Crowell

CLIENT ALERT

Privacy, Information and Consultation of the Works Council

June 30, 2006

In many European countries, employers have an obligation to inform and/or consult the works council (or other bodies representing employees) when making certain decisions involving the privacy of their employees. This is not merely a theoretical obligation, and failure to comply may have important practical consequences. In Germany, for instance, both the lower and appellate courts struck down an “Employee Code of Conduct” affecting worker privacy which US supermarket chain Wal-Mart implemented without obtaining approval of its works council. In addition to violating the law, such decisions may negatively affect the image of a company attempting to gain goodwill and positive publicity abroad.

In other European countries, where no formal obligation to inform and/or consult the works council with respect to employee data protection exists, employers should nevertheless consider providing such information to their employees. Reporting important measures taken to ensure compliance with privacy laws in general and for specific projects, e.g. outsourced payroll processing, to employees is wise, given the increased sensitivity of data protection in Europe.

In addition, irrespective of the existence of any general obligation, legal requirements may exist to consult the works council in specific cases. For example, in Belgium there is such an obligation for the introduction of email and Internet monitoring and video surveillance.

Internet and e-mail monitoring

While more and more employers monitor employee use of e-mail and Internet to prevent abuse of these technologies, such monitoring constitutes an intrusion upon the employees' privacy and may be in violation of applicable privacy legislation.

Employers caught violating this legislation are exposed to criminal or administrative sanctions and/or claims for damages. From a practical point of view, a less known risk is also quite significant: evidence obtained via e-mail or Internet monitoring may not be accepted as evidence by the court in case of proceedings against the employee (e.g. in case of termination for a cause for improper use of e-mail or Internet).

Although there is some variance in the case law, there is a trend among courts in Belgium, the Netherlands and France with regard to the use of such evidence by employers. It seems that, while the basic principle remains that an employer cannot use evidence obtained in violation of privacy and other laws on e-mail and Internet monitoring, such evidence may be admissible in case of “exceptional circumstances”. What these exceptional circumstances are varies from case to case. If the facts that were discovered via the monitoring are very serious (thefts, fraud, …), it appears that courts will allow the evidence, even if it was obtained in violation of these laws.

While such relief may be a possibility, it is always best to take steps to protect employee privacy - and yourself- when possible while monitoring use of the Internet and e-mail by having a proper Internet and e-mail policy. Moreover, the following additional measures could be considered:

- obtaining consent from employees to check the content of e-mails;
- giving the employee the opportunity to explain himself before terminating his or her employment on account of Internet use;
- allowing the employee to be assisted by his/her trade union representative during any hearings that occur;
- obtaining the assistance of experts or witnesses, such as a bailiff, for evidence purposes.

Privacy - Informatie en Consultatie van de ondernemingsraad

In verschillende Europese landen hebben werkgevers een verplichting om de ondernemingsraad (of andere organen die de werknemers vertegenwoordigen) te informeren en/of te consulteren wanneer zij bepaalde maatregelen treffen die verband houden met de privacy van hun werknemers.

Dit is geen louter theoretische verplichting. De niet naleving ervan kan belangrijke praktische gevolgen hebben. Zo werd in Duitsland, zowel in eerste aanleg als in graad van beroep, geoordeeld dat de supermarktketen Wal-Mart haar *"Employee Code of Conduct"* , die onder andere betrekking had op de privacy van werknemers, niet kon inroepen tegen haar werknemers zolang de ondernemingsraad deze niet had goedgekeurd. Dergelijke beslissingen en de publiciteit die daaraan gegeven wordt, kunnen vaak een negatieve invloed hebben op het imago van de onderneming.

In andere Europese landen, waar geen dergelijke formele, algemene verplichting tot informatie en/of consultatie van de ondernemingsraad bestaat, moeten werkgevers niettemin overwegen of zij hun werknemers niet vrijwillig inlichten over dergelijke beslissingen. Het meedelen aan de werknemers van belangrijke maatregelen die worden ingevoerd met het oog op de naleving van de privacy wetgeving is ons inziens aan te raden, gelet op het toenemend belang van privacy en bescherming van persoonsgegevens in Europa.

Daarenboven bestaan in de landen waar geen algemene verplichting tot informatie en/of consultatie met betrekking tot beslissingen inzake privacy bestaat, zoals in België, vaak verplichtingen om de ondernemingsraad in te lichten of te consulteren in specifieke gevallen. In België is er bijvoorbeeld een dergelijke verplichting wanneer e-mail en internet controle of cameratoezicht op de werkplaats wordt ingevoerd.

Internet en e-mail controle ("monitoring")

Terwijl meer en meer werkgevers het gebruik van e-mail en internet door hun werknemers wensen te controleren om misbruik van deze nieuwe technologieën tegen te gaan, mag niet uit het oog worden verloren dat dergelijke maatregelen binnendringen in de privacy van de werknemer en een schending kunnen uitmaken van de toepasselijke privacy wetgeving.

Werkgevers die deze wetgeving overtreden kunnen administratieve en strafsancties oplopen. De betrokken werknemers zouden vorderingen tot schadevergoeding kunnen inleiden. Daar waar dergelijke sancties of vorderingen (nog) niet vaak voorkomen in Europa, is het belangrijkste risico van het niet naleven van de betrokken wetgeving, dat het bewijs dat wordt verkregen met schending van deze wetgeving, waarschijnlijk niet zal worden aanvaard door rechtbanken in geval van procedures tegen de

betrokken werknemers (bijvoorbeeld in geval van een procedure naar aanleiding van een ontslag om dringende reden gebaseerd op misbruik van e-mail of internet of aan het licht gekomen via controle van e-mail of internet).

Alhoewel de rechtspraak uiteenlopende standpunten aanneemt inzake het aanvaarden van dergelijk bewijs, menen wij toch een trend te kunnen waarnemen in België, Nederland en Frankrijk. Het lijkt dat, alhoewel het basisprincipe blijft dat de werkgever geen bewijs kan gebruiken dat hij heeft bekomen met schending van de privacy wetgeving, dergelijk bewijs toch zal worden toegelaten door de rechter in geval van “uitzonderlijke omstandigheden”. Wat deze uitzonderlijke omstandigheden zijn, verschilt van geval tot geval. Indien de feiten die werden ontdekt via de controle zeer ernstig zijn (diefstal, fraude, …), lijken sommige rechtbanken het bewijs te aanvaarden, zelfs al werd de privacy wetgeving overtreden.

Niettegenstaande deze evolutie, is het natuurlijk aan te raden om niettemin de nodige maatregelen te nemen wanneer u het internet- en e-mailgebruik van uw werknemers zou wensen te controleren. Daarbij is het van belang te beschikken over een goede internet- en e-mailpolicy. Daarenboven kunnen onder andere de volgende maatregelen worden overwogen:

- tracht steeds het voorafgaandelijk akkoord te bekomen van uw werknemers om de inhoud van hun e-mails en hun internetgebruik te controleren;
- geef werknemers de kans om zich te verantwoorden alvorens over te gaan tot ontslag of andere sancties voor het foutief gebruik van internet of e-mail;
- geef de werknemer de kans om te worden bijgestaan door een vakbondsafgevaardigde gedurende een eventueel verhoor naar aanleiding van de vastgestelde feiten;
- tracht getuigen, zoals een gerechtsdeurwaarders of andere (IT-)experts, dergelijk verhoor te laten bijwonen of de nodige vaststellingen te laten doen, zodat u de inhoud van het gesprek of de vastgestelde inbreuken later kan bewijzen.

Vie Privée, Information et Consultation du Conseil d'Entreprise

Dans de nombreux Etats européens, les employeurs ont l'obligation d'informer et/ou de consulter le conseil d'entreprise (ou d'autres organes représentatifs des travailleurs) dans les matières touchant à la vie privée de leurs travailleurs. Le non respect de ces dispositions peut avoir des conséquences pratiques importantes. Ainsi, en Allemagne, le tribunal, suivi par la cour du travail, a rejeté le « Employee Code of Conduct », qui contenait des dispositions touchant à la vie privée des travailleurs, du distributeur alimentaire Wal-Mart car celui-ci avait été adopté sans obtenir l'assentiment du conseil d'entreprise. De telles décisions peuvent, en outre, affecter de façon négative l'image de la société.

Dans les autres Etats européens, où il n'existe pas d'obligation expresse d'informer et/ou de consulter le conseil d'entreprise en matière de vie privée, il est néanmoins conseillé d'informer celui-ci des mesures prises ou envisagées par la société susceptibles d'avoir une incidence sur la vie privée des travailleurs, particulièrement lorsqu'il s'agit de projets d'une certaine ampleur, comme l'outsourcing de la gestion des rémunérations. Il s'agira là d'une sage précaution compte tenu de la sensibilité accrue en la matière en Europe.

Indépendamment de l'existence éventuelle d'une obligation générale en matière d'information et/ou de consultation des organes représentatifs des travailleurs, il ne faut enfin pas perdre de vue qu'il existe parfois certaines dispositions régissant des domaines spécifiques, prévoyant l'information ou la consultation du conseil d'entreprise. Tel est par exemple le cas en Belgique en ce qui concerne le contrôle et la surveillance des systèmes de messagerie électronique et de l'Internet ou encore en matière de vidéosurveillance.

Contrôle de l'Internet et des systèmes de messagerie électronique

S'il est certain qu'en pratique de plus en plus d'entreprises contrôlent et surveillent l'utilisation par leurs travailleurs des systèmes de messagerie électronique (e-mails) et de l'Internet, il n'en reste pas moins qu'une telle surveillance constitue une intrusion dans la vie privée des travailleurs et peut être constitutive d'une violation des dispositions légales applicables.

Les employeurs qui se rendraient coupables de telles violations, s'exposent non seulement à des sanctions pénales ou administratives mais également à des demandes en paiement de dommages et intérêts. Le risque le plus important, à l'heure actuelle, nous paraît cependant être celui des éventuels dégâts collatéraux susceptibles de résulter du non respect des dispositions en matière de vie privée : le rejet par un tribunal des éléments de preuve recueillis à l'occasion d'un contrôle du système de messagerie électronique et/ou de l'Internet en violation des dispositions applicables (l'hypothèse la plus courante est celle du licenciement pour motif grave en raison de faits liés à une utilisation abusive ou illicite par l'employé concerné des systèmes de messagerie électronique ou de l'Internet ou découverts par le biais d'un contrôle des e-mails ou de l'Internet).

Observons à cet égard une certaine tendance des cours et tribunaux, notamment en Belgique, aux Pays-Bas et en France, à admettre que des éléments de preuve recueillis de façon illicite puissent, malgré tout, être recevables en cas de circonstances exceptionnelles. En pratique, il semble bien que lorsque les faits ainsi découverts par le biais d'un contrôle illégal sont très graves (vols, escroquerie, …), certains juges font preuve d'une certaine flexibilité et acceptent alors parfois de prendre en compte ces éléments de preuve en dépit de leur illicéité intrinsèque.

L'entreprise prudente veillera toutefois à prendre les mesures nécessaires afin que le droit des travailleurs au respect de la vie privée soit respecté en cas de surveillance et/ou contrôle de l'usage que ceux-ci font des systèmes de messagerie électronique ou de l'Internet. Pour ce faire, l'entreprise veillera tout d'abord à adopter un règlement interne régissant l'usage de l'Internet et du système de messagerie électronique. En outre, les mesures complémentaires suivantes peuvent, selon le cas, être envisagées :

- obtenir l'accord des travailleurs afin de vérifier le contenu de leurs emails;
- donner au travailleur concerné la possibilité de s'expliquer avant de le licencier pour motif grave;
- permettre au travailleur concerné d'être assisté par son représentant syndical pendant une telle audition;
- obtenir l'assistance éventuelle d'experts ou de témoins, tel un huissier de justice ou un expert informatique indépendant, et ce à des fins de preuve.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Emmanuel Plasschaert
Partner – Brussels
Phone: +32.2.282.4084

Email: eplasschaert@crowell.com

Frederik Van Remoortel
Partner – Brussels
Phone: +32.2.282.1844
Email: fvanremoortel@crowell.com

Thomas P. Gies
Partner – Washington, D.C.
Phone: +1.202.624.2690
Email: tgies@crowell.com