Privacy op de werkvloer: van A tot GDPR

Vrije visie, eigen stem

ACLVB
LIBERALE VAKBOND

Privacy op de werkvloer: van A tot GDPR

Vrije visie, eigen stem

ACLVB
LIBERALE VAKBOND

V.U.: Mario Coppens, Koning Albertlaan 95, 9000 Gent. 10/2022

INHOUDSOPGAVE

Privacy op het werk is een thema dat steeds belangrijker wordt. Het toenemende economische en maatschappelijke belang van (informatie)technologie is hier niet vreemd aan. De inwerkingtreding van de GDPR in 2018 gaf een extra duwtje in de rug en plaatste privacy hoog op de agenda. Er blijven echter tot op vandaag veel vragen over de toepassing van het recht op privacy in de specifieke context van de arbeidsrelatie.
In deze brochure vindt u een antwoord op de belangrijkste van deze vragen.

1. Historiek

1.1 Het recht op privacy

Het recht op bescherming van het privé-leven is een aloud recht. De vroegste vorm ervan hield verband met de onschendbaarheid van de woning. In het oudste gekende wetboek, de codex van Hammurabi (ca. 1780 v.Chr.), stond de doodstraf op het zich ongeoorloofd toegang verschaffen tot iemands woning. In de oorspronkelijk **Belgische Grondwet** van 1831 vond het recht op privacy in eerste instantie uitdrukking in het recht op de onschendbaarheid van de woning (art. 15) en het briefgeheim (art. 29). Met het **Europees Verdrag voor de Rechten van de Mens (EVRM)** van 1950 – dat in de Belgische rechtsorde rechtstreekse werking heeft – kreeg het recht op privacy in bredere zin vorm:

> **ARTIKEL 8**
> 1. Een ieder heeft het recht op respect voor zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.

Sinds 1994 is dezelfde breed geformuleerde bepaling opgenomen in de Belgische Grondwet:

> **ARTIKEL 22**
> Ieder heeft recht op eerbiediging van zijn privé-leven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald. De wet, het decreet of de in artikel 134 bedoelde regel waarborgen de bescherming van dat recht.

1.2 De bescherming van persoonsgegevens

Met de opkomst van de eerste voor het brede publiek beschikbare digitale communicatie- en informatiemiddelen in de jaren '70 en '80 ontstond de nood aan specifieke wetgeving voor de **verwerking van persoonsgegevens**. Door de nieuwe technologie konden persoonsgegevens immers veel makkelijker gedeeld en bewaard worden, wat een verhoogd risico inhield voor de privacy van de personen op wie deze gegevens betrekking hadden.

Het **Verdrag nr. 108 van de Raad van Europa** van 1981 legde de grondslag voor alle latere wetgeving ter bescherming van de privacy bij verwerking van persoonsgegevens. De basisprincipes van dit verdrag werden in België al vroeg omgezet in de **Privacywet** van 1992.[1] Het Verdrag nr. 108 werd in 1995 verder geconcretiseerd op Europees niveau in **Richtlijn 95/46/EG**.[2] Deze richtlijn maakte in 2018 plaats voor **Verordening 2016/679**, beter bekend als de **GDPR** (General Data Protection Regulation) of **AVG** (Algemene Verordening Gegevensverwerking).[3] De Belgische privacywet werd aangepast aan deze verordening.[4]

1.3 Het begrip 'verwerking van persoonsgegevens'

Vandaag worden het recht op privacy en de GDPR vaak in één adem genoemd. Het recht op privacy is echter meer dan de GDPR alleen. De GDPR beschermt immers enkel de privacy wanneer een verwerking van persoonsgegevens plaatsvindt. De GDPR definieert een **verwerking** als volgt:

> een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens

Persoonsgegevens worden als volgt gedefinieerd:

> alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon

1 Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.
2 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.
3 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.
4 Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

Wanneer er geen verwerking van persoonsgegevens plaatsvindt is de GDPR niet van toepassing. In die situaties wordt het recht op privacy door de andere hierboven besproken rechtsbronnen beschermd.

2. GDPR

2.1 Nieuw?

2.1.1 Van preventie naar repressie

De inwerkingtreding van de GDPR heeft het thema privacy hoog op de agenda geplaatst. De evidente verklaring hiervoor zijn de **hoge boetes** die kunnen worden opgelegd bij een overtreding van de verordening. Voor de zwaarste overtredingen kan de bevoegde toezichthoudende autoriteit administratieve geldboeten opleggen tot **20 miljoen euro** of voor een onderneming, tot **4% van de totale wereldwijde jaaromzet** in het voorgaande boekjaar, indien dit cijfer hoger is.

Deze hoge boetes passen in een algemene paradigmashift die door de GDPR werd ingeluid van een **preventief** kader naar een **repressief** kader. Onder de oude Richtlijn moest iedere (geautomatiseerde) verwerking van persoonsgegevens vooraf gemeld worden bij de toezichthoudende autoriteit. De autoriteit hield hiervan een openbaar verwerkingsregister bij. Onder de GDPR werd deze logica omgedraaid: verwerkers van persoonsgegevens houden zelf een verwerkingsregister bij, dat niet openbaar is.
Ze moeten de rechtmatigheid van de verwerking kunnen verantwoorden, maar er is geen aanmeldingsplicht. Het risico op hoge boetes zou verwerkers ervan moeten weerhouden de verordening te overtreden.

2.1.2 De basisprincipes blijven onveranderd

De basisprincipes voor een correcte gegevensverwerking die opgenomen zijn in artikel 5 van de GDPR, zijn nog nagenoeg ongewijzigd ten opzichte van deze uit het Verdrag nr. 108 en Richtlijn 95/46/EG. De **beginselen uit dit artikel vormen de ruggengraat en kern van de verordening** en zullen in deze brochure ook als leidraad dienen:

> **ARTIKEL 5**
> 1. Persoonsgegevens moeten:
>
> a) worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is **('rechtmatigheid, behoorlijkheid en transparantie')**;

b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd **('doelbinding')**;

c) toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt **('minimale gegevensverwerking')**;

d) juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren **('juistheid')**;

e) worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, lid 1, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen **('opslagbeperking')**;

f) door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging **('integriteit en vertrouwelijkheid')**.

2. De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 en kan deze aantonen **('verantwoordingsplicht')**.

2.1.3 Andere vernieuwingen

Toch heeft de GDPR nog enkele belangrijke en minder belangrijke vernieuwingen geïntroduceerd:

- De definitie van **toestemming** als grond voor een rechtmatige gegevensverwerking werd aangescherpt. Voortaan wordt deze gedefinieerd als 'elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling (NIEUW) hem betreffende verwerking van persoonsgegevens aanvaardt'.
- Er werden twee nieuwe gegevenstypen toegevoegd die een bijzondere bescherming genieten: **biometrische** en **genetische** gegevens.
- Het **recht op overdraagbaarheid** van gegevens werd geïntroduceerd. Dit houdt het recht in voor iedere betrokkene om de hem betreffende persoonsgegevens, die hij aan een verwerkingsverantwoordelijke heeft verstrekt, in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen en die gegevens aan een andere verwerkingsverantwoordelijke over te dragen.
- Het **recht op een kopie** van de verwerkte persoonsgegevens.
- Het recht om niet te worden onderworpen aan **een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit** waaraan rechtsgevolgen zijn verbonden of dat de persoon waarop ze betrekking hebben anderszins in aanmerkelijke mate treft.
- De verplichte opmaak van een **gegevensbeschermingseffectbeoordeling** wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.
- Voor verwerkers die op een zekere schaal aan gegevensverwerking doen of wanneer gevoelige persoonsgegevens worden verwerkte, de verplichte aanstelling van een **functionaris voor gegevensbescherming ('DPO')**.
- Op basis van de GDPR kunnen **ook verwerkers**, en niet enkel verwerkingsverantwoordelijken, **aansprakelijk** gesteld worden voor een foutieve verwerking wanneer bij de verwerking niet is voldaan aan de specifiek tot verwerkers gerichte verplichtingen van de verordening of buiten dan wel in strijd met de rechtmatige instructies van de verwerkingsverantwoordelijke is gehandeld.
- Een **verplichte melding van een inbreuk** in verband met persoonsgegevens (bv. gegevenslek) bij de toezichthoudende autoriteit binnen de 72 uur, voor zover de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.
- Introductie van de principes **gegevensbescherming door ontwerp ('by design')** en **door standaardinstellingen ('by default').**

2.2 Rechtmatigheid, behoorlijkheid en transparantie

2.2.1 Rechtmatigheid

Als allereerste voorwaarde moet iedere verwerking een rechtsgrondslag hebben. Deze kan volgens de GDPR gevonden worden in één van volgende oorzaken (art. 6):

a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
b) de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
d) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

VOORBEELDEN

- De Spaanse gegevensbeschermingsautoriteit (hierna: GBA) beboette een werkgever die een werknemer ontsloeg op basis van videobeelden van deze werknemer die hij op onrechtmatige wijze had bekomen.
- Dezelfde GBA gaf een boete aan een vakbond die zonder toestemming van de betrokkene persoonlijke gegevens van haar deelde met 400 vakbondsleden.
- Een Hongaarse werknemer had bij de lokale overheid mistoestanden in zijn bedrijf aangekaart. De werkgever had hier lucht van gekregen en toen hij zich bij diezelfde overheid informeerde, deelde deze aan de werkgever de naam van de klokkenluider mee. Uiteraard had de overheid hiervoor geen rechtmatige aanleiding.

2.2.1.1 Gevoelige gegevens

De verwerking van bepaalde **bijzondere categorieën van persoonsgegevens** (gevoelige gegevens) is in principe verboden:

> Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.

Slechts in een beperkt aantal in de GDPR opgesomde gevallen kan het gebruik van dergelijke gegevens gerechtvaardigd worden.

> **VOORBEELD**
>
> - De Cypriotische GBA legde een bedrijf een hoge boete op voor het ongerechtvaardigd gebruik van gezondheidsgegevens van werknemers. Het bedrijf evalueerde de duur en frequentie van afwezigheden wegens ziekte aan de hand van de zogenaamde 'Bradford-factor'. Volgens deze managementtheorie zouden frequente korte afwezigheden de arbeidsorganisatie meer verstoren dan minder frequente langere afwezigheden. Het profileren van werknemers op basis van de duur en frequentie van hun ziektes werd als disproportioneel beschouwd door de bevoegde GBA.

2.2.1.2 Toestemming in arbeidsrelaties

Toestemming is geen evidente rechtsgrond in de verhouding werkgever werknemer. De werkgever moet immers kunnen aantonen dat de toestemming volledig vrijwillig was. Dit is niet evident gezien het machtsonevenwicht dat eigen is aan deze verhouding. Overweging 43 van de GDPR stelt immers dat:

> (43)
> Om ervoor te zorgen dat toestemming vrijelijk wordt verleend, mag toestemming geen geldige rechtsgrond zijn voor de verwerking van persoonsgegevens in een specifiek geval wanneer er sprake is van een duidelijke wanverhouding tussen de betrokkene en de verwerkingsverantwoordelijke, met name wanneer de verwerkingsverantwoordelijke een overheidsinstantie is, en dit het onwaarschijnlijk maakt dat de toestemming in alle omstandigheden van die specifieke situatie vrijelijk is verleend. De toestemming wordt geacht niet vrijelijk te zijn verleend indien geen afzonderlijke toestemming kan worden gegeven voor verschillende persoonsgegevensverwerkingen ondanks het feit dat dit in het individuele geval passend is, of indien de uitvoering van een overeenkomst, daaronder begrepen het verlenen van een dienst, afhankelijk is van de toestemming ondanks het feit dat dergelijke toestemming niet noodzakelijk is voor die uitvoering.

De Groep Gegevensverwerking artikel 29 (vandaag 'EDPB', de Europese toezichthouder inzake privacy) drukt het als volgt uit (Advies 2/2017):

> **"Werknemers verkeren bijna nooit in een positie waarbij ze vrij zijn hun toestemming te verlenen**, te weigeren of in te trekken, gezien hun afhankelijkheid als gevolg van de verhouding tussen werkgever en werknemer. Door deze ongelijke machtsverhouding kunnen werknemers enkel in uitzonderlijke omstandigheden, wanneer er geen enkel gevolg aan de aanvaarding of weigering van een aanbod is verbonden, hun toestemming vrij verlenen."

Werkgevers zullen dus in bijna alle gevallen een andere rechtsgrond moeten zoeken dan toestemming. Enkel wanneer de toestemming wordt gegeven **via collectief overleg/cao** zijn de machtsverhoudingen in evenwicht en kan de toestemming geldig worden gegeven.

2.2.2 Transparantie

De verwerking van persoonsgegevens is enkel toegestaan wanneer hierover transparant gecommuniceerd wordt. Een geheime gegevensverzameling is nooit toegestaan.

De transparantie betreft verschillende facetten van de verwerking. Deze informatie zal veelal zijn opgenomen in een **privacyverklaring**:

a) de identiteit en de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke;
b) in voorkomend geval, de contactgegevens van de functionaris voor gegevensbescherming;
c) de verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd, alsook de rechtsgrond voor de verwerking;
d) de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, indien de verwerking op artikel 6, lid 1, punt f), is gebaseerd;
e) in voorkomend geval, de ontvangers of categorieën van ontvangers van de persoonsgegevens;
f) in voorkomend geval, dat de verwerkingsverantwoordelijke het voornemen heeft de persoonsgegevens door te geven aan een derde land of een internationale organisatie;
g) de periode gedurende welke de persoonsgegevens zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria ter bepaling van die termijn;
h) dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken om inzage van en rectificatie of wissing van de persoonsgegevens of beperking van de hem betreffende verwerking, alsmede het recht tegen de verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid;
i) wanneer de verwerking toestemming is gebaseerd, dat de betrokkene het recht heeft de toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan;
j) dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;
k) of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten, en of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt;
l) het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

VOORBEELD

- Zowel de Franse als Griekse GBA spraken reeds boetes uit tegen werkgevers die op een geheime of onvoldoende transparante manier camerabewaking installeerden op de werkvloer.

2.3 Doelbinding

Doelbinding is een essentieel bestanddeel van een correcte gegevensverwerking. Een verwerking is pas geldig wanneer het doeleind expliciet wordt vastgesteld en gerechtvaardigd is op het moment dat de persoonsgegevens worden verzameld. De gegevens mogen enkel voor dat doel gebruikt worden. Hergebruik voor andere doeleinden, waarvoor ze niet verzameld werden, is niet toegestaan.

VOORBEELD

- Een werkgever die een badge-systeem gebruikt als toegangscontrole tot de onderneming, mag de gegevens van het in- en uitbadgen niet gebruiken om de gepresteerde arbeidstijd te controleren.

2.4 Minimale gegevensverwerking

Er mogen maar zoveel gegevens verwerkt worden als strikt noodzakelijk zijn voor het bereiken van het doel van de verwerking.

VOORBEELDEN

- De Roemeense GBA veroordeelde een werkgever die camera's plaatste in de kleedkamers voor werknemers op basis van de schending van het principe van minimale gegevensverwerking.
- De Spaanse GBA veroordeelde een werkgever die via camera's bedoeld tegen diefstal zijn werknemers in het oog hield voor andere doeleinden.

2.5 Juistheid

Gegevens die verwerkt worden moeten juist zijn en zo nodig worden geactualiseerd. Alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die onjuist zijn, onverwijld te wissen of recht te zetten.

2.6 Opslagbeperking

Gegevens mogen maar zolang bewaard worden als nodig voor de doeleinden waarvoor ze worden verzameld. Daarna moeten ze worden gewist.

VOORBEELDEN

- Een Duitse onderneming werd tot een hoge boete veroordeeld voor het onnodig lang bewaren van gegevens die ze had verzameld van kandidaten in het kader van een sollicitatieprocedure.
- In Hongarije werd een bedrijf beboet voor het niet wissen van persoonlijke e-mails van een ex-werknemer.

2.7 Integriteit en vertrouwelijkheid

Dit principe houdt in dat de verwerker of verwerkingsverantwoordelijke persoonlijke gegevens op een dusdanige manier verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. De verwerker of verwerkingsverantwoordelijke zal hiervoor de passende technische of organisatorische maatregelen moeten nemen.

VOORBEELDEN

- Een Spaanse werknemer die in een brief aan het hotelmanagement en de vakbondsafvaardiging zijn beklag deed over een geval van intimidatie op de werkvloer, stapte naar de nationale GBA omdat het management en de vakbondsafvaardiging hun vertrouwelijkheidsplicht schonden door de brief voor te lezen op een vergadering met andere werknemers.
- Eveneens in Spanje werd een onderneming beboet voor een schending van de vertrouwelijkheid door een loonbrief aan de verkeerde werknemer te bezorgen.
- Een Nederlandse sociale zekerheidsinstantie kreeg een boete opgelegd wegens schending van het integriteit- en vertrouwelijkheidsprincipe omdat ze gevoelige gegevens van werknemers (medische informatie) onvoldoende had beveiligd. Volgens de Nederlandse GBA was voor dermate gevoelige gegevens een multi-factor authenticatie vereist (type 'Itsme').

3. GDPR of cao?

3.1 Uitzondering in het kader van de arbeidsverhouding

Er zijn een aantal belangrijke **interprofessionele cao's** die het recht op privacy verder uitwerken in de specifieke context van de arbeidsverhouding. Deze cao's blijven even belangrijk na als voor de GDPR. In veel gevallen bieden deze cao's een betere bescherming van het recht op privacy dan de GDPR.

Artikel 88 van de GDPR voorziet de mogelijkheid om bij cao (interprofessioneel, sectoraal of op ondernemingsniveau) specifieke regels uit te werken:

> Bij wet of bij collectieve overeenkomst kunnen de lidstaten nadere regels vaststellen ter bescherming van de rechten en vrijheden met betrekking tot de verwerking van de persoonsgegevens van werknemers in het kader van de arbeidsverhouding, in het bijzonder met het oog op aanwerving, de uitvoering van de arbeidsovereenkomst, met inbegrip van de naleving van wettelijke of uit collectieve overeenkomsten voortvloeiende verplichtingen, het beheer, de planning en de organisatie van de arbeid, gelijkheid en diversiteit op het werk, gezondheid en veiligheid op het werk, bescherming van de eigendom van de werkgever of de klant dan wel met het oog op de uitoefening en het genot van de met de arbeidsverhouding samenhangende individuele of collectieve rechten en voordelen, en met het oog op de beëindiging van de arbeidsverhouding.

3.2 Cao 81: Controle van internet- en e-mailgebruik op het werk

3.2.1 Principe

De sociale partners hebben met deze cao een kader willen scheppen waarbinnen werkgevers met respect voor de principes van transparantie, proportionaliteit en finaliteit misbruiken van online-communicatie tijdens de werkuren door werknemers (d.w.z. een gebruik dat verder gaat dan het professioneel- en een normaal occasioneel privé gebruik van het netwerk) kunnen voorkomen en opsporen. De belangrijkste waarborgen ter bescherming van de werknemer zijn de beperking van de doeleinden (finaliteit) waarvoor gecontroleerd mag worden en de getrapte procedure voor individualisering.

3.2.2 Informatie en raadpleging

Werknemers moeten vooraf (collectief en/of individueel) op de hoogte gesteld worden van alle aspecten van de controle en het beleid inzake het (niet) toegelaten gebruik van de online-communicatiemiddelen.

De geïnstalleerde controlesystemen moeten regelmatig geëvalueerd worden, naar gelang het geval in de ondernemingsraad, het comité voor preventie en bescherming op het werk of met de vakbondsafvaardiging, met het oog op voorstellen om ze aan te passen aan de technologische ontwikkelingen.

3.2.3 Doelbinding

De controle op de elektronische online-communicatiegegevens van werknemers is maar toegestaan mits een of meer van de volgende doeleinden worden nagestreefd:

- het voorkomen van **ongeoorloofde of lasterlijke feiten, feiten die strijdig zijn met de goede zeden of de waardigheid** van een andere persoon kunnen schaden;
- de bescherming van de **economische, handels- en financiële belangen van de onderneming** die vertrouwelijk zijn alsook het tegengaan van ermee in strijd zijnde praktijken (bv. verspreiding van bestanden, schending van zakengeheimen, met inbegrip van onderzoek en ontwikkeling, productieprocessen en alle mogelijke vertrouwelijke gegevens);
- de **veiligheid en/of de goede technische werking van de IT-netwerksystemen** van de onderneming, met inbegrip van de controle op de kosten die ermee gepaard gaan, alsook de fysieke bescherming van de installaties van de onderneming;
- het te goeder trouw naleven van de in de onderneming geldende **beginselen en regels voor het gebruik van onlinetechnologieën.**

3.2.4 Individualisering

De controle gebeurt aanvankelijk **enkel op globaal niveau**, d.w.z. zonder dat deze gelinkt kan worden aan een individuele werknemer. Pas in een **tweede fase** kan bij de vaststelling van een inbreuk de controle **geïndividualiseerd** worden.

De individualisering van de elektronische online-communicatiegegevens gebeurt, naargelang het doel van de door de werkgever geïnstalleerde controle:

- in het kader van een **directe procedure**
- in het kader van een **indirecte procedure** (met alarmbelprocedure).

3.2.4.1 Directe procedure

De directe individualisering van de elektronische online-communicatiegegevens is toegestaan als de controle één of meer van de volgende doeleinden nastreeft:

- het voorkomen van ongeoorloofde of lasterlijke feiten, feiten die strijdig zijn met de goede zeden of de waardigheid van een andere persoon kunnen schaden;
- de bescherming van de economische, handels- en financiële belangen van de onderneming die vertrouwelijk zijn alsook het tegengaan van ermee in strijd zijnde praktijken (bv. verspreiding van bestanden, schending van zakengeheimen, met inbegrip van onderzoek en ontwikkeling, productieprocessen en alle mogelijke vertrouwelijke gegevens);
- de veiligheid en/of de goede technische werking van de IT-netwerksystemen van de onderneming, met inbegrip van de controle op de kosten die ermee gepaard gaan, alsook de fysieke bescherming van de installaties van de onderneming;

Een werkgever die in het kader van een globale (anonieme) controle voor de hier opgesomde doeleinden een onregelmatigheid vaststelt, heeft de mogelijkheid om in het licht van de algemene gegevens waarover hij beschikt, direct over te gaan tot een individualisering van de elektronische online-communicatiegegevens, teneinde de identiteit van de verantwoordelijke persoon of personen te kunnen opsporen.

3.2.4.2 Indirecte procedure

Wanneer de controle het te goeder trouw naleven van de in de onderneming geldende beginselen en regels voor het gebruik van onlinetechnologieën nastreeft, is de individualisering maar toegestaan mits een **voorafgaande voorlichtingsfase** wordt in acht genomen.

De voorlichting heeft tot doel de werknemer(s) op een duidelijke en begrijpelijke wijze in te lichten over het bestaan van de onregelmatigheid en over het feit dat de elektronische online-communicatiegegevens geïndividualiseerd zullen worden wanneer opnieuw een dergelijke onregelmatigheid wordt vastgesteld.

De voorlichting moet erin bestaan dat de in de onderneming vastgestelde beginselen en regels in herinnering worden gebracht of worden gepreciseerd, zodat een nieuwe onregelmatigheid van dezelfde aard voorkomen wordt.

Pas bij een nieuwe schending na deze voorlichting is individualisering toegestaan.

De werknemer die bij toepassing van de procedure van indirecte individualisering verantwoordelijk wordt gesteld voor een onregelmatigheid bij het gebruik van de elektronische onlinecommunicatiemiddelen, wordt door de werkgever uitgenodigd voor een gesprek.

Dit gesprek heeft plaats voor iedere beslissing of evaluatie die de werknemer individueel kan raken.

3.3 Cao 68: camerabewaking op de arbeidsplaats

3.3.1 Informatie en consultatie

De werknemers worden vooraf (collectief en/of individueel) geïnformeerd over de geplande camerabewaking.

De informatie die moet verschaft worden heeft ten minste betrekking op:

- het nagestreefde doeleinde;
- het feit of de beeldgegevens al dan niet bewaard worden;
- het aantal en de plaatsing van de camera's;
- de betrokken periode of perioden gedurende dewelke de camera('s) functioneert (functioneren).

Als naar aanleiding van de informatie aan de ondernemingsraad blijkt dat de camerabewaking implicaties voor de persoonlijke levenssfeer van één of meerdere werknemers kan hebben, wijdt de ondernemingsraad of, bij ontstentenis daarvan, het comité voor preventie en bescherming op het werk, een onderzoek aan de maatregelen die dienen genomen te worden om de inmenging in de persoonlijke levenssfeer tot een minimum te beperken. In principe mag de camerabewaking immers geen inmenging in de persoonlijke levenssfeer van de werknemer tot gevolg hebben.

De ondernemingsraad of, bij ontstentenis daarvan, het comité voor preventie en bescherming op het werk, moet bovendien regelmatig de gehanteerde bewakingssystemen evalueren en voorstellen doen met het oog op herziening in functie van de technologische ontwikkelingen.

3.3.2 Doelbinding

Camerabewaking op de arbeidsplaats is enkel toegelaten voor het nastreven van één van de volgende doeleinden:

- de veiligheid en gezondheid;
- de bescherming van de goederen van de onderneming;
- de controle van het productieproces.
- de controle van de arbeid van de werknemer. Camerabewaking met als doeleinde de controle van de arbeid van de werknemer mag de werknemer niet voortdurend in beeld brengen.

3.4 Cao 89: uitgangscontrole

3.4.1 Informatie

Voorafgaandelijk aan het opstarten van een systeem van uitgangcontroles moet de werkgever de ondernemingsraad informatie verschaffen over het systeem.

Bij ontstentenis van een ondernemingsraad wordt deze informatie verschaft aan het comité voor preventie en bescherming op het werk, of, bij ontstentenis daarvan, aan de vakbondsafvaardiging, of, bij ontstentenis daarvan, aan de werknemers.

De informatie die moet verschaft worden, heeft in ieder geval betrekking op:

- de perimeter van de onderneming of van de werkplaats;
- de diefstalrisico's in de onderneming of op de werkplaats;
- de maatregelen om die risico's te voorkomen of te verhelpen;
- en de controlemethodes.

3.4.2 Doelbinding

Uitgangscontroles van werknemers zijn enkel toegelaten indien zij gericht zijn op het voorkomen of vaststellen van de ontvreemding van goederen in de onderneming of op de werkplaats.

De uitgangscontroles van werknemers mogen niet tot doel hebben de arbeidsprestaties van de werknemers te meten of de aanwezigheden van de werknemers te controleren.

Uitgangscontroles van werknemers door personen mogen (enkel) uitgevoerd worden door bewakingsagenten, al dan niet met behulp van elektronische middelen, en bovendien enkel:

- wanneer er, op grond van de gedragingen van de werknemer, van materiële aanwijzingen (bv. een waarschuwingssignaal van een detectiesysteem) of van de omstandigheden, redelijke gronden zijn om te denken dat die werknemer goederen in de plaats die hij verlaat, heeft ontvreemd;
- steekproefsgewijze ter voorkoming van diefstal.

Systematische uitgangcontroles zijn alleen toegelaten als ze uitgevoerd worden door middel van elektronische en/of technische detectiesystemen (dus zonder tussenkomst van een bewakingsagent).

De uitgangscontrole kan uitsluitend bestaan uit het nazicht van de door de gecontroleerde werknemer vrijwillig aan de bewakingsagent voorgelegde goederen, die hij op zich draagt of in zijn handbagage draagt en/of die zich in zijn of een door hem gebruikt voertuig bevinden.

De werknemer fouilleren met het oog op het ontdekken van verborgen goederen, mag dus niet.

Vaststellingen die tegen de werknemer gebruikt kunnen worden, moeten schriftelijk meegedeeld worden.

3.5 Cao 38: werving en selectie

De persoonlijke levenssfeer van de sollicitant moet bij de selectieprocedure worden geëerbiedigd. Vragen over het privéleven zijn slechts verantwoord indien zij relevant zijn wegens de aard en de uitoefeningsvoorwaarden van de functie. Dit geldt niet alleen voor de werkgever maar ook voor de personen die namens hem aan de selectiewerkzaamheden deelnemen, zoals b.v. de psychologen en de geneesheren.

Alle inlichtingen betreffende de sollicitant worden door de werkgever vertrouwelijk behandeld.

VOORBEELD

- Een werkgever mag de uittreksels uit het strafregister (het vroegere 'getuigschrift van goed gedrag en zeden') van sollicitanten niet verwerken, tenzij wanneer de sollicitatie een functie betreft waarvoor bij wet is voorgeschreven dat zij slechts mag worden uitgeoefend door een persoon die niet is veroordeeld tot bepaalde straffen (zie bv. artikel 275 van de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid).
- Een werkgever mag geen persoonlijke gegevens opzoeken over een sollicitant (via bv. sociale media) die niet rechtstreeks relevant zijn voor de aangeboden functie (bv. over hobby's, politieke voorkeuren etc.).

3.6 Cao 39: nieuwe technologieën

3.6.1 Principe

De invoering van nieuwe technologieën in de onderneming gaat vaak gepaard met privacyvraagstukken. Daarom is cao 39 betreffende voorlichting en overleg inzake de sociale gevolgen van de invoering van nieuwe technologieën hier relevant.

Wanneer de werkgever heeft besloten over te gaan tot een investering in een nieuwe technologie en wanneer die investering belangrijke collectieve gevolgen heeft voor de werkgelegenheid, de werkorganisatie of de arbeidsvoorwaarden, dan moet hij uiterlijk 3 maanden vóór het begin van de inplanting van de nieuwe technologie:

- enerzijds informatie verschaffen over de aard van de nieuwe technologie, over de factoren die de invoering ervan rechtvaardigen alsmede over de aard van de sociale gevolgen; en
- anderzijds met de werknemersvertegenwoordigers overleg plegen over de sociale gevolgen van de invoering van de nieuwe technologie.

3.6.2 Toepassingsgebied

De cao nr. 39 is van toepassing op de ondernemingen die gewoonlijk ten minste 50 werknemers tewerkstellen gedurende het kalenderjaar voorafgaand aan de periode tijdens welke de informatie moet worden verstrekt.

3.6.3 Informatie en consultatie

De te verstrekken geschreven informatie heeft betrekking op:

- de aard van de nieuwe technologie;
- de economische, financiële of technische factoren die de invoering ervan verantwoorden;
- de aard van de sociale gevolgen;
- op de termijnen van inwerkingstelling van de nieuwe technologie.

De informatie wordt verstrekt aan de ondernemingsraad of, bij ontstentenis daarvan, aan de vakbondsafvaardiging. Bij ontstentenis van ondernemingsraad en vakbondsafvaardiging wordt de informatie verstrekt aan het comité voor preventie en bescherming op het werk.

Het overleg heeft betrekking op:

- de vooruitzichten inzake de werkgelegenheid van het personeel, de werkgelegenheidsstructuur en de voorgenomen sociale maatregelen inzake werkgelegenheid;
- de werkorganisatie en de arbeidsvoorwaarden;
- de gezondheid en de veiligheid van de werknemers;
- de vakbekwaamheid en de eventuele maatregelen voor opleiding en omscholing van de werknemers.

4. Geolokalisatie

Er bestaat tot op heden geen specifieke wetgeving die de controle van werknemers via GPS-systemen regelt. Enkel in het Paritair Comité 219 (Erkende controleorganismen) werd hierover een sectorale cao afgesloten.

Uit de rechtspraak en de adviezen van de GBA kunnen wel enkele duidelijke krijtlijnen worden afgeleid waaraan ieder systeem van geolokalisatie met betrekking tot werknemers of de voertuigen die zij besturen moet voldoen.

4.1.1 Doelbinding

Een systeem dat mogelijk maakt personeelsleden precies te lokaliseren, moet beantwoorden aan welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden, die de installatie en het gebruik ervan rechtvaardigen.

Bijvoorbeeld in functie van de veiligheid van de werknemer, in functie van de bescherming van de dienstvoertuig, om in te spelen op welomschreven professionele behoeften aangaande transport en logistiek, of nog, om bewust toezicht op het personeel te houden, dus ter controle van het professioneel gebruik van de dienstvoertuig en de behoorlijke uitvoering van hun arbeidsregime.

4.1.2 Proportionaliteit

Indien het systeem geïnstalleerd is met de bedoeling de uitvoering van de taken toevertrouwd aan de werknemers te controleren, dan zou dit een gerichte controle moeten zijn en gerechtvaardigd door aanwijzingen die misbruik door bepaalde werknemers doen vermoeden.

Een permanente controle waarbij er middels een lokalisatiesysteem een systematische lezing van de geregistreerde gegevens plaatsvindt, moet in principe als overmatig worden beschouwd.

Er zijn niettemin bepaalde hypotheses waarbij een meer regelmatige controle gerechtvaardigd zou kunnen zijn indien deze rechtstreeks verband houdt met de aard van de te vervullen taken door de werknemer, en meer bepaald om het beheer van de verplaatsingen van de professionele voertuigen (verkopers, technici te velde) te optimaliseren. Zelfs in dat geval mogen de voertuigen niet continu gevolgd worden. Het systeem zou in ieder geval moeten kunnen gedesactiveerd worden wanneer het voertuig door betrokkene buiten de werkuren (woon-werkverkeer, pauzes...) wordt gebruikt.

Ander niet toegestaan gebruik is o.a.:

- Om de naleving van de snelheidslimiet te controleren;
- Geolokalisatie in het voertuig van een werknemer die de vrijheid heeft zijn verplaatsingen zelf te regelen;
- Om verplaatsingen van personeelsvertegenwoordigers te volgen die in het kader van de uitoefening van hun mandaat gebeuren;
- Om de werktijd van werknemers te berekenen wanneer er al een ander systeem voor voorzien is.

4.1.3 Informatie en consultatie

Het transparantiebeginsel kan worden vertaald door het voorzien in een uitgebreide kennisgeving ten behoeve van de personen wier gegevens verwerkt worden, in het bijzonder over:

- de rechtsgrond voor de gegevensverwerking. In het geval van geolokalisatie is het waarschijnlijk een gerechtvaardigd belang van de onderneming of van derden;
- wie gecontroleerd wordt;
- de mate waarin er gecontroleerd wordt;
- de doelen die door de controle worden nagestreefd;
- de aard van de misstanden die tot een controle kunnen leiden;
- de duur van de controle;
- de verwerkte gegevens;
- of de gegevens buiten de Europese Unie worden verzonden;
- wat de rechten van de werknemer zijn, zoals het recht de gegevens te raadplegen, het recht een klacht in te dienen bij de Gegevensbeschermingsautoriteit, het recht de verwerking van de gegevens te beperken, ...;
- de procedure die na de controle zal worden gevolgd.

Daarnaast moeten ook de informatie- en consultatieprocedures uit cao 39 worden gerespecteerd (zie hierboven).
Het wordt ook algemeen aangenomen dat een voorafgaandelijke gegevensbeschermingseffectbeoordeling (zie hierboven 2.1.3) nodig is.

4.1.4 Arbeidsreglement

Aangezien de invoering van een GPS-tracering een bijkomende controlebevoegdheid van het toezichthoudend personeel inhoudt, zal een aanpassing van het arbeidsreglement vereist zijn.

5. Het communicatiegeheim

5.1 Verbod

Het communicatiegeheim wordt onder andere gewaarborgd door artikel 314bis van het Strafwetboek. Op grond van dat artikel is het de werkgever verboden om, met behulp van een toestel, telefoongesprekken van zijn werknemers af te luisteren of op te nemen, of kennis te nemen van de inhoud van (professionele of privé) e-mails die niet voor hem bestemd zijn, zonder dat hij hiervoor hun toestemming heeft.

De Wet Elektronische Communicatie sanctioneert ook strafrechtelijk wie kennis neemt van het bestaan of van de afzender/bestemmeling van iedere informatie die via elektronische weg wordt verstuurd en die niet persoonlijk voor hem bestemd is (dit verbod betreft dus niet enkel het kennisnemen van de inhoud, maar ook de aan de communicatie verbonden meta-gegevens).

5.2 Uitzondering: bewijs commerciële transacties en callcenters

Er geldt één uitzondering op bovenstaand verbod. Deze uitzondering geldt in twee gevallen en onder volgende voorwaarden:

- de registratie van elektronische communicatie en de daarmee verband houdende verkeersgegevens uitgevoerd in het legale zakelijke verkeer **ten bewijze van een commerciële transactie of van een andere zakelijke communicatie** (denk hierbij aan het bank- en beleggingswezen) toegestaan, op voorwaarde dat de bij de communicatie betrokken partijen vóór de registratie op de hoogte gebracht worden van de registratie, de precieze doeleinden ervan en de duur van de opslag van de registratie.
- het kennisnemen en registreren van elektronische communicatie en de verkeersgegevens **met als enig doel de kwaliteit van de dienstverlening in callcenters te controleren**, is toegestaan, op voorwaarde dat de personen die werkzaam zijn in het callcenter op voorhand op de hoogte gebracht worden van de mogelijkheid tot kennisnemen en registreren, het precieze doel ervan en de duur van bewaring van de geregistreerde communicatie en gegevens. Die gegevens mogen ten hoogste gedurende één maand worden bewaard.

6. Met schending van de privacy verkregen bewijs

Moet bewijsmateriaal dat werd bekomen in strijd met de voorschriften die beogen de persoonlijke levenssfeer van de werknemer te beschermen, ter zijde worden geschoven? Kan een dringende reden bijvoorbeeld worden bewezen aan de hand van een in strijd met de cao nr. 68 met een bewakingscamera gemaakte opname of aan de hand van elektronische online-communicatiegegevens die werden bekomen in strijd met de cao nr. 81?

Net zoals in strafzaken (de zogenaamde Antigoonleer) is het Hof van Cassatie in sociale zaken sinds enige tijd van oordeel dat, behoudens wanneer de wet uitdrukkelijk anders bepaalt, het de rechter toekomt de toelaatbaarheid van een onrechtmatig verkregen bewijs te beoordelen, rekening houdende met de elementen van de zaak in haar geheel genomen, inbegrepen de wijze waarop het bewijs werd verkregen en de omstandigheden waarin de onrechtmatigheid werd begaan. Tenzij wanneer een op straffe van nietigheid voorgeschreven vorm is miskend, mag een dergelijk bewijs alleen worden geweerd wanneer de bewijsverkrijging is aangetast door een gebrek waardoor de betrouwbaarheid ervan wegvalt of waardoor het recht op een eerlijk proces in het gedrang kan worden gebracht.

Verschillende arbeidsgerechten sluiten zich in hun recente rechtspraak aan bij die Cassatierechtspraak. Maar er is ook rechtspraak die oordeelt dat dit Cassatie-arrest niet van toepassing is in geschillen over van het einde van de arbeidsrelatie tussen de werkgever en de werknemer. Het met schending van de privacy verkregen bewijs wordt dan uit de debatten geweerd.

Gezien deze verdeelde rechtspraak, moet een werknemer er rekening mee houden dat het risico steeds bestaat dat bewijsmateriaal dat door de werkgever met schending van de privacy-wetgeving werd bekomen, in een rechtszaak alsnog tegen hem gebruikt mag worden.

7. Portretrecht

Het recht op afbeelding is een recht waarbij voor het maken van elke menselijke afbeelding, maar ook het gebruik van die afbeelding toestemming vereist is van de afgebeelde persoon (art. XI.174 Wetboek Economisch Recht):

> De auteur of de eigenaar van een portret dan wel enige andere persoon die een portret bezit of voorhanden heeft, heeft niet het recht het te reproduceren of aan het publiek mede te delen zonder toestemming van de geportretteerde of, gedurende twintig jaar na diens overlijden, zonder toestemming van zijn rechtverkrijgenden.

Dit recht staat eigenlijk los van de bescherming van de privacy. Toch komt dit recht soms ter sprake in een arbeidsrechtelijke context.
De draagwijdte van het portretrecht wordt door rechtspraak en rechtsleer als volgt ingevuld:

- Rechtsleer en rechtspraak zijn het er grotendeels over eens dat wanneer een persoon zich in de openbaarheid begeeft, bijvoorbeeld op **een publieke plaats**, hij zijn stilzwijgende toestemming geeft. Deze toestemming wordt afgeleid uit de feitelijke omstandigheden. De toestemming blijft wel vereist voor het gebruik en de reproductie van de genomen foto of video. De persoon moet in dit geval wel het hoofdonderwerp vormen.
- Wanneer bepaalde personen **toevallig op een foto of video** staan, genomen op een publieke plaats (bv. een foto van een monument waar enkele personen toevallig mee op afgebeeld staan), dan gaat men er in principe van uit dat een toestemming voor het verdere gebruik van die foto of video niet vereist is.
- Wanneer **afbeeldingen van een menigte** worden genomen, is er in principe ook geen toelating nodig (noch voor het nemen, noch voor het gebruik nadien), omdat ook hier de weergave van de persoon bijkomstig is. Wat onder de noemer 'menigte' valt, wordt geval per geval beoordeeld.
- **Publieke personen** (bv. politici, sportvedetten, zangers, ...) dienen in principe ook geen voorafgaande toestemming te geven. Hier geldt immers het recht op informatie (persvrijheid), mits enkele voorwaarden worden nageleefd. Sommige personen worden slechts tijdens een welbepaalde gebeurtenis als publieke persoon aanzien (bijvoorbeeld naar aanleiding van een ramp of een misdrijf).