COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

DELIBERAÇÃO n.º 1638/ 2013

Aplicável aos tratamentos de dados pessoais decorrentes do controlo da utilização para fins privados das tecnologias de informação e comunicação no contexto laboral

Considerando que:

1. A evolução tecnológica no domínio das comunicações traz novos e constantes desafios na relação laboral e na adaptação do Direito à realidade;
2. A «sociedade do conhecimento» assume hoje formas de expressão que têm elevado impacto no modo como os cidadãos e os agentes económicos se relacionam e, portanto, também no âmbito da relação ente entidades empregadoras e trabalhadores;
3. As tecnologias de comunicação, e o incremento da sua utilização, constituem um fator determinante para a modernização, a organização, o aumento da produtividade e competitividade das empresas, que simultaneamente podem ser utilizadas para potenciar um maior controlo dos trabalhadores em matéria de produtividade, na verificação do grau de eficiência e na apreciação da sua competência no desempenho das funções, e até na aferição do cumprimento das ordens e instruções da entidade empregadora;
4. A hodierna relevância das comunicações e a massificação da sua utilização no seio empresarial, seja através de telefones e telemóveis, seja através do correio eletrónico e da utilização da Internet – *maxime* das redes sociais –, implicam uma nova configuração de problemas jurídicos relacionados com a salvaguarda da privacidade, uma vez que o empregador tem a possibilidade fáctica de tratar e controlar os dados e conteúdos daquelas formas de comunicação, o que se traduz num verdadeiro tratamento de dados pessoais dos trabalhadores;

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

5. É, em consequência, fundamental garantir o justo equilíbrio entre a tutela da esfera jurídica do trabalhador e o princípio da liberdade de gestão empresarial e organização dos meios de trabalho que visem a promoção da produtividade e desenvolvimento da empresa, e especificamente conciliar estes princípios com os direitos fundamentais da reserva da intimidade da vida privada e da proteção de dados pessoais;
6. O artigo 8.º, n.º 1, da Convenção Europeia dos Direitos do Homem estabelece que qualquer pessoa tem direito à sua vida privada e familiar, do seu domicílio e da sua correspondência; e no ordenamento jurídico da União Europeia, o artigo 7.º da Carta dos Direitos Fundamentais da União Europeia impõe o «respeito pela vida privada e familiar, pelo seu domicílio e pelas suas comunicações» estando consagrado no artigo 8.º da mesma Carta e no artigo 16.º do Tratado sobre o Funcionamento da União Europeia o direito à proteção dos dados pessoais;
7. A Constituição da República Portuguesa (CRP), no catálogo formal dos direitos, liberdades e garantias, prevê o direito à reserva da vida privada e familiar e à proteção legal contra qualquer forma de discriminação (artigo 26.º), enquanto expressão da dignidade da pessoa humana, consagrada no seu artigo 1.º, bem como o direito à proteção dos dados pessoais (artigo 35.º);
8. A CRP determina ainda que *são nulas todas as provas obtidas mediante (...) abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações* (artigo 32.º, n.º 8) e *que o domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis* (artigo 34.º);
9. O tipo legal de crime previsto e punido nos termos definidos no artigo 194.º do Código Penal compreende qualquer intrusão nas comunicações, sejam elas telefónicas, eletrónicas ou outras (*v.g.*, *facebook*, *twitter*, salas de conversação

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

– *chats* –, entre outras), quando determinadas ou executadas pela entidade empregadora sobre o seu trabalhador;

10. No estrito plano da prova de condutas ilícitas, o artigo 189.º do Código de Processo Penal estende o regime nele previsto às comunicações eletrónicas ou de qualquer outra natureza. Ou seja, mesmo para o regime de prova em processo penal, a obtenção daqueles meios de prova não é generalizada e só pode ser ordenada ou autorizada por despacho do juiz, para certos tipos de crime e em relação a certas categorias de pessoas;
11. O artigo 2.º e 5.º da Lei n.º 67/98, de 26 de outubro, consagram princípios nucleares em matéria de proteção de dados, firmando-se que o tratamento de dados se deve processar «*de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias*»;
12. O Código do Trabalho (CT) contém disposições específicas relativas à tutela dos direitos de personalidade, as quais são expressão da tutela constitucional e civilística dos direitos de personalidade do trabalhador no quadro da relação laboral, com especial destaque para o direito à reserva da intimidade da vida privada, previsto no artigo 16.º do CT, e para proteção de dados pessoais dos trabalhadores, consagrada no artigo 17.º do CT;
13. A subordinação jurídica no âmbito da relação laboral, quando confrontada com a utilização das tecnologias e com o tratamento de dados pessoais do trabalhador, deve ser adequada às exigências legais atinentes ao regime de proteção de dados, assumindo particular relevância, nomeadamente, os princípios do fim, da adequação, da necessidade e da proporcionalidade, da transparência e da boa-fé, bem como os direitos de informação, acesso e oposição;

Entende a Comissão Nacional de Protecção de Dados que se impõe proceder à revisão da Deliberação de 29 de outubro de 2002, sobre *o tratamento de dados em centrais telefónicas, o controlo de e-mail e do acesso à Internet*.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Assim, tendo em conta:

- A Convenção 108 do Conselho da Europa, de 28 de janeiro de 1981, para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal, e o seu Protocolo Adicional, de 8 de novembro de 2001;

- A Carta Social Europeia (revista) do Conselho da Europa (CETS n.º 163), aprovada em Estrasburgo em 3 de maio de 1996;

- O artigo 8.º da Convenção Europeia dos Direitos do Homem, do Conselho da Europa, de 4 de novembro de 1950;

- Os artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia;

- O artigo 16.º do Tratado sobre o Funcionamento da União Europeia;

- A Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados;

- A Declaração sobre privacidade no trabalho da Organização Internacional do Trabalho, de 18 de junho de 1998;

- Os artigos 26.º, n.º1, 32.º, n.º 8, 34.º e 35.º da Constituição da República Portuguesa;

- A Lei n.º 67/98, de 26 de outubro, que transpõe para a ordem jurídica portuguesa a Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados;

- O artigo 80.º do Código Civil;

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

- O Código de Trabalho, aprovado pela Lei n.º 7/2009, de 12 de fevereiro, alterado pelas Leis n.ºs 105/2009, de 14 de Setembro, 53/2011, de 14 de outubro, e 23/2012, de 25 de junho, designadamente os seus artigos 10.º, 16.º, 17.º, 22.º, 97.º, 99.º, 106.º e 107.º;

A Comissão Nacional de Protecção de Dados (**doravante, CNPD**) delibera estabelecer as condições gerais para os **tratamentos de dados pessoais no âmbito do controlo da utilização para fins privados das tecnologias de informação e comunicação no contexto laboral.**

Não serão considerados nesta deliberação os tratamentos de dados pessoais resultantes dos sistemas de geolocalização, que serão objeto de deliberação específica da CNPD.

Capítulo I - O direito à privacidade dos trabalhadores no contexto da relação laboral

As características distintivas da relação laboral colocam vários desafios em matéria de proteção de dados, relativamente ao cumprimento das obrigações e exercício dos direitos das partes. Com efeito, o poder de direção representa, *ex vi* artigos 10.º e 97.º do CT, o direito da entidade empregadora fixar os termos em que deve ser prestado o trabalho, nos limites estabelecidos pelo contrato de trabalho e pelas normas que o regem – o que é, em certa medida, a concretização do disposto nos artigos 61.º (*direito à iniciativa privada*) e 62.º (*direito de propriedade privada*), ambos da CRP. Tal poder tem como limite os direitos e garantias do trabalhador, expressão da proteção jurídica que a lei e a Constituição a este conferem.

No que diz respeito ao controlo da utilização para fins privados das tecnologias de informação e comunicação no contexto laboral, há que encontrar a justa composição entre o direito à privacidade dos trabalhadores e a liberdade de gestão e organização

que é conferida pela lei aos empregadores, para o que importa considerar o artigo 22.º do CT.

O n.º 1 do artigo 22.º do CT consagra o princípio geral de confidencialidade das mensagens e acesso à informação, estando, por isso, vedado ao empregador o *acesso ao conteúdo das mensagens de natureza pessoal e à informação de carácter não profissional*, em caso de utilização pelo trabalhador dos meios de comunicação do empregador.

Com a ressalva deste limite, o n.º 2 do mesmo artigo reconhece ao empregador o poder de empreender formas de controlo decorrentes do estabelecimento de regras de conduta e de utilização dos meios de trabalho. Impõe-se assim determinar a extensão e o alcance do poder de estabelecer semelhantes regras bem como as condições que devem estar reunidas para a sua definição, para que as compressões dos direitos dos trabalhadores sejam ainda proporcionais à finalidade que prosseguem e respeitem o núcleo essencial dos direitos e liberdades daqueles.

Refira-se que fica fora do espectro do artigo 22.º, n.º 2, do CT qualquer mensagem ou comunicação que o trabalhador efetue através de contas de correio eletrónico, de 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. Está absolutamente vedada ao empregador qualquer forma de controlo do conteúdo da informação da área privativa do trabalhador enquanto utilizador de um daqueles serviços.

Questão prévia ao controlo pelo empregador dos meios de comunicação propriamente ditos centra-se na possibilidade ou admissibilidade da proibição de utilização dos meios do trabalho para fins pessoais. Num mundo cada vez mais dominado pelas tecnologias de informação e comunicação, em que os meios de comunicação são centrais no trabalho de qualquer empresa ou empregador, não se afigura lógico nem

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

realista que, no contexto da relação de trabalho, se proíba – de forma absoluta – a utilização de telefones e telemóveis, do correio eletrónico e o acesso à Internet para fins que não sejam estritamente profissionais.

Ademais, se o envio de correio eletrónico ou a realização de contactos telefónicos está no domínio do trabalhador, é manifestamente impossível que este possa controlar o correio eletrónico, os telefonemas ou mensagens que recebe na conta de correio ou nos telefones da empresa. Do mesmo modo, a definição de regras organizacionais no contexto laboral não pode ignorar os imponderáveis ou necessidades extraordinárias de utilização daqueles meios para fins que não sejam estritamente profissionais.

De resto, podendo não ser fácil por vezes estabelecer a fronteira entre uma comunicação pessoal ou profissional, sempre se dirá, na esteira do que já afirmou o Supremo Tribunal de Justiça[1], que devem ser encontradas formas equilibradas que possam conciliar os interesses do empregador e a realidade atual dos meios de comunicação. As supracitadas regras de utilização devem balizar o uso desses meios por parte do trabalhador, através de regulamento interno que disponha sobre essa matéria, nos termos do artigo 99.º do CT.

O amplo poder de organização reconhecido pelo CT à entidade empregadora há-de implicar que o correspondente poder de controlo do cumprimento das regras de organização tenha a medida necessária à efetivação daquele poder.

Mas a escolha dos meios de controlo por parte do empregador tem de obedecer aos princípios da necessidade, da proporcionalidade e da boa-fé, devendo este demonstrar que escolheu as formas de controlo com menor impacto sobre os direitos fundamentais dos trabalhadores.

---

[1] Acórdão de 5-07-2007, Processo 07S043, disponível em *www.dgsi.pt*.

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS

Capítulo II – Tratamento de dados: regime geral

A. Princípios jurídicos de proteção de dados

O controlo da utilização para fins privados das tecnologias de informação e comunicação no contexto laboral consubstancia um tratamento de dados pessoais, pelo que está submetido às disposições da Lei n.º 67/98, de 26 de outubro – a Lei de Proteção de Dados Pessoais (de ora em diante, LPD). De acordo com a alínea b) do n.º 1 do artigo 5.º da LPD, a recolha de dados deve visar finalidades determinadas, explícitas e legítimas, não podendo os dados ser tratados para alcançar objetivos incompatíveis com a finalidade (ou finalidades) que a justificou inicialmente.

Concretamente, os tratamentos de dados a ser efetuados no controlo da utilização para fins privados pelos trabalhadores das tecnologias de informação e comunicação no contexto laboral podem ter como finalidades a gestão dos meios da empresa e a produtividade dos trabalhadores.[2].

O princípio da proporcionalidade, previsto na alínea c) do n.º 1 artigo 5.º da LPD, reclama que os dados recolhidos sejam adequados a prosseguir a finalidade da sua recolha, e os estritamente necessários para o mesmo efeito, devendo, por isso, o tratamento de dados reduzir-se ao mínimo indispensável ao cumprimento da respetiva finalidade. Além disso, impõe-se ainda um último juízo de ponderação entre os benefícios obtidos com o tratamento e os prejuízos decorrentes para os direitos dos trabalhadores, de modo a garantir que o tratamento não seja excessivo.

---

[2] Destaca-se, como se referiu *supra*, que os tratamentos aqui considerados não abrangem os resultantes dos sistemas de geolocalização, os quais serão objeto de deliberação específica da CNPD.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Por aplicação deste princípio, os dados a tratar e os meios utilizados devem ser ajustados à organização da empresa, ao desenvolvimento da atividade produtiva e ser compatíveis com os direitos e obrigações dos trabalhadores consignados na legislação do trabalho; correspondendo a um "interesse empresarial sério" que, através do exercício dos poderes de direção e esperando a subordinação do trabalhador, tal tratamento não se revele abusivo e desproporcionado em relação à proteção da esfera privada do trabalhador.

Assim, a entidade empregadora deve privilegiar metodologias genéricas de controlo, afastando, sempre que possível, a consulta individualizada de dados pessoais. Uma adequada parametrização aplicada ao universo global dos trabalhadores (*v.g.,* quantidade, custo e duração de chamadas telefónicas, número de mensagens enviadas e tipo de ficheiros em anexo, tempo gasto em consultas na Internet) é suficiente para satisfazer os objetivos do controlo, permitindo detetar eventuais utilizações abusivas.

Por outro lado, sublinha-se que a entidade empregadora tem a possibilidade de aceder aos dados de tráfego[3] associados às comunicações realizadas pelos trabalhadores, na medida em que detém, na generalidade das situações, o seu registo. Ora, os dados de tráfego são dados igualmente abrangidos pelo sigilo das comunicações, pelo que os controlos individualizados não devem ocorrer.

Com efeito, neste contexto, impõe-se proteger em particular aqueles dados de tráfego que são reveladores de aspetos da vida privada do trabalhador, como sejam o número de telefone chamado, o endereço de correio eletrónico do destinatário ou a identificação do sítio da Internet visitado.

---

[3] O conceito de dados de tráfego é utilizado com o sentido definido na Lei n.º 41/2004, de 18 de agosto, com a redação que lhe foi dada pela Lei n.º 46/2012, de 29 de agosto.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

A este propósito, alerta-se para o facto de a extração de listagens de comunicações, mesmo que remetidas ao trabalhador para seu suposto controlo pessoal, configurar um tratamento de dados não consentâneo com os princípios da necessidade e da adequação, não devendo por isso realizar-se.

Nessa medida, considera-se que os intuitos do controlo serão alcançados com a adoção de mecanismos técnicos que possibilitem apenas o tratamento de alguns dados, tais como a hora e duração da comunicação, que dissociados da informação acima referida, não apresentam risco para a privacidade do trabalhador, enquanto permitem descobrir algum desvio às normas estabelecidas para a utilização dos meios da entidade empregadora.

Na verdade, o acesso sistemático ao registo das comunicações eletrónicas seria claramente desproporcional relativamente à finalidade que se pretende atingir além de violador da dignidade do trabalhador. A este propósito salienta ainda a Organização Internacional do Trabalho que este acesso pode, de igual modo, não se revelar eficaz e necessariamente produtivo, pelo "clima de angústia e tensão" que todos estes métodos podem criar no seio da empresa[4].

Em conformidade com o artigo 5.º, n.º 1, alínea e), da LPD, os dados pessoais tratados devem ser conservados apenas pelo período de tempo necessário à prossecução das finalidades do tratamento. A sensibilidade dos dados em causa compele à adoção de garantias reforçadas que minimizem efetivamente os riscos para a privacidade dos trabalhadores, pelo que o seu prazo de conservação deve ser curto.

Assim sendo, considera a CNPD que os dados pessoais tratados no âmbito do controlo da utilização, para fins privados, dos meios de informação e comunicação no

---

[4] Neste sentido, cf. o comentário do Código de Boas Práticas da Organização Internacional do Trabalho. *Protection of workers' personal data. An ILO code of practice*, Genebra, International Labour Office, 1997.

contexto laboral podem ser conservados pelo prazo máximo de 6 meses, sem prejuízo da sua manutenção no decurso de processo disciplinar ou judicial.

Também por força do princípio da boa-fé, tem de ser integralmente cumprido o dever de informação aos trabalhadores, em conformidade com os artigos 2.º, 5.º, n.º 1, alíneas a) e b), e 10.º da LPD e artigos 106.º e 107.º do CT. Deste modo, a entidade empregadora deve – antes de iniciar o tratamento – informar o trabalhador sobre as condições de utilização dos meios da empresa para fins privados e a realização do seu controlo (formas e metodologias adotadas), sobre a existência do tratamento de dados que lhe está associado, suas finalidades, os dados tratados e o seu tempo de conservação, bem como sobre o grau de tolerância admitido e as consequências da má utilização ou utilização indevida dos meios de comunicação colocados à sua disposição.

Sublinha-se que o direito de informação assume particular relevância neste tipo de tratamentos, na medida em que os referidos controlos são suscetíveis de ser efetuados sem que o trabalhador deles se aperceba.

B. Condições de legitimidade

Os dados de tráfego, bem como os dados contidos nas comunicações de natureza privada e outros dados de utilização das comunicações, constituem informação relativa a pessoas singulares identificadas ou identificáveis, a qual, por dizer respeito à vida privada dos trabalhadores, se enquadra no conceito de dados sensíveis, em conformidade com o disposto na alínea a) do artigo 3.º e n.º 1 do artigo 7.º da LPD.

Uma vez que o n.º 1 do artigo 7.º da LPD proíbe qualquer tratamento destes dados, o mesmo só pode ocorrer se se verificar alguma das situações previstas no n.º 2 do artigo 7.º da LPD.

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS

Em face do poder do empregador de estabelecer 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 da observância desses termos e regras, o fundamento de legitimidade para os tratamentos em causa reside na lei, *in casu*, no disposto nos artigos 22.º, n.º 2, e 97.º do CT.

O n.º 2 do artigo 7.º da LPD impõe ainda a garantia de não discriminação e a aplicação das medidas de segurança previstas no artigo 15.º da LPD.

C. Interconexões e comunicações de dados a terceiros

A interconexão de dados pessoais deve ser, nos termos do artigo 9.º, n.º 2, da LPD adequada à prossecução das finalidades legais e aos interesses legítimos dos responsáveis dos tratamentos, e não implicar discriminação ou diminuição de direitos, liberdades e garantias dos titulares dos dados.

O controlo legitimamente exercido pela entidade empregadora no contexto aqui em análise pretende atingir objetivos específicos, os quais são passíveis de ser plenamente alcançados sem necessidade de recurso a interconexões com outros tratamentos de dados, em particular da responsabilidade do mesmo empregador, como sejam as bases de dados de recursos humanos.

Tal interconexão apresentar-se-ia como desproporcional, tendo em conta o nível e o tipo de controlo permitido e a natureza dos dados em causa, os quais reclamam a adoção de formas menos intrusivas para garantir o interesse legítimo do empregador.

Sem prejuízo dos resultados do controlo serem eventualmente utilizados posteriormente, no âmbito de processo disciplinar, caso revelem utilização abusiva que se pretenda sancionar, o tratamento de dados para as finalidades acima descritas

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS

não pode ser sujeito a interconexões com outros tratamentos de dados da responsabilidade da entidade empregadora ou de terceiros.

No que diz respeito a comunicações de dados a terceiros, dada a natureza do controlo pretendido não existem situações que justifiquem, no âmbito dos tratamentos com esta finalidade, comunicações, nos termos da definição prevista na alínea f) do artigo 3.º da LPD, sem prejuízo das comunicações resultantes do cumprimento de obrigação legal no contexto de processo judicial.

D. Direito de acesso, retificação e eliminação

Ao abrigo do disposto no artigo 11.º da LPD, os titulares dos dados pessoais têm o direito de acesso aos dados que lhes digam respeito, bem como o direito à sua retificação, apagamento ou bloqueio se os dados objeto de tratamento não cumprirem o disposto na LPD.

A entidade empregadora deve assim informar os trabalhadores sobre as condições para o exercício destes direitos e facultar-lhes mediante pedido individual, livremente e sem restrições, com periodicidade razoável e sem demoras ou custos excessivos, as informações previstas nas alíneas a), b) e c) do n.º 1 do artigo 11.º da LPD.

E. Procedimentos a adotar pelas entidades empregadoras

O estabelecimento de regras de utilização dos meios de comunicação da empresa ou de organismo público, a delimitação das condições do tratamento de dados e a especificação das formas de controlo devem constar de Regulamento Interno, assim se cumprindo em parte, por esta via, o direito de informação consagrado no artigo 10.º da LPD. A elaboração do Regulamento obriga à audição, nos termos do artigo 99.º, n.º

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

2, do CT, da comissão de trabalhadores ou de outras estruturas representativas dos trabalhadores, caso esta não exista, e cuja produção de efeitos depende da publicitação do respetivo conteúdo e, nos termos previstos naquele Código, do envio para a Autoridade para as Condições do Trabalho.

Previamente à definição destas normas internas, deve o empregador avaliar o impacto que as medidas de controlo pretendidas poderão ter na privacidade dos trabalhadores e, em função disso, encontrar aquelas que sejam menos intrusivas para a privacidade dos trabalhadores, e que simultaneamente satisfaçam os legítimos objetivos da organização *(Privacy Impact Assessment).*

Nos termos dos artigos 27.º, n.º 1, e 28.º, n.º 1, alínea a), da LPD, as entidades empregadoras, enquanto responsáveis pelo tratamento de dados pessoais, devem proceder à sua notificação com vista à obtenção da competente autorização por parte da CNPD. Para este efeito, a CNPD disponibiliza no seu sítio da Internet, em http://www.cnpd.pt/bin/legal/forms.htm, um formulário específico para os tratamentos de dados neste âmbito.

F. Medidas de segurança

No que toca a medidas de segurança, deve o responsável, por em causa estarem dados sensíveis, cumprir o disposto no artigo 15.º da LPD.

Em especial, devem adotar-se medidas que impeçam o acesso à informação por pessoas não autorizadas, estabelecendo-se um perfil de acesso específico para as finalidades aqui em análise. Os acessos aos sistemas que registem estas informações só poderão ser efetuados com contas de utilizador que permitam identificar univocamente o indivíduo.

Tem de ser garantido um acesso restrito, sob o ponto de vista físico e lógico, aos servidores do sistema, os quais devem manter um registo de acesso à informação sensível para controlo das operações e para a realização de auditorias internas e externas.

Esta é uma questão primordial e essencial para a proteção de dados pessoais, pelo que um tratamento desta natureza tem, necessariamente, que possuir um sistema de auditoria fiável.

Assim, por forma a garantir a rastreabilidade dos acessos de monitorização impõe-se que os responsáveis parametrizem os sistemas para que os *logs* registem 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).

Os *logs*, para terem validade legal, têm de estar assinados digitalmente.

Deve o responsável identificar um conjunto de situações consideradas anómalas de forma a poder desenvolver um sistema de alarmes que permita identificar utilizações indevidas do sistema.

Deverá ser implementada uma política de análise de *logs,* com a realização de relatórios periódicos de análise, que devem ser mantidos para efeitos de fiscalização pela CNPD.

No que respeita à conservação destes *logs,* estabelece-se o prazo de um ano, atendendo ao prazo máximo de conservação dos dados e à natureza do tratamento.

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS

Capítulo III – Os tratamentos de dados em especial

A. Controlo de dados de comunicações telefónicas e de dados de tráfego

A entidade empregadora deve definir, com rigor, o grau de tolerância quanto à utilização dos telefones, fixos ou móveis, e as formas de controlo realizadas. Dificilmente será admissível que os trabalhadores sejam impedidos – no tempo e local de trabalho – de responder a necessidades estritamente privadas e que correspondem, em certa medida, à forma como se encontra estruturada a nossa sociedade. Há necessidades e problemas do dia-a-dia que não podem deixar de ser resolvidos e que podem implicar o recurso ao telefone do empregador durante o tempo e no local de trabalho.

De todo o modo, é em geral proibido o acesso ao conteúdo das comunicações, a utilização de qualquer dispositivo de escuta, armazenamento, interceção e vigilância de comunicações pelo empregador.

E, desde logo, há atividades profissionais em que o sigilo ou confidencialidade são essenciais ao desempenho da profissão. É o caso, designadamente, do segredo médico[5], sigilo profissional de advogado[6] ou de proteção de fontes, no caso de jornalistas[7]. Nestas atividades, 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, uma vez que semelhante tratamento coloca em causa os princípios constitucionalmente previstos relativos aos deveres de sigilo profissional

---

[5] Cfr. artigos 85.º e ss. do Código Deontológico da Ordem dos Médicos e o artigo 13.º, alínea c), dos Estatutos da Ordem dos Médicos.

[6] Cfr. artigo 87.º do Estatuto da Ordem dos Advogados.

[7] Cfr. artigo 11.º do Estatuto do Jornalista.

(que decorrem do artigo 26.º CRP) e à liberdade de imprensa (artigo 38.º, n.º 2, alínea b), da CRP)[8].

Nesse sentido, havendo faturação detalhada, deve o empregador garantir, através de solicitação junto do operador de telecomunicações, que os últimos quatros dígitos dos números chamados venham truncados na fatura, seja esta em formato eletrónico ou em suporte de papel.

A gravação de chamadas telefónicas só pode ocorrer nas situações e termos definidos na lei e concretizados na Deliberação n.º 629/2010 da CNPD, de 13 de setembro, que estabelece os princípios aplicáveis ao tratamento de dados de gravação de chamadas. Assim, este tratamento só é admissível para as finalidades de prova da relação contratual, chamadas de emergência e monitorização da qualidade do atendimento, nunca podendo ser utilizado para os fins de gestão de meios e controlo da produtividade do trabalhador (cf. artigo 20.º do CT), no contexto aqui em análise.

Caso tenha sido estabelecido o controlo de 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 da chamada e custo da comunicação.

Deve ser estabelecido um prazo limitado de conservação, que não deve exceder o período legal de contestação da fatura. Os motivos que presidem à liberdade de organização por parte da entidade empregadora não justificam que a conservação dos dados tratados para a finalidade de controlo dos dados de tráfego se estenda para além daquele prazo.

---

[8] Cf. J. J. GOMES CANOTILHO e VITAL MOREIRA, *Constituição da República Portuguesa Anotada,* Volume I, 4.ª edição revista, Artigos 1.º a 107.º, Coimbra, 2007.

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS

Pode ser equacionada, em função do tipo de empresa e de acordo com os princípios da proporcionalidade, a possibilidade de a empresa assegurar a existência de uma linha não conectada à central telefónica ou o acesso a serviço público de telecomunicações, de forma a permitir ao trabalhador uma forma de comunicação para fins pessoais, tomando em consideração necessidades, tal como referido *supra,* correspondentes à forma como a sociedade se estrutura nos dias de hoje.

B. Controlo de correio eletrónico e de dados de tráfego

Sejam quais forem as regras definidas pela empresa para a utilização do correio eletrónico para fins privados, o empregador não tem o direito de abrir, automaticamente, o correio eletrónico dirigido ao trabalhador. Não é o facto de certas mensagens ficarem gravadas em servidores da propriedade do empregador que lhe dá o direito de aceder àquelas mensagens, as quais não perdem a sua natureza pessoal ou confidencial, mesmo quando esteja em causa investigar e provar uma eventual infração disciplinar[9].

Mas deve ser exigida aos trabalhadores a criação de pastas próprias, devidamente identificadas, onde o trabalhador arquive os correios eletrónicos de conteúdo pessoal que constam da caixa de correio profissional.

Como se referiu, a entidade empregadora deve escolher metodologias de controlo não intrusivas, que estejam de acordo com os princípios previamente enunciados, *maxime*, o da proporcionalidade, e que sejam do conhecimento dos trabalhadores.

A entidade empregadora não deve fazer um controlo permanente e sistemático do correio eletrónico dos trabalhadores. O controlo deve ser pontual e direcionado para

---

[9] Cf. a argumentação expendida no acórdão do Tribunal da Relação de Lisboa de 7-03-2012, Processo 24163/09.0T2SNT.L1-4, disponível em *www.dgsi.pt*

as áreas e atividades que apresentem um maior "risco" para a empresa. O grau de autonomia do trabalhador e a natureza da atividade desenvolvida, bem como as razões que levaram à atribuição de um endereço de correio eletrónico àquele, devem ser tomadas em conta, decisivamente, em relação à forma como vão ser exercidos os poderes de controlo.

Também no que diz respeito ao correio eletrónico, o segredo profissional específico que impende sobre o empregado (*v.g.,* sigilo médico, sigilo profissional de advogado, ou segredo das fontes) tem de ser preservado, não devendo o conteúdo das suas mensagens ser acedido em circunstância alguma nem os dados de tráfego reveladores dos remetentes ou destinatários exteriores ser objeto de tratamento para fins de controlo.

Por princípio, o controlo dos correios eletrónicos deve ser realizado de forma aleatória.

Sublinha-se que a necessidade de deteção de vírus ou de outro tipo de *software* malicioso não justifica, só por si, a leitura dos correios eletrónicos recebidos.

A entidade empregadora pode adotar os procedimentos necessários para – sempre com o conhecimento dos trabalhadores – fazer uma «filtragem» de certos ficheiros que, pela natureza da atividade desenvolvida pelo trabalhador podem indiciar, notoriamente, não se tratar de correios eletrónicos de serviço (*v.g.,* ficheiros «.exe», .mp3 ou de imagens).[10]

Também eventuais 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.

---

[10] Cf. no mesmo sentido, PEDRO ROMANO MARTINEZ *et alii – Código do Trabalho Anotado, 5ª edição, pp 129 e 130.*

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Na verdade, a preservação de segredo comercial, industrial ou de propriedade intelectual deve ser realizada a montante, adotando as entidades empregadoras mecanismos estritos de controlo de acesso à informação sigilosa, minimizando deste modo eventuais riscos de divulgação indevida.

Perante a constatação 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.

É de diferenciar claramente o grau de exigência e de rigor em relação ao controlo das mensagens expedidas e recebidas, uma vez que a entrada de correspondência na caixa de correio eletrónico do trabalhador é independente da sua vontade. Por isso, devem ser dadas instruções ao trabalhador para que apague as mensagens eventualmente recebidas que contrariem o Regulamento Interno.

O acesso ao correio eletrónico deverá ser o último recurso a utilizar pela entidade empregadora, sendo necessário que seja 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 referido acesso deve limitar-se à visualização dos endereços dos destinatários, o assunto, a data e hora do envio, podendo o trabalhador – se for o caso – especificar a existência de algumas mensagens de natureza privada e que não pretende que sejam lidas pela entidade empregadora, caso ainda não tenha tido a oportunidade de os eliminar ou arquivar em pasta específica.

Perante tal situação, a entidade empregadora tem de abster-se de consultar o conteúdo das mensagens de correio eletrónico, uma vez que o mero registo do envio das mesmas cumpre o objetivo do tratamento. Eventual consulta constituirá um acesso não autorizado, porque extravasa a finalidade do tratamento. Impõe-se ao

empregador (e qualquer seu representante) que, tendo consciência da natureza pessoal de uma comunicação, desista da leitura do seu conteúdo e não o divulgue[11].

Nas situações de ausência programada (*v.g.,* férias, licença de parentalidade) deve ser adotado um mecanismo de resposta automática de ausência (*out of office reply*) com indicação de endereço alternativo.

As razões determinantes da entrada na caixa postal dos trabalhadores, com fundamento em ausência, têm de ser claramente explicitadas e semelhante controlo deve ser previamente comunicado ao trabalhador, e ser realizado também na presença de um representante da comissão de trabalhadores, ou de alguém indicado pelo trabalhador. Nos casos em que tal não seja possível e nas empresas que tenham um delegado de proteção de dados (*data protection officer*), será este o responsável por garantir que é cumprida a lei e que os direitos do trabalhador são acautelados, prevenindo acessos ilegítimos por parte da entidade empregadora.

É também necessário que sejam definidos procedimentos internos relativamente ao conteúdo de caixas de correio eletrónico de trabalhadores que saem da empresa. Nestes casos, deve dar-se um prazo ao trabalhador 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.

Além disso, o empregador deve assegurar que o mesmo endereço eletrónico não será ulteriormente atribuído a outro trabalhador *(email heritage)*.

---

[11] Ac. STJ de 5-07-2007, processo 07S043, disponível em *www.dgsi.pt*

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS

C. Controlo de navegação na Internet

A entidade empregadora deve, aquando da elaboração e divulgação do Regulamento Interno, assegurar-se que os trabalhadores estão claramente informados e conscientes dos limites estabelecidos em relação à utilização de Internet para fins privados e que conhecem as formas de controlo que podem ser adotadas.

Entende-se ser de admitir um certo grau de tolerância em relação ao acesso à Internet para fins privados, nomeadamente se este ocorrer fora do horário de trabalho.

A atuação da empresa deve centrar-se numa filosofia preventiva, dando-se preferência à criação de um sistema de filtros que impossibilite, à partida, a visita e a navegação de *websites* eventualmente não autorizados pelo empregador.

Qualquer decisão sobre a realização de controlo deve ser criteriosa e pautar-se pelo princípio da proporcionalidade, garantindo-se que a lesão a causar à privacidade e à autonomia dos empregados não seja superior aos benefícios que a entidade empregadora pretende obter.

Na definição das regras de utilização dos meios de comunicação, a entidade empregadora pode delimitar os períodos em que autoriza a utilização da Internet através dos meios da empresa. Essas regras devem tomar em consideração os casos em que há trabalho por turnos, adaptando a regulação da utilização aos tempos de trabalho dos funcionários.

A entidade empregadora não deve fazer um controlo permanente e sistemático do acesso à Internet. O controlo dos acessos à Internet – a ser decidido – deve ser feito de modo global devidamente parametrizado, a fim de poder detetar eventuais desvios ou abusos à norma estabelecida.

Desde logo, a realização de estudos estatísticos pode ser suficiente para a entidade empregadora se aperceber do grau de utilização da Internet no local de trabalho e em

que medida o acesso compromete a dedicação às tarefas profissionais ou a produtividade.

Admite-se, no entanto, que seja feito um tratamento estatístico dos sítios mais consultados na empresa, sem identificação dos postos de trabalho, para que possam ser aplicados os filtros que se tenham por convenientes.

Se estiverem em causa razões de custos ou de produtividade, o controlo do trabalhador deve ser feito, num primeiro momento, através da contabilização do tempo médio de conexão, independentemente dos sítios consultados.

Perante a verificação de acessos excessivos e desproporcionados deste meio de comunicação deve seguir-se um aviso ao trabalhador em relação ao grau de utilização.

O controlo em relação ao tempo de acesso diário e aos sítios consultados por cada trabalhador só deverá ser realizado em circunstâncias excecionais, nomeadamente 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.

Em particular, poderá ser necessário verificar as horas de conexão (início e fim) para comprovar que o acesso para fins privados ocorreu fora do horário de trabalho.

Mesmo que o trabalhador utilize a Internet no local de trabalho, em condições não permitidas pelo Regulamento Interno da Empresa, sublinha-se que o acesso ao perfil pessoal do trabalhador em redes sociais é proibido.

Nas redes sociais os perfis pessoais são espaços utilizados para expressar a individualidade de cada um, caindo no círculo restrito da reserva de intimidade da vida privada, contendo, por regra, informações de carácter pessoalíssimo, e mesmo íntimo.

O acesso a esta informação está manifestamente fora do espectro da norma ínsita no artigo 22.º, n.º 2, do CT.

D. Acesso remoto ao computador do trabalhador

O artigo 20.º do CT, sob a epígrafe *Meios de vigilância à distância*, consagra a proibição da utilização de meios tecnológicos de vigilância para controlar o trabalhador, apenas admitindo a utilização destes meios para a finalidade de proteção e segurança de pessoas e bens.

Assim, em caso algum será admissível a utilização pela entidade empregadora de sistemas ou aplicações que permitam visualizar, seguir ou monitorizar as ações que o trabalhador efetua no computador, sem o seu conhecimento, ou que permitam procurar e extrair informação por este produzida ou guardada.

Assim, é proibido o controlo à distância da atividade do trabalhador, através designadamente de ambientes de trabalho remotos ou partilha de ambiente gráfico, por exemplo *VNC – Virtual Network Computing*, que permitam acompanhar as ações e operações que o trabalhador leva a cabo no computador, seja em tempo real, seja em tempo diferido através da gravação daquelas operações.

Essas ferramentas só podem ser utilizadas para assistência técnica, a pedido ou com o conhecimento do trabalhador, de todas as vezes que ocorra esse tipo de intervenção.

Também não é admissível que a entidade empregadora recorra a sistemas que permitam a pesquisa, localização e obtenção de dados e informações eletrónicas (*Electronically Stored Information*), o que abrange todo o tipo de ficheiros e mensagens de correio eletrónico, nos computadores da organização.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Estes sistemas possibilitam, de modo centralizado e à distância, automatizar o varrimento de informação em qualquer computador ou outro tipo de máquina acessível na rede interna e efetuar pesquisas por documentos ou mensagens em função de expressões selecionadas, sendo que os referidos documentos podem ser copiados e guardados centralmente, sem que o trabalhador disso se aperceba.

Quaisquer mecanismos adotados pela entidade empregadora, relativamente à realização de cópias de segurança da informação contida nos computadores individuais atribuídos aos trabalhadores ou à centralização em arquivo geral de documentação profissional dispersa, devem garantir que não é acedida e copiada informação de natureza privada.

Para este efeito, tais procedimentos devem prever a existência de uma separação inequívoca de pastas pessoais e profissionais, ser transparentes e claramente descritos aos trabalhadores, com prestação de informação e orientação prática quanto à forma correta de arquivar eventuais documentos privados.

As entidades empregadoras que pretendam efetuar o controlo da utilização para fins privados das tecnologias de informação e comunicação devem observar as condições e limites estabelecidas na presente Deliberação.

*Aprovada na sessão plenária da CNPD de 16 de Julho de 2013