CCA ADVOGADOS | ONTIER

NEWSLETTER

01.04.2014

LABORAL E TMT
Nº 01/2014

CONTROLO DA UTILIZAÇÃO PARA FINS PRIVADOS DAS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO NO CONTEXTO LABORAL

A Deliberação n.º 1638/2013 da Comissão Nacional de Proteção de Dados (adiante CNPD) aplica-se ao tratamento de dados pessoais decorrentes do controlo da utilização para fins privados das tecnologias de informação e de comunicação no contexto laboral, nomeadamente no que diz respeito a comunicações telefónicas, utilização da internet e do correio eletrónico.

Neste âmbito a CNPD dá, assim, novas directrizes às empresas nesta matéria, sempre norteadas pelo respeito e verificação dos princípios do fim, da adequação, da necessidade, da proporcionalidade, da transparência e da boa-fé.

Nesta deliberação não são considerados os tratamentos de dados pessoais dos sistemas de geolocalização, que serão objeto de deliberação específica da CNPD.

I – Condições de legitimidade:

Por dizerem respeito à vida privada dos trabalhadores, e como tal se enquadrarem como dados sensíveis, está proibido o tratamento de (i) dados de tráfego; (ii) dados contidos nas comunicações de natureza privada e (iii) outros dados de utilização das comunicações.
Não obstante, o poder do empregador de definir os termos em que o trabalho deve ser prestado e, especificamente de definir regras de utilização dos meios de comunicação na empresa e do consequente controlo do cumprimento das mesmas encontra-se legitimado, com fundamento na lei, em concreto no disposto nos artigos 22º, n.º 2 e 97º do Código do Trabalho.

Ora, a CNPD considera que não pode ser absolutamente proibida a utilização dos meios tecnológicos do trabalho para fins pessoais. Podendo, no entanto, a entidade empregadora, tal como referido supra de acordo com a lei, estabelecer regras de utilização dos meios de comunicação na empresa, designadamente do correio eletrónico. Não obstante, estas regras devem ser proporcionais à finalidade que prosseguem e respeitar o núcleo essencial dos direitos, das liberdades e das garantias dos trabalhadores. Mais, o empregador tem que demonstrar que escolheu as formas de controlo com menor impacto sobre os direitos fundamentais dos trabalhadores.

Nestes termos, genericamente, as entidades empregadoras deverão respeitar o seguinte:

- Deve ser utilizada uma **metodologia genérica de controlo** afastando sempre que possível a consulta individualizada de dados pessoais.

- Deve ser feita uma **adequada parametrização** aplicada ao universo global dos trabalhadores, por exemplo: quantidade, custo, duração de chamadas telefónicas, número de mensagens enviadas, tipo de ficheiros em anexo, tempo gastos em consulta na internet, entre outros. A CNPD considera que uma adequada parametrização é suficiente para satisfazer os objetivos do controlo, permitindo detetar eventuais utilizações abusivas.

CONTACTOS

DEPARTAMENTO LABORAL
jcb@cca-ontier.com

DEPARTAMENTO TMT
fm@cca-ontier.com

A presente NEWSLETTER foi elaborada com fins informativos, sendo disponibilizada de forma gratuita, para uso exclusivo e restrito dos clientes da CCA, encontrando-se vedada a sua reprodução e circulação não expressamente autorizadas. Esta informação tem caráter geral e não substitui o aconselhamento jurídico para a resolução de casos concretos.

www.cca-ontier.com

- **Não** deve ser feito um **acesso sistemático ao registo das comunicações eletrónicas**. A CNPD considera que tal seria desproporcional quanto à finalidade que se pretende atingir e violador da dignidade do trabalhador.

- Os dados a tratar e os meios utilizados devem ser ajustados:

(i) à organização da empresa;
(ii) ao desenvolvimento da atividade produtiva; e
(iii) ser compatíveis com os direitos e as obrigações dos trabalhadores consignados na legislação do trabalho.

- Tendo em conta o princípio do sigilo das comunicações os controlos individualizados não devem ocorrer. Impõe-se em particular proteger os dados de tráfego que são reveladores de aspetos da vida privada do trabalhador, por exemplo: número de telefonema chamado; endereço de correio eletrónico do destinatário; identificação do sítio da internet visitado e extração de listagens de comunicação.
A CNPD considera, consequentemente, que se alcança a finalidade pretendida com a adoção de mecanismos técnicos que possibilitem apenas o tratamento de alguns dados como por exemplo a hora e a duração da comunicação, os quais não apresentam riscos para a privacidade do trabalhador e ao mesmo tempo permitem descobrir algum desvio às normas estabelecidas para a utilização dos meios da entidade empregadora.

- É vedado ao empregador: Qualquer forma de controlo do conteúdo da informação da área privativa do trabalhador enquanto utilizador de conta pessoal de correio eletrónico, das redes sociais ou de quaisquer outras contas às quais o trabalhador aderiu a título pessoal ainda que a elas aceda através do computador da empresa.

VI- Prazo de conservação dos dados:
Devem adotar-se garantias reforçadas que minimizem efetivamente os riscos para a privacidade do trabalhador, pelo que o prazo de conservação deve ser o mais curto possível: prazo máximo de 6 meses, sem prejuízo da sua manutenção no decurso de processo disciplinar ou judicial.

IV - Finalidades admissíveis para o controlo de utilização para fins privados pelos trabalhadores das tecnologias de informação e comunicação no contexto laboral

1. Gestão dos meios da empresa
2. Produtividade dos trabalhadores

V-Interconexões e comunicações de dados a terceiros:
A interconexão de dados pessoais deve ser: **(i)** adequada à prossecução das finalidades legais; e **(ii)** não implicar discriminação ou diminuição de direitos, de liberdades e de garantias dos titulares dos dados.
A CNPD considera que é possível atingir as finalidades deste tratamento de dados sem recurso à interconexão com outros dados, como sejam as bases de dados de recursos humanos igualmente da responsabilidade do empregador. Em conclusão, sem prejuízo dos resultados do controlo podem ser eventualmente utilizados no âmbito de processo disciplinar caso revelem utilização abusiva que se pretende sancionar, o tratamento destes dados não pode ser sujeito a interconexões com outros dados da responsabilidade da entidade empregadora ou de terceiros.
Não se verificam quaisquer comunicações de dados a terceiros, sem prejuízo do cumprimento de obrigação legal no contexto de processo judicial.

VI- Direito de acesso, retificação e eliminação:
A entidade empregadora deve informar os trabalhadores sobre as condições para o exercício deste direito.

VIII-Procedimentos a adotar:
Antes de iniciar o tratamento, a entidade empregadora deve informar o trabalhador sobre:
a) As condições de utilização dos meios da empresa para fins privados;
b) A realização do seu controlo (formas e metodologias adotadas);
c) A existência do tratamento de dados que lhe está associado;
d) Finalidades do tratamento;
e) Dados tratados;
f) Tempo de conservação;
g) Grau de tolerância admitido;
h) Consequência da utilização indevida dos meios de comunicação colocados à sua disposição.

A delimitação das condições de tratamento de dados e a especificação das formas de controlo deve constar de Regulamento Interno.

A elaboração do Regulamento obriga à audição da comissão dos trabalhadores, caso esta exista, e cuja produção de efeitos depende da publicitação do respetivo conteúdo e do envio para a Autoridade para as Condições do Trabalho (ACT) ou outra entidade de competência inspetiva que lhe venha a suceder, bem como da autorização da CNPD para o tratamento de dados, para a qual existe já um formulário eletrónico específico.

IX-Medidas de segurança:
Por estarem em causa dados sensíveis devem adoptar-se especiais medidas de segurança, de acordo com o disposto no artigo 15º da Lei de Proteção de Dados Pessoais:
(i) Deve estabelecer-se um perfil de acesso específico para este tipo de tratamento;

LISBOA | ASUNCIÓN | BOGOTÁ | CARACAS | LA PAZ | LIMA | LONDON | MADRID | MAPUTO | MÉXICO D.F. | MIAMI | OVIEDO | PANAMÁ CITY | SANTA CRUZ | SANTANDER | SÃO PAULO | SHANGHAI P.R.C. THE FIRST GLOBAL FIRM WITH A LOCAL SOUL

(ii) Os acessos aos sistemas que registem estas informações só poderão ser efetuados com contas de utilizador que permitam identificar univocamente o indivíduo;
(iii) O acesso tem de ser restrito e deve-se manter um registo de acesso à informação sensível para controlo das operações e para realização de auditorias internas e externas;
(iv) Tem que ficar registado quem fez o acesso, respetiva data e hora (timestamp), operações efetuadas atribuindo um número sequencial (id) a cada ocorrência e um campo de hash aplicado sobre os elementos anteriores (id, utilizador, data, hora e operação). Importa referir que os logs para terem validade legal têm de estar assinados digitalmente;
(v) Deve ser desenvolvido um sistema de alarmes que permita identificar utilizações indevidas do sistema e implementada uma política de análise de logs, com a realização de relatórios periódicos de análise.
(vi) Relativamente ao prazo de conservação destes logs estabelece-se o prazo de um ano.

X-O tratamento de dados em especial

1. Controlo de dados de comunicações telefónicas e de dados de tráfego
Neste âmbito impõem-se os seguintes limites:
(i) Deve ser definido o grau de tolerância quanto à utilização dos telefones, fixos ou móveis, e as formas de controlo realizadas.
(ii) É proibido o acesso ao conteúdo das comunicações, bem como a utilização de qualquer dispositivo de escuta, armazenamento, interceção e vigilância de comunicações pelo empregador.
Nas profissões em que o sigilo ou confidencialidade sejam essenciais, nomeadamente, no caso de jornalista, médico ou advogado não é admissível qualquer tipo de controlo, designadamente através da análise da faturação detalhada ou da informação registada em centrais telefónicas por referência a extensões telefónicas ou códigos individuais de utilizador. No caso de existir faturação detalhada, o empregador deve solicitar à operadora de telecomunicações que, nas faturas (em formato eletrónico ou em papel), os últimos quatro dígitos dos números chamados venham truncados.
(iii) Quanto à gravação de **chamadas telefónicas** só é admissível para as finalidades de (i) prova da relação contratual, (ii) chamadas de emergência e (iii) monitorização da qualidade do atendimento, nunca podendo ser utilizado para os fins de gestão de meios e controlo da produtividade do trabalhador. Caso tenha sido estabelecido o controlo das **chamadas realizadas** não devem ser tratados dados não necessários à realização da finalidade de controlo: o tratamento deve limitar-se à identificação do utilizador, à sua categoria/função, número de telefone chamado/recebido com supressão dos últimos quatro dígitos, tipo de chamada (local, regional e internacional), duração de chamada e custo de comunicação.
(iv) O prazo limite de conservação não deve exceder o período legal de pagamento da fatura.
(v) Em todo o caso há sempre a possibilidade de a empresa assegurar a existência de uma linha não conectada à central telefónica ou o acesso a serviço público de telecomunicações permitindo ao trabalhador uma forma de comunicação para fins pessoais.

2. Controlo de correio eletrónico e de dados de tráfego
As regras a estabelecer pela entidade empregadora devem respeitar o seguinte:
(i) O empregador não tem o direito de abrir automaticamente o correio eletrónico dirigido ao trabalhador.
(ii) Deve ser exigida aos trabalhadores a criação de pastas próprias devidamente identificadas, onde o trabalhador deve arquivar os emails de conteúdo pessoal.
(iii) Não deve ser feito um controlo permanente e sistemático dos emails dos trabalhadores.
(iv) O controlo deve ser pontual e direcionado para as áreas e atividades que apresentem maior risco para a empresa.
(v) Relativamente ao correio eletrónico de determinadas profissões, por exemplo médicos e jornalistas, dado o segredo profissional específico que impende sobre estes, o mesmo tem que ser preservado não devendo o conteúdo das suas mensagens ser acedido em circunstância alguma nem os dados de tráfego reveladores dos remetentes ou dos destinatários exteriores ser objeto de tratamento para fins de controlo.
(vi) O controlo deve ser realizado de forma aleatória.
(vii) A necessidade de **deteção de vírus ou outro tipo de software malicioso** não justifica a leitura dos emails recebidos.
(viii) A entidade empregadora pode adotar os procedimentos necessários para, com conhecimento dos trabalhadores, fazer uma filtragem de certos ficheiros que, pela natureza da atividade desenvolvida pelo trabalhador, podem indicar notoriamente, não se tratar de correios eletrónicos de serviço ex. ficheiros ".exe"; "mp3"; ou de imagens.
(ix) Os controlos fundamentados na prevenção ou deteção da divulgação de segredos comerciais devem ser direcionados exclusivamente para as pessoas que têm acesso a esses segredos e apenas quando existam fundadas suspeitas daquele facto.
(x) Em caso de utilização desproporcionada do correio eletrónico, que será apreciada em função da natureza e do tipo de atividade desenvolvida, é aconselhável a emissão de um aviso ao trabalhador.
(xi) Quanto às mensagens recebidas e mensagens enviadas: considerando que a entrada de correspondência na caixa de correio eletrónico do trabalhador ocorre independentemente da sua vontade, devem ser dadas instruções aos trabalhadores para que apaguem eventualmente mensagens recebidas que contrariem o Regulamento Interno.

(xii) O acesso ao correio eletrónico deve ser o último recurso a utilizar pela entidade empregadora devendo o mesmo ser feito na presença do trabalhador visado e de preferência na presença de um representante da comissão de trabalhadores ou de outra estrutura representativa (v.g. delegados sindicais) ou de alguém indicado pelo trabalhador. **O acesso deve limitar-se:** à visualização dos endereços dos destinatários, do assunto; e da data e hora do envio. O trabalhador pode se for o caso especificar a existência de algumas mensagens de natureza privada, caso ainda não tenha tido tempo para arquivar em pasta específica ou eliminar. Neste caso a entidade empregadora deve abster-se de consultar o conteúdo das mensagens, uma vez que o mero registo do envio das mesmas cumpre o objetivo do tratamento.
(xiii) Em **situações de ausência programada** (ex. férias, licença de paternidade,..) deve ser adotado um mecanismo de resposta automática de ausência (out of office reply) com indicação de endereço alternativo. A **entrada na caixa postal dos trabalhadores devido a ausência** tem de ser claramente explicitadas e deve ser realizado também na presença de um representante da comissão de trabalhadores ou de alguém indicado pelo trabalhador ou um delegado de proteção de dados (data protection officer).
(xiv) Email heritage: quando os trabalhadores saem da empresa deve dar-se um prazo para retirar o conteúdo de cariz pessoal dos arquivos do correio eletrónico, decorrido o qual o empregador deve eliminar a conta, para evitar que continue em funcionamento um endereço de correio eletrónico que já não é acedido pelo seu titular. Deve assegurar-se que o mesmo endereço eletrónico não será ulteriormente atribuído a outro trabalhador.

3. Controlo de navegação na Internet

A entidade empregadora deve assegurar que, tanto na elaboração como na divulgação do regulamento interno os trabalhadores **estão claramente informados e conscientes dos limites** estabelecidos em relação à utilização da internet para fins privados e que sabem quais as formas de controlo que podem ser adotadas.

Nestes termos, o controlo pode ser efetuado com as seguintes limitações:
(i) Deve existir um certo grau de tolerância relativamente ao acesso à Internet para fins privados, por exemplo, fora do horário de trabalho.
(ii) A entidade empregadora deve atuar de forma preventiva, dando preferência à implementação de um sistema de filtros que impossibilite a visita e a navegação de websites não autorizados pela entidade empregadora.
(iii) No regulamento devem ficar definidas as regras de utilização da Internet, nomeadamente os períodos em que se autoriza a utilização da internet para fins privados. Estas regras devem ter em conta os casos em que há trabalhos por turnos.
(iv) O controlo do acesso a internet não deve ser permanente e sistemático, mas antes **deve ser efetuado de modo global devidamente parametrizado**, a fim de se poder detetar eventuais desvios ou abusos às regras estabelecidas, por exemplo através da realização de estudos estatísticos. Não obstante, aceita-se que possa ser efetuado um tratamento estatístico dos sites mais consultados na empresa de forma a aplicar-se os respetivos filtros.
(v) Se estiverem em causa razões de produtividade ou de custos, o controlo do trabalhador deveser efetuado numa primeira fase através da contabilização do tempo médio de conexão à internet. Caso se verifiquem excessos deve ser efetuado um aviso ao trabalhador em relação ao grau de utilização. O controlo em relação ao tempo despendido na internet e aos sites consultados por cada trabalhador só deve ser efetuado em circunstâncias excecionais, designadamente por iniciativa do trabalhador, quando no contexto da sua advertência, aquele puser em causa as indicações da entidade empregadora e quiser conferir a realização de tais acessos.
(vi) Importa alertar, que o perfil pessoal do trabalhador é uma área que se considera estar na esfera da vida privada do trabalhador e como tal está fora do âmbito do artigo 22º, n.º2 do CT.

4. Acesso remoto ao computador do trabalhador

No que respeita ao acesso remoto ao computador do trabalhador, a entidade empregadora deverá respeitar o seguinte:
(i) Não é permitido a entidade empregadora utilizar sistemas ou aplicações que permitam visualizar, monitorizar ou seguir as ações dos trabalhadores nos seus computadores sem o seu conhecimento ou que permitam extrair informação pelos trabalhadores produzidas ou guardadas.
(ii) Este tipo de ferramentas só pode ser utilizado para assistência técnica, a pedido ou com o consentimento do trabalhador.
(iii) Mais, não é permtido o uso de sistemas que autorizem a pesquisa, a localização e a obtenção de dados e informações eletrónicas.
(iv) Importa referir que qualquer mecanismo adotado pela entidade empregadora referente às denominadas cópias de segurança deve garantir que não é acedida ou copiada informação de natureza privada.