsgegevens voorkomen. Dit is een uitwerking van het centrale beginsel van doelbinding: de instelling moet specifieke doelen definiëren voor het verzamelen en verwerken van persoonsgegevens van medewerkers en studenten, en moet de verwerking tot die doelen beperken.

3. Het Wetboek van Strafrecht kent twee bepalingen over *strafbare nalatigheid* bij informatiebeveiliging. Art. 350c WvSr stelt strafbaar (met gevangenisstraf van ten hoogste een maand) iemand aan wiens schuld te wijten is dat ernstige schade ontstaat door de aantasting van computergegevens. Nu wordt dit artikel zelden toegepast (er is geen jurisprudentie over), maar het suggereert wel een minimumeis van aandacht voor informatiebeveiliging bij systeembeheerders als er risico's zijn op ernstige schade door bijvoorbeeld computervirussen. Minder relevant, maar met een hoger strafmaximum, is art. 161septies WvSr, dat een vergelijkbare bepaling bevat toegespitst op computers of netwerken voor het algemeen nut of publieke diensten; dit legt de minimumdrempel hoger voor informatiebeveiliging in een academisch medisch centrum, en wellicht ook voor de Open Universiteit.

4. Er bestaan, in aanvulling op de geheimhoudingsplicht van art. 12 Wbp, enkele specifieke juridische *geheimhoudingsplichten*, zoals voor ICT-medewerkers die rechtmatig kennis nemen van de inhoud van emails of telefoongesprekken (art. 273d lid 1 onder c en lid 2 WvSr) en voor medewerkers die op bevel gegevens aan politie en justitie verstrekken (zie hfd. 6) (art. 126bb lid 5 WvSv).

5. Er bestaat *geen* wettelijke plicht om *beveiligingsincidenten* ('datalekken') te *melden* (de zogeheten *data security breach notification*). Het wetsvoorstel dat een meldplicht invoert (ter implementatie van de Europese Richtlijn 2009/136/EG) beperkt zich tot aanbieders van *openbare* telecommunicatiediensten, waar (hoger)onderwijsinstelling niet onder vallen.

---

[12] G.W. van Blarkom & J.J. Borking, *Beveiliging van persoonsgegevens*, Achtergrondstudies & Verkenningen 23, Den Haag: Registratiekamer 2001, beschikbaar op http://www.cbpweb.nl/Pages/av_23_Beveiliging.aspx.

[13] Voor een bruikbare afvinklijst bij de Code voor informatiebeveiliging, zie http://www.euronet.nl/users/ernstoud/praktijkgids/Checklist%20D1.pdf. Juridische aspecten van en aanvullingen op de Code worden toegelicht in B.J. Koops, 'De Code voor Informatiebeveiliging naar Nederlands recht', *Informatiebeveiliging* 2003 nr. 5, p. 20-24.

# Loggen en monitoren

## Algemeen

Het loggen en monitoren van ICT-gebruik van medewerkers en studenten zal meestal plaatsvinden om te controleren of de ICT-faciliteiten worden gebruikt in overeenstemming met de geldende regels – regels van wetgeving (bijvoorbeeld auteursrecht en strafwetgeving) of regels en richtlijnen uit de gedragscode van de instelling.

Op het controleren van email- en Internetgebruik van medewerkers en studenten is de Wbp van toepassing (zie algemeen hfd. 2), alsook het goed werkgeverschap en goed werknemerschap. De kenbaarheid van rechten en plichten is daarbij een belangrijk criterium om te bepalen of, en zo ja in hoeverre, inbreuken op de privacyrechten van medewerkers en studenten gerechtvaardigd zijn. Buiten expliciete bepalingen in de arbeidsovereenkomst (medewerkers) of de overeenkomst tot afname van onderwijs (student), zal de kenbaarheid van de regels over gebruik van ICT-faciliteiten en het monitoren om mogelijk misbruik op te sporen, vooral gebaseerd moeten zijn op gedragscodes of een privacybeleid.

Er zijn diverse model-gedragscodes ontwikkeld die instellingen kunnen gebruiken. Het College Bescherming Persoonsgegevens heeft uitgebreid richtlijnen en aandachtspunten beschreven voor het monitoren van email en Internet in de publicatie *Goed werken in netwerken*,[14] en ook een *Raamregeling voor email- en internetgebruik* opgesteld die instellingen nader kunnen invullen.[15] Alternatieven zijn de modelgedragscodes van het CNV[16] en VNO-NCW;[17] de eerste heeft over het algemeen wat vriendelijker bepalingen voor werknemers, de laatste wat strengere.

## Monitoren van email- en Internetgedrag

### Omschrijving

Om het ICT-gedrag van medewerkers en studenten in kaart te brengen kan gebruik gemaakt worden van het loggen en monitoren van email- en surfgedrag. Een belangrijk onderscheid is of het monitoren generiek gebeurt (altijd van iedereen) of specifiek (tijdelijk in een concreet geval). Generiek monitoren is mogelijk om algemeen te controleren of de gedragscode ICT-gebruik wordt nageleefd (zoals camera's op de snelweg in het algemeen controleren of snelheidswetgeving wordt nageleefd). Daarvoor gelden strengere regels dan voor specifieke monitoring bij een concrete verdenking van misbruik. Het laatste kan het geval zijn bij medewerkers, bijvoorbeeld bij verdenking van buitenproportionele privéactiviteiten op het werk of, in uitzonderlijke omstandigheden, controle op thuiswerken. Bij studenten kan gedacht worden aan de verdenking van misbruik van faciliteiten van de onderwijsinstelling voor het uploaden van auteursrechtelijk beschermd materiaal of het binnenhalen van kraaksoftware.

### Relevante wet- en regelgeving en jurisprudentie

- Grondwet, artikel 10, en Europees Verdrag voor de Rechten van de Mens, art. 8

---

[14] Beschikbaar op http://www.cbpweb.nl/Pages/av_21_Goed_werken_in_netwerken.aspx.

[15] Beschikbaar op http://www.cbpweb.nl/downloads_av_sv/av21_raamregeling.pdf.

[16] Beschikbaar op http://www.cnv.nl/fileadmin/files/downloads/Gedragscode_email_en_internet.pdf.

[17] Beschikbar op http://www.vno-ncw.nl/SiteCollectionDocuments/Cmsdocs/Brochure%20e-werken.pdf.

- Wet bescherming persoonsgegevens
- goed werknemerschap (art. 7:611 BW)
- goed werkgeverschap (art. 7:611 BW)
- Wet op de ondernemingsraden, art. 27
- Wetboek van Strafrecht, art. 139c en art. 273d
- arbeidscontract
- gedragscode van de instelling (bijv. 'Gedragscode e-mail, internet- en telefoonfaciliteiten UvT')

## Juridische voorwaarden

1. Bij generieke controle op naleving van een ICT-gedragscode mag de werkgever nooit kennis nemen van *communicatie-inhoud* (gesprekken, email). Bij concrete verdenking van misbruik en een specifiek onderzoek naar dat misbruik, is kennis nemen van de inhoud van communicatie wel toegestaan, maar alleen als het noodzakelijk is en er geen ander, minder ingrijpend, middel voorhanden is om hetzelfde doel te bereiken (Wbp; art. 8 EVRM; art. 273d WvSr).

2. Bij het invoeren van een generiek controlesysteem, waarbij het mail- en Internetgedrag van werknemers wordt gevolgd, moet de werkgever voorafgaand *toestemming* vragen aan de *ondernemingsraad* omdat het een zogeheten *personeelsvolgsysteem* betreft (art. 27, lid 1, onder k en l Wet op de ondernemingsraden). Dit geldt voor instellingen die onder deze wet vallen, dat wil zeggen ondernemingen[18] met in de regel 50 of meer werknemers. Merk op dat universiteiten en hogescholen kunnen kiezen de Wet op de ondernemingsraden buiten toepassing te laten (art. 9.30 en 10.16a Wet op het hoger onderwijs en wetenschappelijk onderzoek). Voor instellingen die hebben gekozen voor een andere medezeggenschapsregeling dan een ondernemingsraad is art. 27 Wor misschien niet formeel van toepassing, maar naar de geest van de wet zou volgens ons wel instemming van het medezeggenschapsorgaan moeten worden gevraagd; de universiteitsraad of medezeggenschapsraad moet immers instemming verlenen met regels op het gebied van de arbeidsomstandigheden (art. 8.33(e) en art. 10.20(f) WHW).

3. Wanneer bij het loggen of monitoren gegevens te pas komen die tot individuele werknemers herleidbaar zijn, is de *Wet bescherming persoonsgegevens* van toepassing (zie algemeen hfd. 2). Dat betekent onder andere dat het monitoren een expliciet gedefinieerd doel moet dienen en niet verder mag gaan dan nodig is voor dit doel; dat er een legitieme grondslag moet zijn; en dat het loggen of monitoren proportioneel en subsidiair (het minst ingrijpende middel) moet zijn. Permanente controle op individueel niveau is niet toegestaan. Zie verder hfd. 2 (algemeen) en hieronder bij juridische aandachtspunten.

4. Wanneer het loggen of monitoren op *geaggregeerd* niveau plaatsvindt of op individueel niveau met (onomkeerbare) *anonimisering*, waarbij gegevens niet te herleiden zijn tot individuele werknemers of studenten, is de Wbp niet van toepassing.

5. De werkgever mag *geen misbruik* maken van zijn bevoegdheid of de technische mogelijkheid tot het monitoren van email- of Internetgedrag (art. 7:611 BW; art. 139c WvSr).

---

[18] Een onderneming is een 'als zelfstandige eenheid optredend organisatorisch verband waarin krachtens arbeidsovereenkomst of krachtens publiekrechtelijke aanstelling arbeid wordt verricht' (art. 1 lid 1 onder c Wor).

## Juridische aandachtspunten

### *A. Inzage van email en afluisteren telefoonverkeer*

1. Voor het kennisnemen van communicatie-inhoud (de inzage van email of het afluisteren en opnemen van telefoongesprekken) gelden strenge regels in verband met het (tele)communicatiegeheim, dat ook op de werkvloer geldt. Onderwijsinstellingen zijn geen openbare telecommunicatieaanbieders (die vallen onder de Telecommunicatiewet) maar zijn wel aanbieders van communicatiediensten zoals omschreven in art. 126la WvSv.[19] Dat betekent dat art. 273d WvSr van toepassing is: iemand die werkzaam is bij een aanbieder van een communicatiedienst is strafbaar als zij opzettelijk en wederrechtelijk kennisneemt van de inhoud van communicatie die niet voor haar zelf is bestemd. Ook het overnemen voor een ander, aftappen of opnemen is strafbaar. De vraag bij deze strafbepaling is nu wanneer inzage in communicatie door de ICT-medewerker *wederrechtelijk* is. Dat is het geval bij overtreding van rechtsnormen, zoals het goed werkgeverschap (art. 7:611 BW), de Wet bescherming persoonsgegevens, of het afluisteren of opnemen van communicatie waarbij sprake is van kennelijk misbruik (art. 139c WvSr). Bij kennelijk misbruik kun je denken aan de ICT-medewerker die haar bevoegdheden om email te controleren duidelijk overschrijdt, of die in opdracht van de werkgever alle email van een ongeliefde collega doorneemt in de hoop een aanleiding te vinden voor een ontslagprocedure.

2. Ook los van het strafrecht zijn sowieso de algemene norm van het goed werkgeverschap, het recht op privacy van art. 10 Gw en art. 8 EVRM, en de Wbp van toepassing op de inzage van email. Ook als de ICT-medewerker niet art. 273d WvSr overtreedt, kan het inzien van email door of namens de werkgever onrechtmatig zijn (dus in civielrechtelijk zin). Hierbij gelden strengere eisen dan het strafrecht: ook als er geen evident misbruik van bevoegdheid is door de werkgever, mag de ICT-medewerker niet disproportioneel handelen (het inzien van de mailbox van een werknemer op basis van een anonieme beschuldiging van kinderporno, zonder eerst nader onderzoek te doen of deze beschuldiging wel enigszins aannemelijk is). In verband met het belang van de bescherming van de inhoud van communicatie, is het belangrijk dat er een zorgvuldige procedure is, die kenbaar is voor de medewerkers en studenten, voor het kunnen onderzoeken van de inhoud van email of het afluisteren van telefoonverkeer. Het is aan te raden dat dit alleen toegestaan is in opdracht van de directie van de instelling.

### *B. Generiek loggen of monitoren*

Vaak zal de Wbp van toepassing zijn op de algemene controle op email- en Internetgedrag van werknemers of studenten, aangezien daarbij meestal persoonsgegevens in beeld komen (behalve als er uitsluitend niet-herleidbaar wordt gelogd, bijvoorbeeld statistisch per diensteenheid). Voor een algemene bespreking van de eisen van de Wbp verwijzen we naar hoofdstuk 2. Hier stippen we de belangrijkste eisen aan.

1. Het *doel* van het loggen of monitoren moet vooraf uitdrukkelijk omschreven worden, bijvoorbeeld in een gedragscode of privacybeleid.

2. Het loggen of monitoren moet zich vervolgens daadwerkelijk *beperken tot dit doel*.

---

[19] Een aanbieder van een communicatiedienst is ‘de natuurlijke persoon of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst’.

3. Er moet een *legitieme grondslag* zijn (art. 8 Wbp). Dit kan de uitvoering van de arbeidsovereenkomst of de overeenkomst met de student zijn, als daarin staat vermeld dat het monitoren onderdeel is van het werk (dan geldt art. 8 onder b Wbp), maar meestal zal de grondslag zijn dat het legitieme belang van de werkgever zwaarder weegt dan het privacybelang van de werknemer en de student (art. 8 onder f Wbp). Dit vraagt om een belangenafweging door de instelling, die dan zijn weerslag vindt in de gedragscode of het privacybeleid.

4. Het doel en de controlemogelijkheid moeten *vooraf kenbaar* zijn bij de medewerkers en betrokkenen. De gedragscode of het privacybeleid moeten dus voldoende kenbaar worden gemaakt aan hen, bijvoorbeeld bij indiensttreding of het begin van de studie maar vervolgens ook goed vindbaar en zichtbaar op de webpagina (het intranet) van de instelling.

5. De werkgever moet onderscheid maken tussen *zakelijke* en privécommunicatie; alleen zakelijke communicatie mag worden gemonitord.

6. De maatregel moet *proportioneel* zijn (in verhouding staan tot het nagestreefde doel). Dit vraagt om terughoudendheid in het beleid.

7. Het doel moet niet op een minder privacyingrijpende manier kunnen worden bereikt (*subsidiariteit*). In dit verband kan de privacypiramide worden gehanteerd, waarbij van laag tot laag gekeken wordt of het nodig is dit aspect van emailverkeer in kaart te brengen; van minst tot meest ingrijpend bestaat de privacypiramide uit volume, welke bijlagen er zijn (maar niet de inhoud daarvan), geadresseerde, het onderwerpsveld, een scan op plaatjes in of bij de email, een scan op de tekstuele inhoud (zoektermen), en het lezen van de inhoud zelf.[20] (Bij dat laatste geldt wat hierboven onder A. is gezegd: inzage van inhoud is niet toegestaan voor algemene controle, dat mag alleen in concrete gevallen van verdenking van onrechtmatig gedrag.)

8. De controle moet op een *behoorlijke en zorgvuldige* manier worden uitgevoerd (art. 6 Wbp).

9. De resultaten van het loggen of monitoren moeten, voor zover deze tot individuen herleidbare gegevens bevatten, adequaat worden *beveiligd* (art. 13 Wbp) (vgl. over beveiliging hfd. 3).

### *C. Specifiek loggen of monitoren bij concrete verdenking*

Wanneer een werknemer of student wordt verdacht van misbruik van de ICT-faciliteiten of van anderszins onrechtmatig gedrag, kan de werkgever besluiten om dit te onderzoeken door het email- of Internetgedrag van deze persoon te monitoren (toekomstige gegevens) of inzage te krijgen in de mailbus (opgeslagen gegevens). Hierop zijn zowel de punten onder A als onder B hierboven geschetst van toepassing.

De situatie is echter anders dan bij B, omdat er aanwijzingen zijn van misbruik door de werknemer of student, waardoor er ingrijpender maatregelen gerechtvaardigd zijn. Anders dan bij generiek monitoren, mag de werkgever (en in diens opdracht de ICT-medewerker) de inhoud van communicatie inzien als dat nodig is om het misbruik aan het licht te brengen en er geen minder ingrijpende middelen (lager in de privacypiramide, zoals inzage in verkeersgegevens) voorhanden zijn.

---

[20] Vgl. L.F. Asscher en W.A.M. Steenbruggen, 'Het Emailgeheim op de werkplek. Over de toelaatbaarheid van inbreuken op het communicatiegeheim van de werknemer in het digitale tijdperk', *Nederlands Juristenblad* 2001 nr. 37.

Bij dwingende en zwaarwegende bedrijfsbelangen mag zelfs de privécommunicatie worden gecontroleerd (voor zover de werknemer of student daarbij gebruik maakt van door de werkgever ter beschikking gestelde middelen). Er moeten dus voldoende aanwijzingen zijn dat de betrokkene verdacht is van wangedrag, en het wangedrag moet voldoende ernstig zijn om de inbreuk op de privacy van de betrokkene te legitimeren. Zo stelde de kantonrechter van Haarlem dat de privacybescherming niet kan ingeroepen worden wanneer de werknemer afbeeldingen met gewelddadig en pornografische inhoud verstuurt (Ktr. Haarlem 16 juni 2000). Dat geldt ook voor seksuele intimidatie (Rb. Rotterdam 29 maart 2001).

Ook bij thuiswerk staat de werknemer onder het gezag van de werkgever. De hiervoor besproken uitgangspunten kunnen voor het thuiswerk in aanmerking worden genomen, zij het onder nog striktere voorwaarden. Thuiswerk berust op een hoge mate van vertrouwen tussen de werkgever en de werknemer. Dit vertrouwen moet ook een weerslag hebben op de mate van controle voor de werkgever. Zo is van belang of de werknemer met zijn eigen computer werkt, of dezelfde computer ook door andere gezinsleden wordt gebruikt en de eventuele mogelijkheid om ook buiten het netwerk van het bedrijf te werken. In ieder geval mag de werkgever zich geen toegang verschaffen tot de bestanden van de andere gezinsleden met wie hij geen arbeidsverhouding heeft. Of de werkgever de communicatie (verkeersgegevens of inhoud) mag controleren die door de werknemer buiten diens werkuren werd uitgevoerd, zal afhangen van eventuele zwaarwichtige vermoedens van ernstig misbruik die de controle rechtvaardigen. Voor zover wij weten is hierover nog geen rechtspraak.

Belangrijk is voorts, als er een ontslag- of verwijderprocedure gaat volgen, dat de betrokkenen eerst een waarschuwing heeft gehad en dat het misbruik daarna, ondanks de waarschuwing, is doorgegaan; de enkele kenbaarheid van de gedragscode in het algemeen is niet voldoende (EHRM 25 juni 1997, NJ 1998, 506, *Halford*). Daarbij moeten we overigens wel aantekenen dat de Nederlandse rechtspraak niet altijd een strikte eis van voorafgaande kenbaarheid lijkt te hanteren; afhankelijk van de omstandigheden van het geval – bijvoorbeeld bij zeer ingrijpend wangedrag – kan ook het monitoren zonder kenbare procedure (gedragscode) of zonder waarschuwing toelaatbaar zijn.

Het blijft wel aan te raden aan instellingen om in een gedragscode op te nemen onder welke omstandigheden door wie (en in opdracht van wie) en op welke manier(en) het email- en Internetverkeer van werknemers of studenten gelogd of gemonitord kan worden, zowel generiek (algemene controle) als specifiek (individueel bij verdenking van misbruik).

# Verstrekken van gegevens (private partijen)

## Algemeen

De verstrekking van persoonsgegevens aan private partijen (voor verstrekking aan de overheid zie het volgende hoofdstuk) kan relevant zijn voor collega's of leidinggevenden (bijvoorbeeld bij langdurige afwezigheid van een werknemer), voor familie (bij overlijden van een werknemer of student) of voor derden, zoals iemand die als auteursrechthebbende gegevens opvraagt. Op deze situaties is grotendeels hetzelfde juridische kader van toepassing, dat we in deze algemene paragraaf schetsen; de toepassing verschilt echter afhankelijk van de context, die we in de volgende paragraaf daarom nader uitwerken in de vorm van casussen.

### *Omschrijving*

Bij verstrekken van gegevens gaat het erom dat gegevens onder beheer van persoon A, op de een of andere wijze overgaan naar het beheer van persoon B. Dit kan zijn doordat persoon A met de wachtwoorden en login van persoon B inlogt in het systeem, maar ook bijvoorbeeld door het doorsturen van gegevens door persoon A naar persoon B. Wanneer het verstrekken van gegevens ook persoonlijke gegevens omvat, kan de Wet bescherming persoonsgegevens (Wbp) van toepassing zijn. Op specifieke Wbp-verplichtingen rond het verstrekken van persoonsgegevens wordt hieronder aan de hand van verschillende casussen ingegaan; voor de overige, algemeen geldende verplichtingen uit de Wbp verwijzen we naar hfd. 2, Wet bescherming persoonsgegevens (Wbp).

### *Relevante wet- en regelgeving en jurisprudentie*

- Grondwet, artikel 10, en Europees Verdrag voor de Rechten van de Mens, art. 8
- Wet bescherming persoonsgegevens
- Goed werknemerschap (art. 7:611 BW)
- Goed werkgeverschap (art. 7:611 BW)
- Arbeidscontract
- Eventuele gedragscodes (Bijv. 'Gedragscode e-mail, internet- en telefoonfaciliteiten UvT')

### *Jurisprudentie*

- Hoge Raad 25 november 2005 (Lycos-Pessers) (LJN AU4019)
- Voorzieningenrechter Rechtbank Amsterdam 24 augustus 2006 (BREIN-UPC) (LJN AY6903)

### *Juridische voorwaarden en aandachtspunten*

Om conflicten in situaties als hieronder in verschillende casussen geschetst te voorkomen en om transparantie bij zowel medewerkers als leidinggevenden te vergroten, is het verstandig afspraken over het verstrekken van persoonsgegevens, voor zover niet al onderdeel van de arbeidsovereenkomst, vast te leggen in een gedragscode of privacyreglement. Dergelijke instrumenten van zelfregulering, die door verwijzing in de arbeidsovereenkomst onderdeel uit kunnen maken van het arbeidscontract en daarmee, voor zover niet strijdig met de wet, ook contractueel afdwingbaar zijn, kunnen inzicht bieden in hoe zowel studenten, medewerkers en leidinggevenden, om moeten gaan met het gebruik van faciliteiten als email en internet.

Hierin kan onder andere ook vastgelegd worden wie binnen de onderwijsinstelling bevoegd is onder welke omstandigheden persoonsgegevens te verwerken en wie bevoegd is namens de onderwijsinstelling de belangenafwegingen uit te voeren die vaak nodig is op grond van artikel 8 onder f Wet bescherming persoonsgegevens (zie hieronder bij de casusbespreking). Vanuit dit perspectief kan het verstandig zijn een functionaris voor de gegevensverwerking aan te stellen, zoals bedoeld in art. 62 Wbp, of in ieder geval een persoon binnen de organisatie aan te wijzen als specifiek aanspreekpunt voor privacygerelateerde vraagstukken, die duidelijk kenbaar een aanspreekbaar is voor medewerkers en studenten. Voorlichting en scholing zijn noodzakelijke instrumenten om binnen de organisatie bewustwording te creëren hoe omgegaan mag en moet worden met aangeboden (internet)faciliteiten en met de privacy van werknemers en studenten.

## Verstrekken van gegevens aan collega's of leidinggevende

### *Juridische voorwaarden en aandachtspunten*

*Casus I: ziekte*

*Medewerker A heeft een mailaccount bij de onderwijsinstelling waarin hij zowel zijn privémail als zijn werkgerelateerde mail ontvangt. Werkgerelateerd is medewerker A betrokken in het onderwijs, hij is docent van een twintigtal studenten, en hij is betrokken bij een groot onderzoeksproject, KERST genaamd. Op een dag, vlak voor de deadline van het inleveren van de examencijfers van zijn studenten, maar ver vóór de deadline van het onderzoeksproject KERST, wordt medewerker A ernstig ziek waardoor hij tijdelijk het bed moet houden. Mogen nu gegevens van medewerker A aan zijn leidinggevende of een collega verstrekt worden bij zijn afwezigheid?*

In deze casus zijn een aantal partijen in het geding bij het verstrekken van gegevens van medewerker A aan de leidinggevende of de collega. In eerste instantie medewerker A. Hij kan er zelf voor kiezen zijn leidinggevende of een collega gegevens te verstrekken, zodat zij taken van hem waar kunnen nemen tijdens zijn afwezigheid. Ook kan medewerker A toestemming geven aan de leidinggevende of een collega om bestanden uit zijn mailaccount of (online) bestanden te halen zodat zij zijn taken waar kunnen nemen. In beide gevallen is er in de relatie tussen medewerker A en de leidinggevende of de collega een gerechtvaardigd doel en een legitieme verwerkingsgrond voor de verwerking van de persoonsgegevens van medewerker A, voor zover deze volgen uit de mailaccount of de (online) bestanden. Artikel 7 vereist voor een zorgvuldige verwerking van persoonsgegevens een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel voor verwerking, in deze casus is dat bijvoorbeeld de tijdige afhandeling van de examencijfers van de studenten van medewerker A. Artikel 8 van de Wbp vereist voor een behoorlijke en zorgvuldige verwerking van persoonsgegevens een legitieme verwerkingsgrond. Toestemming van de betrokkene (de persoon wiens gegevens verwerkt worden) is een legitieme verwerkingsgrond. In de geschetste casus moet nog wel rekening gehouden worden met het feit dat wanneer medewerker A niet zelf bestanden doorstuurt naar de leidinggevende of de collega, maar deze toegang verleent tot zijn mail en bestanden, de leidinggevende en de collega enkel die mail en bestanden mogen raadplegen die noodzakelijk zijn met het oog op het doel, het tijdig kunnen aanleveren van examencijfers. Privémail en bestanden mogen uiteraard niet geopend worden, maar ook de mail en bestanden over het project KERST moeten onberoerd blijven. Wanneer medewerker A langdurig ziek blijft, dan kan hij de mail en bestanden betreffende het project KERST aan zijn leidinggevende of collega verstrekken, hij kan hen ook, met het oog op het doel van de voortgang van het project KERST, toegang geven tot zijn mailaccount en zijn (online) bestanden. Wederom geldt dan dat het verwerken van de gegevens beperkt moet blijven met het oog op het doel; de voortgang van het project KERST. Dit volgt overigens niet alleen uit de Wbp, maar voor de leidinggevende volgt bijvoorbeeld ook uit het goed werkgeverschap dat privémail van

medewerkers niet gelezen mag worden. Hoe zit dit als gedragscode werknemer uitdrukkelijk verbied op mailaccount werkgever privémail te ontvangen?[21]

In de casus spelen echter ook nog persoonsgegevens van de personen die vermeld staan met identificerende gegevens (op grond van de Wbp is een persoonsgegeven een gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon) in de mail en de bestanden van medewerker A, zoals de studenten en de medewerkers van het project KERST, en de personen in de privémail van medewerker A. Zoals hierboven al aangegeven zullen de leidinggevende en de collega zich in bovenstaande casus moeten onthouden van het neuzen in de privémail van medewerker A, het 'verstrekken van' persoonsgegevens van anderen dan medewerker A zal zich dan ook beperken tot hetgeen zichtbaar is in titels van bestanden en onderwerpsvelden van emailberichten. Hoewel het hierbij dan toch gaat om de verwerking van deze persoonsgegevens (de Wbp omschrijft verwerking heel breed, alles van creatie tot vernietiging van gegevens, waaronder dus ook het 'tevoorschijn toveren' van gegevens op een computerscherm). Er blijft een legitiem doel voorhanden, het tussen de mails en bestanden uitvissen van de bestanden betreffende de examenuitslagen, en bij langdurige ziekte ook die betreffende het project KERST. De verwerkingsgrond toestemming is echter discutabel, nu medewerker A geen toestemming kan geven voor de verwerking van persoonsgegevens die niet hem, maar zijn studenten en zijn collega's in het project KERST betreffen, en eventueel zijn privé relaties die hem een mail hebben gestuurd op zijn werk mail account. Voor zowel de verwerking van de persoonsgegevens van de studenten als voor de persoonsgegevens van de medewerkers in het project KERST kan gesteld worden dat verwerkingsgrond 8 c) van de Wbp mogelijk uitkomst kan bieden. Artikel 8 c) geeft aan dat persoonsgegevens verwerkt mogen worden wanneer deze verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst. De student heeft een overeenkomst met de onderwijsinstelling met betrekking tot het afnemen van onderwijsdiensten. Voor een deugdelijke uitvoering van deze overeenkomst van de zijde van de onderwijsinstelling, kan gesteld worden dat het in het onderhavige geval noodzakelijk is de gegevens van medewerker A naar een andere medewerker te verstrekken. De overeenkomst van de student met de onderwijsinstelling kan dusdanig worden uitgelegd dat een ieder binnen de organisatie van de onderwijsinstelling de persoonsgegevens van de student mag verwerken, voor zover dit noodzakelijk is met het oog op het kunnen voorzien in de onderwijsdienstverlening aan de student. In dit voorbeeld, het tijdig verwerken van examenuitslagen. Met betrekking tot de medewerkers in het project KERST geldt waarschijnlijk hetzelfde. Het gaat dan niet om de overeenkomst tussen student en de onderwijsinstelling, maar om de overeenkomst die ten grondslag ligt aan het project KERST, waarbij (de onderwijsinstelling van) de medewerkers in het project KERST partij zijn. Voor de uitvoering van deze overeenkomst is het noodzakelijk dat wanneer medewerker A langdurig ziek wordt, hij gegevens door kan geven aan zijn leidinggevende of zijn collega, met het oog op voortgang van het project. Ook hier geldt weer de doelbinding, gegevens mogen slechts verwerkt worden voor zover noodzakelijk met het oog op het legitieme doel. Zelfs al zou discussie bestaan over art. 8 c) als verwerkingsgrond, dan kan nog een beroep gedaan worden op de verwerkingsgrond van artikel 8 f): gegevens mogen verwerkt worden indien de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de

[21] Zie bijv. Rechtbank Den Haag, sector kanton, 5 januari 2010, LJN BM3315. Zie ook http://carriere.blog.nl/actualiteit/2010/05/21/betrapt-door-je-werkgever-in-je-prive-mail en http://www.security.nl/artikel/35217/1/Juridische_vraag%3A_personeel_ontvangt_priv%C3%A9mail_op_werk-pc.html.

fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert. Deze grond zal ook als rechtvaardiging kunnen dienen voor de beperkte verwerking van persoonsgegevens die voortvloeien uit de titels en onderwerpsvelden van privémail en privébestanden die de leidinggevende en/of de collega 'tegenkomen' in de zoektocht naar bestanden over de examenuitslagen van studenten en het project KERST. Indien de medewerker A een map met mailbestanden en een map met documenten expliciet gelabeld heeft als privé, is de kans overigens klein dat leidinggevende en/of collega überhaupt met persoonlijke gegevens van privé contacten van medewerker A geconfronteerd worden, en dan worden deze dus ook niet verwerkt.

Maar wat nu als medewerker A niet zelf de bestanden doorstuurt naar zijn leidinggevende of collega, en ook geen toestemming aan hen geeft deze bestanden in te zien? Ook in dit geval zal het ophalen van de relevante (email) bestanden uit het systeem van medewerker A, en daarmee de verwerking van de persoonsgegevens van zowel medewerker A als derden (studenten, projectmedewerkers KERST, privécontacten medewerker A) geoorloofd zijn. Tenminste, voor zover dit noodzakelijk is met het oog op de doelen, tijdige voorziening in examenuitslagen en de voortgang van het project KERST, en niet meer gegevens verwerkt worden dan voor deze doelen noodzakelijk is. Ook hierbij kan eventueel grond 8 c) of anders grond 8 f) aangevoerd worden als verwerkingsgrond. Ook hier spelen naast de Wbp het goed werkgever en het goed werknemerschap een rol. Bij langdurige ziekte mag immers van een medewerker verwacht worden dat hij, met het oog op de voortgang van aan hem toevertrouwde taken, bestanden worden overgedragen voor zover dit noodzakelijk is voor andere medewerkers om (tijdelijk) taken waar te nemen. Aan de ander kant geldt dat de werkgever hierbij zorgvuldig moet handelen en niet meer gegevens in moet zien dan noodzakelijk is met het oog op het waarnemen van taken.

*Casus II: ontslag*

*Deze casus betreft dezelfde situatie als in casus I, maar nu is medewerker A niet ziek, maar is hij ontslagen.*

Hoewel de redenering zoals hierboven weergegeven vanuit het recht op gegevensbescherming niet anders zal zijn, speelt hier het goed werknemerschap en werkgeverschap wellicht nog meer een rol. De medewerker zal de gelegenheid geboden moeten worden om zijn accounts, zowel email als bestanden, op te schonen en zijn werk over te dragen aan andere medewerkers. Wellicht dat het arbeidscontract bepalingen bevat over het sluiten van accounts of dat hierover nadere specificaties zijn opgenomen in een gedragscode. Zo niet, dan zal teruggevallen moeten worden op de Wbp en het goed werkgeverschap en goed werknemerschap. Het gaat dan om een zorgvuldige afhandeling van de (email) bestanden van de ontslagen medewerker, zowel van de zijde van ontslagen werknemer als van de zijde van de werkgever. De medewerker zal mee moeten werken aan de overdracht van lopende zaken, waarbij (email) bestanden aan leidinggevenden en collega's doorgegeven moeten worden. Hierbij gelden dezelfde voorwaarden voor gegevensbescherming als hierboven bij casus I geschetst. Mocht de medewerker niet meewerken aan overdracht en het opschonen van zijn bestanden, dan zal de werkgever de account op mogen heffen, en enkel voor zover noodzakelijk met het oog op zijn gerechtvaardigde belang (bijvoorbeeld overdracht van lopende zaken van de ontslagen medewerker) zich op grond van artikel 8 onder f Wbp) toegang mogen verschaffen tot de email (bestanden), waarbij zoveel mogelijk het privacybelang van de ontslagen medewerker gerespecteerd moet worden. Indien het arbeidscontract bepalingen bevat betreffende het sluiten van accounts en de overdracht van taken na ontslag, kunnen verwerkingen van persoonsgegevens in dit verband tevens gestoeld worden op artikel 8 onder c Wbp, tenminste voor zover het de verwerking van de persoonlijke gegevens van de ontslagen medewerker betreft. Voor de gegevens van studenten, projectmedewerkers en privécontacten van de ontslagen medewerker, geldt hetgeen hierboven bij casus I vermeld is.

*Casus III: overlijden*

*Deze casus betreft dezelfde situatie als casus I, alleen nu komt medewerker A te overlijden. Hij is dus niet meer in staat om (email)bestanden over te dragen aan de leidinggevende of collega's.*

Voor gegevens van een overleden persoon geldt dat Wbp niet van toepassing is, tenzij de persoonsgegevens van de overleden persoon eveneens betrekking hebben op nog levende personen.[22] Voor de persoonsgegevens van de overleden medewerker geldt dus met name het goed werkgeverschap. Eventueel kan dit aangevuld en/of verduidelijkt zijn door bepalingen in de arbeidsovereenkomst, gedragscode of privacyreglement. Voor zover de (email)bestanden van de overleden medewerker noodzakelijke informatie bevatten voor de voortgang van taken van deze medewerker binnen de organisatie, zal de werkgever deze bestanden mogen verwerken om de taken van de overleden medewerker over te dragen aan andere medewerkers. Op grond van goed opdrachtgeverschap zal hij zich moeten beperken tot zakelijke bestanden die noodzakelijk zijn voor de voortgang van taken van de overleden medewerker; privébestanden moeten gerespecteerd worden en mogen niet worden verwerkt. Voor de verwerking van persoonsgegevens van anderen dan de overleden medewerker, die blijken uit de (email)bestanden van de overleden medewerker (studenten, projectmedewerkers, privécontacten van de overleden medewerker) geldt verder hetzelfde als vermeld bij casus I.

## Verstrekken van gegevens aan familie

*Casus IV: overlijden*

*Medewerker A is overleden. Zijn familieleden vragen de werkgever om de (email)bestanden van medewerker A aan hen te verstrekken.*

In principe is de Wet bescherming persoonsgegevens niet meer van toepassing op de gegevensverwerking van de persoonsgegevens van de overledene, tenzij deze eveneens betrekking hebben op nog levende personen. Dit zijn veelal de nabestaanden. De vraag daarbij is echter of de gegevens betrekking hebben op dezelfde nabestaanden als degenen die om de gegevens verzoeken. Indien ja, dan geven de nabestaanden dus als het ware toestemming voor de verstrekking van de persoonsgegevens van medewerker A, die betrekking hebben op henzelf. Indien nee, en hebben de gegevens tevens betrekking op andere nabestaanden, dan is de Wbp dus van toepassing op de verwerking van de persoonsgegevens van medewerker A, omdat zij mede van toepassing zijn op nog levende nabestaanden, anderen dan die om de gegevens verzoeken, en moet er dus sprake zijn van een van de verwerkingsgronden genoemd in artikel 8 Wbp. Dit zal waarschijnlijk alleen grond 8 onder f kunnen zijn: de belangenafweging waarbij het belang van de vrager zwaarder weegt dan het belang van degenen op wie de gegevens betrekking hebben. Echter, er spelen in deze situatie nog meer persoonsgegevens, namelijk die van de identificeerbare personen die voorkomen in de (email)bestanden van medewerker A. Ook hier is noodzakelijk dat er een legitiem doel is voor de verstrekking (in dit geval zal het doel zijn om de nabestaanden zaken van hun overleden dierbare terug te geven in een periode van rouw) en een legitieme grond. Ook hier zal de grond enkel artikel 8 onder f kunnen zijn (het zal lastig zijn de personen om toestemming te vragen, aangezien het zonder de bestanden in te zien, en dus persoonsgegevens te verwerken, niet mogelijk is te weten van wie toestemming gevraagd moet worden). Het is echter discutabel of het belang van de nabestaanden bij het verkrijgen van de (zakelijke) (email)bestanden van medewerker A, zwaarder weegt dan de privacybelangen van diegenen die op basis van deze bestanden identificeerbare personen zijn.

[22] Zie T. F. M. Hooghiemstra, *Tekst en toelichting Wet bescherming persoonsgegevens* ,derde druk, p. 36.

Wat hier uitkomst kan bieden is dat in een gedragscode een werkgever bepaalt dat een werknemer zijn privé(email)bestanden die hij op zijn werk bewaart, duidelijk moet etiketteren als privé. Wellicht dat een werkgever dan enkel de privébestanden kan overdragen aan de nabestaanden. Maar dan nog geldt de afweging of het belang van de nabestaanden om deze bestanden verstrekt te krijgen, wel zwaarder weegt dan het privacybelang van de personen die op basis van deze bestanden identificeerbaar zijn, en wiens gegevens dus verwerkt worden door deze bestanden aan andere nabestaanden te verstrekken. Nabestaanden zullen dus mogelijk een zwaarwegender belang moeten kunnen aantonen dan enkel 'het bevorderen van het rouwproces' om hun belang te laten wegen boven het privacybelang van de betrokken personen.

## Verstrekken van gegevens aan derden

*Casus V: auteursrechtclaim*

*De onderwijsinstelling het verzoek van een derde partij, namelijk stichting BREIN, om van een bij de instelling aangesloten persoon – een student of medewerker die IP-adres 012.345.678.901 gebruikt – de daarbij behorende NAW-gegevens (naam, adres, woonplaats) op te zoeken en te verstrekken, zodat BREIN deze persoon aansprakelijk kan stellen voor inbreuk op auteursrechten.*

In deze casus moeten we aansluiting zoeken bij de uitspraak die de Hoge Raad heeft gedaan in het arrest Lycos-Pessers (LJN AU4019) en de uitspraak van de voorzieningenrechter van de rechtbank Amsterdam in de zaak BREIN-UPC (LJN AY6903).Uit de zaak Lycos-Pessers blijkt dat een Internetaanbieder (ISP) zich, bij een verzoek om NAW-gegevens van een derde, de vraag moet stellen of de uiting (die aanleiding geeft tot het verzoek om de gegevens, in deze zaak ging het om laster) "onmiskenbaar" onrechtmatig is dan wel of de uiting onrechtmatig "zou kunnen zijn". Indien dit het geval is, zal de ISP de NAW-gegevens moeten verstrekken. Hierbij is wel de vraag van belang of de verzoeker de noodzakelijke adresgegevens op een minder ingrijpende wijze zou kunnen verkrijgen. Indien dit het geval is hoeft de ISP de gegevens niet te verstrekken. Engelfriet[23] omschrijft de test in Lycos-Pessers als een vierstappentoets om het verstrekken van persoonsgegevens aan een derde – de ISP – te rechtvaardigen:

1. het is voldoende aannemelijk dat de informatie, op zichzelf beschouwd, tegenover de derde onrechtmatig en schadelijk is;
2. de derde heeft een reëel belang bij de verkrijging van de NAW-gegevens;
3. het is aannemelijk dat er in het concrete geval geen minder ingrijpende mogelijkheid bestaat om de NAW-gegevens te achterhalen;
4. een afweging van de betrokken belangen van de ISP en degene op wie de NAW-gegevens betrekking hebben (voor zover kenbaar) valt uit in het voordeel van de ISP.

Dat de in Lycos-Pessers gevolgde redenering ook op gaat in gevallen van inbreuk op intellectuele eigendomsrechten, blijkt uit de zaak BREIN-UPC (LJN AY6903):

> "Ten eerste moet daarvoor voldoende aannemelijk zijn dat sprake is van inbreukmakend (onrechtmatig) handelen van de desbetreffende abonnees en ten tweede dient buiten redelijke twijfel te zijn dat degene(n) van wie de identificerende gegevens ter beschikking worden gesteld ook daadwerkelijk degenen zijn die zich aan dit handelen schuldig zouden hebben gemaakt. In dat geval kan het zo zijn dat de privacybelangen van de betrokkenen bij het geheim houden van hun gegevens moeten wijken voor het belang van de rechthebbenden om tegen het onrechtmatig handelen op te treden".

[23] http://www.iusmentis.com/auteursrecht/privacy/.

Als we deze jurisprudentie toepassen op de casus, dan is de onderwijsinstelling verplicht NAW-gegevens te verstrekken aan BREIN als de verzoeker kan aantonen dat een van de aan de onderwijsinstelling gelieerde IP-adressen betrokken is bij handelingen die onrechtmatig zouden kunnen zijn, tenzij de verzoeker deze gegevens op een eenvoudigere wijze kan verkrijgen. Indien gerede twijfel bestaat bij de onderwijsinstelling of er sprake is van handelen dat onrechtmatig kan zijn, kan de onderwijsinstelling afgifte van de gegevens weigeren, tot het moment dat de verzoeker deugdelijk bewijs (bijvoorbeeld een rechterlijke uitspraak) kan overleggen waaruit nadrukkelijk het onrechtmatig karakter van het handelen blijkt.

Mocht de onderwijsinstelling – bij gerede twijfel – weigeren en vervolgens door BREIN alsnog via de rechter worden gevraagd de NAW-gegevens te leveren, dan hoeft, ook als BREIN in het gelijk wordt gesteld, de instelling alleen de eigen proceskosten te betalen, niet die van BREIN of een schadevergoeding (Rechtbank ’s-Gravenhage 5 januari 2007, BREIN-KPN, LJN: AZ5678).

# Verstrekken van gegevens (overheid)

## Verstrekken van opgeslagen gegevens aan politie en justitie

### Omschrijving

Het verstrekken van gegevens aan politie en justitie komt misschien niet vaak maar toch regelmatig voor, vooral van identificerende gegevens. Het is aan te raden een eenheid en/of functionaris aan te wijzen aan wie alle vragen van politie of justitie over gegevensverstrekking worden doorgeleid. Verstrekking kan op basis van vrijwilligheid of een bevel. Daarom moet eerst duidelijk zijn of politie of justitie verzoekt om de gegevens of beveelt om gegevens uit te leveren.

Het strafrecht maakt onderscheid tussen verschillende typen gegevens. Ten eerste bestaan er verschillende regimes voor gegevens die met communicatie te maken hebben (zoals email en telefonie), en overige gegevens. Ten tweede bestaat er een onderscheid tussen gegevens naar mate van gevoeligheid: identificerende gegevens, 'gewone' gegevens en gevoelige gegevens (zie daarover ook hfd. 2, Wet bescherming persoonsgegevens (Wbp)). Het opvragen van identificerende gegevens mag door de politie zelf, het opvragen van alle andere gegevens kan alleen op basis van een bevel van justitie (officier van justitie, al dan niet met machtiging van een rechter-commissaris).

### Relevante wet- en regelgeving en jurisprudentie

- Wetboek van Strafvordering, art. 126nc t/m 126nh (algemene gegevens)
- Wetboek van Strafvordering, art. 126n, 126na, 126ng (communicatiegegevens)
- Besluit vorderen gegevens telecommunicatie, *Staatsblad* 2004, 394.

Naast de vermelde bepalingen bestaan er ook vrijwel identieke bepalingen voor de opsporing in het kader van georganiseerde misdaad en bij aanwijzingen van terroristische misdrijven. Die komen in de context van onderwijsinstellingen zo weinig voor dat we die hier buiten beschouwing laten.

#### *Jurisprudentie*

- Hoge Raad 5 september 2006, LJN AX7473 (naast verplichte medewerking bestaat ook de mogelijkheid van vrijwillige verstrekking op basis van art. 8 onder f Wbp)

### Juridische voorwaarden

#### *A. Algemene gegevens (d.w.z. niet communicatie-gerelateerd):*

1. *Identificerende gegevens*: deze mogen in geval van elk misdrijf[24] worden opgevraagd door een politieambtenaar, in het belang van een strafrechtelijk onderzoek; onder identificerende gegevens vallen naam-adres-woonplaats, geboortedatum en geslacht en administratieve kenmerken (zoals een personeels- of studentennummer) (art. 126nc WvSv). Het gaat bovendien alleen om gegevens 'die anders dan ten behoeve van persoonlijk gebruik' worden

[24] Het strafrecht onderscheidt strafbare feiten in misdrijven en overtredingen. Misdrijven (art. 92-420 Wetboek van Strafrecht) zijn de wat ernstiger strafbare feiten, overtredingen (art. 424-476 Wetboek van Strafrecht, en bijzondere wetten) zijn lichtere strafbare feiten.

verwerkt, dus om beroeps- of bedrijfsmatig verwerkte gegevens (niet het privé-adresboek van de systeembeheerder).

2. *Gewone gegevens*: deze mogen worden opgevraagd door een officier van justitie in het belang van een strafrechtelijk onderzoek, bij verdenking van een misdrijf dat wordt genoemd in art. 67 lid 1 WvSv, d.w.z. misdrijven waarvoor voorlopige hechtenis mogelijk is – meestal misdrijven waarop een maximumstraf staat van 4 jaar of meer gevangenisstraf, maar ook enkele specifiek genoemde misdrijven, waaronder bijna alle vormen van computercriminaliteit (art. 126nd WvSv). Het mag daarbij ook gaan om gegevens die voor persoonlijk gebruik worden verwerkt, dus in principe ook dagboekaantekeningen en boodschappenlijstjes die in computers van medewerkers of studenten liggen opgeslagen. Het bevel mag echter niet vragen om gevoelige persoonsgegevens (zoals ras, geloof of gezondheid); daarvoor is het volgende artikel van toepassing. Ook mag niet de inhoud van communicatie, zoals email, worden opgevraagd, daarvoor is een apart artikel bedoeld (zie hieronder, onder B.3).

3. *Gevoelige gegevens*: dit zijn gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven of lidmaatschap van een vakvereniging. Deze gegevens mogen worden opgevraagd door een officier van justitie, mits zij machtiging heeft van een rechter-commissaris en mits het dringend nodig is voor een strafrechtelijk onderzoek (dit is een zwaardere eis dan het 'belang van het onderzoek' bij de andere gegevens), waarbij het moet gaan om een ernstig misdrijf, dat wil zeggen een misdrijf dat wordt genoemd in art. 67 lid 1 WvSv (zie onder Gewone gegevens) dat bovendien een ernstige inbreuk op de rechtsorde maakt (art. 126nf WvSv). Ook bij dit bevel bestaat geen beperking tot bedrijfsmatige gegevens; ook privégegevens kunnen worden opgevraagd, mits dat dringend nodig is voor het strafrechtelijk onderzoek.

Bij al deze bevoegdheden bestaan nog twee algemene beperkingen aan wie het bevel kan worden gegeven:

- het bevel kan worden gericht aan iemand die vermoedelijk toegang heeft tot de genoemde gegevens; voor onderwijsinstellingen zal dat meestal een systeembeheerder zijn, maar politie of justitie kan het bevel ook richten aan de organisatie als geheel (die immers ook als rechtspersoon toegang heeft tot de gegevens), waarbij de organisatie dan zelf de juiste persoon moet aanwijzen om de gegevens te verstrekken;

- het bevel mag niet worden gegeven aan de verdachte zelf, bijvoorbeeld niet aan een systeembeheerder die wordt verdacht van het onderhavige misdrijf; ook mag degene die het bevel krijgt zich verschonen (dus niet meewerken) als zij daarmee belastend materiaal zou aanleveren voor zichzelf, haar echtgeno(o)t(e) of een naast familielid (tot in de derde graad).

### *B. Communicatie-gerelateerde gegevens:*

Onder communicatie-gerelateerde gegevens vallen gegevens die samenhangen met een communicatiedienst, d.w.z. een dienst die 'de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk [d.w.z. een computer], of gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst' (art. 126la WvSv). Onderwijsinstellingen bieden meestal aan hun medewerkers en studenten zulke diensten aan, in de vorm van emailfaciliteiten en interne telefoonnetwerken. Hoewel onderwijsinstellingen en bedrijven met interne communicatienetwerken geen aanbieders van openbare telecommunicatie zijn (en dus niet onder de Telecommunicatiewet vallen), worden zij sinds 2006 (Wet computercriminaliteit II) wel volgens het strafrecht gekwalificeerd als 'communicatieaanbieders' (art. 126la WvSv). Zij moeten dan ook meewerken aan het verstrekken van communicatiegegevens en aftappen.

Ook hierbij worden verschillende gegevens onderscheiden:

1. *Gebruikersgegevens* (vergelijkbaar met de identificerende gegevens hierboven): deze mogen in geval van elk misdrijf worden opgevraagd door een politieambtenaar, in het belang van een strafrechtelijk onderzoek; onder identificerende gegevens vallen naam-adres-woonplaats, nummer en soort dienst van de gebruiker (art. 126na WvSv). Onder nummer valt bijvoorbeeld het telefoonnummer, IP-adres en emailadres van de gebruiker.

2. *Verkeersgegevens*: deze mogen worden opgevraagd door een officier van justitie in het belang van een strafrechtelijk onderzoek, bij verdenking van een misdrijf dat wordt genoemd in art. 67 lid 1 WvSv (zie boven onder A.2) (art. 126n WvSv). Verkeersgegevens zijn meta-gegevens over communicatiegebruik: wie heeft met wie, op welk tijdstip, hoe lang gebeld of gemaild; op welk tijdstip logde iemand in of uit. De precieze verkeersgegevens die onder dit bevel vallen staan vermeld in het Besluit vorderen gegevens telecommunicatie. Onder het opvragen van verkeersgegevens valt ook het opvragen van gebruikersgegevens, dat kan in één bevel op basis van art. 126n WvSv. Het bevel mag echter niet vragen om de *inhoud* van communicatie; daarvoor is het volgende artikel van toepassing.

3. *Inhoud*: de inhoud van communicatie – de body maar ook het onderwerpsveld van een emailbericht, de inhoud van een telefoongesprek – geniet extra bescherming vanwege het grondwettelijke telecommunicatiegeheim. Daarom gelden voor het vorderen van communicatie-inhoud (art. 126ng lid 2 WvSv) de voorwaarden die vergelijkbaar zijn met die voor het vorderen van gevoelige gegevens (zie hierboven). Bovendien mag alleen communicatie-inhoud worden opgevraagd die van of voor de verdachte is, of over de verdachte of het misdrijf gaat.

### *Juridische aandachtspunten*

1. Bij *vrijwillige* verstrekking (dus een verzoek) kan de functionaris zelf bepalen, op basis van de politie-informatie, of zij meewerkt of niet. Meestal gaat het om persoonsgegevens, zodat dan artikel 8 onder f Wet bescherming persoonsgegevens van toepassing is: de functionaris beoordeelt dan of het belang van de verstrekking zwaarder weegt dan het privacybelang van de betrokkene (degene op wie de persoonsgegevens betrekking hebben). Deze verstrekking valt onder het civiele recht en kan eventueel door de betrokkene worden bestreden voor de rechter als deze vindt dat de gegevens onterecht zijn verstrekt.

2. Bij *verplichte* verstrekking (dus een bevel) moet de functionaris normaliter gewoon meewerken. Het is niet de bedoeling dat de functionaris zelf gaat beoordelen of het bevel wel aan alle wettelijke eisen voldoet. Zij kan ook niet aansprakelijk worden gehouden voor de verstrekking, omdat er immers van een ambtelijk bevel sprake is (daarop is de grondslag van art. 8 onder c Wbp van toepassing). De functionaris dient alleen te letten op evidente fouten in het bevel, zoals een bevel van een politieambtenaar (in plaats van een officier van justitie) om andere dan identificerende gegevens te verstrekken, of een bevel om medische gegevens te verstrekken zonder machtiging van de rechter-commissaris. Als er praktische fouten zitten in het bevel (bijvoorbeeld gegevens bij een niet-bestaand studentnummer), kan de functionaris het beste overleggen met de politieambtenaar of officier welke gegevens precies bedoeld worden.

3. De vordering moet normaliter *schriftelijk* worden gedaan. Hiervoor worden standaard-formulieren gebruikt. In de vordering moet worden vermeld:

4. indien bekend, de naam of anders een zo nauwkeurig mogelijke aanduiding van de persoon of de personen over wie gegevens worden gevorderd;

    a. een zo nauwkeurig mogelijke aanduiding van de gegevens die worden gevorderd (zie punt 5);
    b. een aanduiding van de termijn waarbinnen en de manier waarop de gegevens moeten worden verstrekt;
    c. de titel van de vordering.

5. In zeer urgente gevallen (het wetboek spreekt van ‘dringende noodzaak’) kan de vordering *mondeling* worden gedaan. De opsporingsambtenaar of officier van justitie moet dan wel binnen drie dagen na de vordering alsnog de vordering schriftelijk toesturen.

6. De gegevens moeten voldoende *specifiek* worden aangeduid. Hoe specifiek hangt af van de context. Het moet in elk geval voldoende duidelijk zijn voor de functionaris welke gegevens zij moet opzoeken en verstrekken; er mag weinig keuzevrijheid over blijven. Voldoende specifiek is bijvoorbeeld: alle bestanden die student Jan Jansen op 4 februari 2011 op de server heeft bewerkt of opgeslagen. Of: alle MP3-bestanden die medewerker Pietersen op zijn harde schijf heeft opgeslagen. Niet voldoende specifiek is: alle mails van medewerker Klaassen die over de boekhouding gaan (dan moet de functionaris namelijk interpreteren wanneer iets over ‘de boekhouding’ gaat). Wel kan: alle mails van Klaassen waarin het woord ‘boekhouding’ of ‘boeken’ in het onderwerpsveld staat. Verder is het niet de bedoeling dat een sleepnet wordt uitgegooid (‘de namen van alle studenten die illegale muziek uploaden’). Ook moeten de gevorderde gegevens proportioneel zijn in de context van het misdrijf; daarover kan de functionaris echter moeilijk oordelen, dus alleen bij evidente visexpedities of overvraging zou de functionaris kunnen weigeren.

7. Politie en justitie bepalen de vorm waarin de gegevens worden geleverd. Het is niet de bedoeling dat de functionaris gegevens moet bewerken (bijvoorbeeld bestanden koppelen) alvorens ze te overhandigen; wel kan omzetting in een bepaald formaat worden gevraagd.

8. Als gegevens *versleuteld* zijn – bijvoorbeeld opgeslagen bestanden van een medewerker – kan justitie vorderen dat deze worden ontsleuteld (art. 126nh WvSv). Dat kan echter alleen worden gevraagd van iemand die vermoedelijk de wijze van versleuteling (lees: de decryptiesleutel of het wachtwoord waarmee deze is beveiligd) kent, en dat zal meestal niet het geval zijn bij gegevens die door studenten of medewerkers zelf zijn versleuteld. Het mag dan natuurlijk wel aan die student of medewerker worden gevraagd, maar niet als deze zelf verdachte is (vanwege het beginsel van niet-meewerken aan de eigen veroordeling).

### *Juridische problemen en onduidelijkheden*

- Het is niet duidelijk wanneer een vordering precies ‘gevoelige gegevens’ betreft. Het is duidelijk wanneer justitie gegevens vordert over ‘alle Marokkaanse studenten’ of over ‘wie er op 28 januari bij de eucharistieviering in de aula aanwezig was’, of de vraag stelt of student Jansen bij de bedrijfspsycholoog in behandeling is. Maar het is minder duidelijk wanneer bestanden worden opgevraagd waarin mogelijk – maar niet zeker – dergelijke gegevens staan. Wij gaan ervan uit dat het neerkomt op een waarschijnlijkheidsinschatting: als er een redelijke verwachting is dat opgevraagde gegevens mede gevoelige persoonsgegevens (bijvoorbeeld medische of etnische gegevens) omvatten, dan moet er een bevel liggen om gevoelige gegevens te vorderen. Wanneer de kans op dergelijke gegeven echter klein is, mogen ze via de

gewone bevoegdheid worden opgevraagd; eventuele gevoelige gegevens die daarbij zitten gelden dan als bijvangst.

- Ook nader onderzoek vergt de vraag of een foto (bijvoorbeeld op een universiteitspas) onder een gevoelig persoonsgegeven valt (aangezien er soms etnische afkomst of geloof, of bepaalde medische condities, op kunnen worden afgelezen).

## Verstrekken van toekomstige gegevens aan politie en justitie

### Omschrijving

Naast het opvragen van bestaande, opgeslagen, gegevens, kan justitie ook bevel dat toekomstige gegevens worden verstrekt. Dit houdt in dat de onderwijsinstelling, vanaf het tijdstip van de vordering en voor de duur van de vordering, de aangeduide gegevens op het moment van ontstaan/verwerking vastlegt en vervolgens verstrekt aan justitie. Die verstrekking kan aan het eind van de gevraagde periode, of periodiek tussendoor, maar justitie kan ook bevelen de gegevens 'direct na de verwerking' (dus *real-time*) door te geleiden.

### Relevante wet- en regelgeving en jurisprudentie

- Wetboek van Strafvordering, art. 126ne (algemene gegevens)
- Wetboek van Strafvordering, art. 126n (communicatiegegevens)

### Juridische voorwaarden

1. Voor *algemene* gegevens: dit kan onder dezelfde voorwaarden als het bevel tot verstrekking van gewone gegevens (zie boven, Verstrekken van opgeslagen gegevens aan politie en justitie, A.2), maar alleen voor gegevens die beroeps- of bedrijfsmatig worden verwerkt. De vordering kan voor maximaal vier weken gelden, maar deze termijn kan telkens met vier weken worden verlengd (er zit dus geen absolute limiet aan de totale periode). Wanneer gegevens in *real-time* moeten worden doorgeleverd aan justitie, heeft de officier van justitie daarvoor een machtiging van de rechter-commissaris nodig.
2. Voor *communicatiegegevens*, d.w.z. verkeersgegevens: hiervoor gelden dezelfde voorwaarden als bij de verstrekking van verkeersgegevens (zie boven, Verstrekken van opgeslagen gegevens aan politie en justitie, B.2). De termijn is maximaal drie maanden. Deze termijn is niet-verlengbaar. De praktijk bij telecombedrijven is dat verkeersgegevens in real-time moeten worden doorgeleverd; of justitie dat ook eist bij niet-openbare communicatieaanbieders, zoals onderwijsinstellingen, is bij de onderzoekers niet bekend.

## Verstrekken van gegevens aan bijzondere opsporingsdiensten en toezichthouders

### Omschrijving

Evenals politie en justitie kunnen ook bijzondere opsporingsdiensten en toezichthouders gegevens opvragen. Er zijn sectorale opsporingsdiensten, zoals de FIOD voor de opsporing van fiscale en economische delicten en de SIOD voor opsporing van fraude met werk en inkomen. Toezichthouders zijn bestuursorganen die belast zijn met handhaving van wet- en regelgeving,

zoals het CBP voor de Wet bescherming persoonsgegevens, de NMa voor mededingingswetgeving, de OPTA voor telecommunicatieregels en Inspectie van het Onderwijs voor het onderwijs.[25]

## Relevante wet- en regelgeving en jurisprudentie

- Algemene wet bestuursrecht (Awb), art. 5:11 t/m 5:20
- sectorale wetten, zoals:
  - Algemene wet op de rijksbelastingen
  - Wet op het hoger onderwijs en wetenschappelijk onderzoek
  - Wet werk en inkomen
  - Zorgverzekeringswet
- wetten en regels betreffende specifieke opsporingsdiensten en toezichthouders, zoals
  - Regeling toedeling bepaalde opsporingstaken SIOD en FIOD-ECD
  - Wet Onafhankelijke post- en telecommunicatieautoriteit
  - Wet op het onderwijstoezicht

## Juridische voorwaarden

1. *Bijzondere opsporingsdiensten*. De bevoegdheden van bijzondere opsporingsdiensten, zoals de FIOD en de SIOD, zijn geregeld in de desbetreffende sectorale wetgeving. (De Wet op de bijzondere opsporingsdiensten bevat geen specifieke bevoegdheid tot het opvragen van gegevens.)
   Volgens art. 47 van de Algemene wet op de rijksbelastingen (Awr) moet eenieder, dus ook een onderwijsinstelling, de belastinginspecteur alle gegevens en inlichtingen verstrekken die voor de belastingheffing van belang kunnen zijn. Daartoe moet men ook de relevante boeken, bescheiden en computerbestanden beschikbaar stellen aan de inspecteur. Dat geldt ook voor derden die deze bescheiden of bestanden onder zich hebben (art. 48). De gegevens moeten ‘duidelijk, stellig en zonder voorbehoud’ worden verstrekt, op de wijze en binnen de termijn die de inspecteur aangeeft; de inspecteur mag daarbij de gegevens kopiëren (art. 49). Medewerking is verplicht, op straffe van maximaal zes maanden gevangenisstraf (art. 68).

2. *Toezichthouders*. Toezichthouders zijn bestuursorganen en vallen onder de Algemene wet bestuursrecht. Deze wet kent algemene bevoegdheden toe aan toezichthouders, die gedefinieerd worden als ‘een persoon, bij of krachtens wettelijk voorschrift belast met het houden van toezicht op de naleving van het bepaalde bij of krachtens enig wettelijk voorschrift’ (art. 5:12 Awb). Toezichthouders mogen:

   a. binnentreden, desnoods met geweld, bij onderwijsinstellingen (5:15),
   b. inlichtingen vorderen (5:16) en
   c. zakelijke gegevens en bescheiden inzien en kopiëren (5:17).

   Bij uitoefening van deze bevoegdheden moet de toezichthouder zich desgevraagd legitimeren (5:12) en zich beperken tot wat redelijkerwijs nodig is voor de desbetreffende taak (5:13). De

[25] Nederland kent erg veel toezichthouders; zie voor een overzicht http://nl.wikipedia.org/wiki/Toezichthouder_(overheid).

onderwijsinstelling is verplicht alle naar redelijke maatstaven nodige medewerking te verlenen (5:20).

### Juridische aandachtspunten

De bevoegdheden van toezichthouders worden bij specifieke wetten geregeld en verschillen in nuances, al hebben toezichthouders bijna altijd ruime bevoegdheden om gegevens op te vragen. De toezichthouders kunnen op basis van de Algemene wet bestuursrecht bevoegdheden gebruiken om hun taken uit te oefenen, inclusief het vorderen van inlichtingen en inzien van gegevens en bescheiden. De reikwijdte van deze bevoegdheid is niet verder ingekaderd – in principe kunnen dus alle gegevens worden gevorderd – behalve door de algemene proportionaliteitseis van art. 5:13: 'Een toezichthouder maakt van zijn bevoegdheden slechts gebruik voor zover dat redelijkerwijs voor de vervulling van zijn taak nodig is.'

Soms regelt de wet echter ook specifieke taken en daarbij behorende bevoegdheden. Zo mag de Onderwijsinspectie alle bevoegdheden uit de Awb inzetten voor het toezicht op de naleving van onderwijswetten, zoals de Wet op het hoger onderwijs en wetenschappelijk onderzoek. Daarnaast bepaalt art. 9 van de Wet op het onderwijstoezicht dat de Onderwijsinspectie voor het uitoefenen van andere taken, zoals het beoordelen en het bevorderen van de kwaliteit van het onderwijs, de artikelen 5:12 tot en met 5:17 en 5:20 Awb van toepassing zijn.

Twee voorbeelden uit de socialezekerheidswetgeving: art. 63 Wet werk en bijstand bepaalt dat de werkgever verplicht is aan het college van burgemeester en wethouders alle inlichtingen te verstrekken die nodig zijn in het kader van een bijstandsverzoek van een werknemer, ex-werknemer of potentieel toekomstige werknemer. En volgens art. 88 Zorgverzekeringswet is de werkgever verplicht om aan onder andere zorgverzekeraars, het College zorgverzekeringen of het college van B&W kosteloos alle inlichtingen, waaronder persoonsgegevens, te verstrekken die nodig zijn voor de uitvoering van zorgverzekeringen of van de Zorgverzekeringswet.

Het is dus van belang bij specifieke toezichthouders om de desbetreffende wetgeving te raadplegen om de precieze reikwijdte van de bevoegdheden te kennen.

## Verstrekken van gegevens aan inlichtingen- en veiligheidsdiensten

### Omschrijving

Ook inlichtingen- en veiligheidsdiensten (de AIVD en MIVD) kunnen gegevens opvragen. Daarbij lijkt echter geen sprake van verplichte medewerking.

### Relevante wet- en regelgeving en jurisprudentie

- Wet op de inlichtingen- en veiligheidsdiensten 2002, art. 17

### Juridische voorwaarden

De AIVD en MIVD mogen bij de uitoefening van hun taak gegevens opvragen bij:

a. bestuursorganen, ambtenaren en voorts een ieder die geacht wordt de benodigde gegevens te kunnen verstrekken;
b. de verantwoordelijke voor een gegevensverwerking (dat wil zeggen degene die, volgens art. 1 Wbp, het doel en de middelen van een verwerking van persoonsgegevens bepaalt).

In het geval onder b) moet de AIVD- of MIVD-ambtenaar zich bij de geadresseerde legitimeren met een door het hoofd van de dienst verstrekt legitimatiebewijs. Op de volgens b) verstrekte gegevens is de Wet bescherming persoonsgegevens niet van toepassing (art. 17 onder 3 Wiv 2002).

## Juridische aandachtspunten

1. Bij onderwijsinstellingen kunnen in principe bij iedereen alle mogelijke gegevens worden opgevraagd op basis van a) (‘een ieder die geacht wordt de benodigde gegevens te kunnen verstrekken’). Elke individuele medewerker kan worden gevraagd bestanden en gegevens waar zij toegang toe heeft, te verstrekken. Als het persoonsgegevens betreft waarvoor de instelling verantwoordelijk is – bijvoorbeeld gegevens over medewerkers en studenten, maar ook bestanden van medewerkers en studenten op de servers en computers die de instelling ter beschikking stelt – is de situatie onder b) van toepassing. Omdat in die situatie de Wbp buiten toepassing wordt gesteld, is de instelling niet aansprakelijk voor het verstrekken van persoonsgegevens (behalve in het zeer onwaarschijnlijke geval de verstrekking een onrechtmatige daad (art. 6:162 BW) zou opleveren).

2. De medewerking is *vrijwillig*. De formulering in de Memorie van Toelichting (*Kamerstukken II* 1997/98, 25 877, nr. 3, p. 23) suggereert dat de houder van de gegevens zelf besluit om wel of niet te verstrekken.