

DISSERTAÇÃO DE MESTRADO

**A ADMISSIBILIDADE DO CONTROLO ELECTRÓNICO PELO EMPREGADOR E
O RESPECTIVO PROCEDIMENTO**

- Acesso à Internet e ao *E-mail* -

UNIVERSIDADE CATÓLICA PORTUGUESA
FACULDADE DE DIREITO

Estudos Avançados em Direito do Trabalho

Mestrado

Direito do Trabalho na Empresa

Coordenação científica: Professor Doutor Bernardo Xavier

Vice-Coordenação: Professora Doutora Joana Vasconcelos

Orientação: Professora Doutora Joana Vasconcelos

Mestranda: **Paula Raquel de Almeida Reis Martins**

Data de conclusão: 10 de Janeiro de 2014



UNIVERSIDADE
CATÓLICA PORTUGUESA | FACULDADE
DE DIREITO
ESCOLA DE LISBOA

Aos meus Pais

Agradecimentos

Ao Senhor Professor Doutor Bernardo Xavier, por toda a dedicação, presença e ensinamentos com que nos presenteou.

À Senhora Professora Doutora Joana Vasconcelos, pela sua orientação, sempre precisa e pertinente, e pela paciência e dedicação que depositou no meu trabalho.

Aos Professores do Curso de Estudos Avançados de Direito do Trabalho que leccionaram no ano 2011-2012, por todos os ensinamentos que nos transmitiram.

Aos Colegas deste Curso, pela troca de conhecimentos e companheirismo.

À Dra. Elisabete Pereira, pelo apoio, orientação e troca de conhecimentos que me transmitiu, não apenas durante este trabalho mas também ao longo da minha jornada profissional.

Às pessoas com quem desenvolvo a minha actividade profissional, pelas oportunidades e pela compreensão.

À Caixa Central – Caixa Central de Crédito Agrícola Mútuo, C.R.L., minha entidade empregadora, pelo apoio concedido para a realização deste trabalho.

À minha família, pelo apoio incondicional, paciência e carinho que sempre demonstraram ao longo da minha jornada pessoal e profissional.

Aos meus amigos, pelo companheirismo e amizade, oportunos em todas as ocasiões.

Ao Marco, pelo incentivo, compreensão e confiança que deposita em mim.

LISTA DE ABREVIATURAS

Art. – Artigo

Cfr. – Conforme

CNPD – Comissão Nacional de Protecção de Dados

CRP – Constituição da República Portuguesa

CT – Código do Trabalho

***E-mail* – (inglês) electronic mail, correio electrónico**

***Ex vi* – (latim) por força de**

NTIC – Novas Tecnologias de Informação e Comunicação

N.º – Número

***Op. cit.* – (latim) *opus citatum*, obra já citada anteriormente pelo mesmo Autor**

Por ex. – Por exemplo

Segs. - Seguintes

***Site* – (inglês) sítio electrónico**

***Spam* – (inglês) lixo electrónico**

***Supra* – (latim) ver acima**

V. - Ver

***V.g.* – (latim) *verbi gratia*, por exemplo**

“The principle that a man’s home is his castle is under a new attack. For centuries the law of trespass protected a man’s lands and his home. But in this age of advance technology, thick walls and locked doors cannot guard our privacy or safeguard our personal freedom”
(Presidente Americano Lyndon Johnson ⁽¹⁾)

⁽¹⁾ *Apud* François Blanchette, *L’expectative raisonnable de vie privée et les principaux contextes de communications dans Internet*, tese de Mestrado em Direito, Montreal, 2001, in www.juriscom.net, p. 17, Teresa Alexandra Coelho Moreira, in “A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: contributo para um estudo dos limites do poder de controlo electrónico do empregador”, Almedina, 2010, p. 54.

ÍNDICE

	PÁGINA
Introdução	8
Capítulo I – Assento Legal	11
I. As principais disposições internacionais e europeias	11
II. As principais disposições nacionais – A protecção da privacidade no ordenamento jurídico português	13
Capítulo II – “Princípios sobre a Privacidade no Local de Trabalho” – Comissão Nacional de Protecção de Dados (CNPd)	17
Capítulo III – Dados Pessoais e Tratamento de Dados Pessoais	18
Capítulo IV – O Poder de Controlo Electrónico e os Poderes de Direcção, Disciplinar e Regulamentar do Empregador	23
Capítulo V – Caracterização da Posição Jurídica – Balanço dos Interesses Procedimentais – Os Interesses do Empregador e os Direitos do Trabalhador	30
Capítulo VI – Vantagens da utilização da Internet e do <i>e-mail</i> para fins pessoais e adopção de normas regulamentares	35
Capítulo VII – O Controlo Electrónico efectuado pelo Empregador	38
Princípios Gerais na execução do controlo electrónico	42
I. Princípio da Finalidade	43
II. Princípio da Transparência	43
II. Princípio da Proporcionalidade	44
Capítulo VIII – A utilização do <i>e-mail</i>	47
<i>E-mails</i> pessoais e <i>e-mails</i> profissionais	47
Capítulo IX – O Procedimento atinente ao exercício do poder de controlo pelo Empregador	54
I. Envolvimento do Trabalhador	54

Direito de Informação	54
Consentimento	55
Presença do Trabalhador no acesso ao <i>e-mail</i>	57
Direito de oposição	57
II. Envolvimento das Estruturas de Representação Colectiva dos Trabalhadores (ERCT's) ..	58
III. Intervenção de Entidades Terceiras	59
III.1. Autoridade para as Condições do Trabalho (ACT)?	59
III.2. Comissão Nacional de Protecção de Dados (CNPD)	59
Capítulo X – Responsabilidade Contra-Ordenacional e Penal	64
I. Vícios	64
Contra-ordenações	64
Crimes	64
II. Nulidade da prova	65
III. Controlo formal	66
III.1. Indeferimento do pedido de autorização para o tratamento de dados pessoais	66
III.2. Aplicação de coimas	67
IV. Controlo substantivo	67
V. Acção de tutela da personalidade do trabalhador	68
Conclusão	70
Bibliografia	78
Anexos	
Anexo I – Assento Legal	
I – A protecção da privacidade no Direito Internacional	82
II – A protecção da privacidade no Direito Europeu	83
III – A protecção da privacidade no Ordenamento Jurídico Português	85
Anexo II – “Princípios sobre a privacidade no local de trabalho” – Comissão Nacional de Protecção de Dados (CNPD)	92
Adenda – Deliberação n.º 1638/2013, de 16 de Julho – Comissão Nacional de Protecção de Dados (CNPD)	94

INTRODUÇÃO

A era das novas tecnologias deu já lugar à sucessora Sociedade de Informação ⁽²⁾ ⁽³⁾, sendo indiscutível que a disseminação das comunicações electrónicas e a vulgarização do acesso à Internet, e a todas as demais formas e tecnologias de informação, obriga hoje à identificação das fronteiras e dos limites legítimos que salvaguardam a utilização das ferramentas electrónicas.

A sociedade está, pois, a transformar-se numa sociedade de rotulagem, de classificação, de perfis presumidos, de pessoas virtuais ou electrónicas, em detrimento de pessoas reais.

Efectivamente, ter acesso a tecnologias de informação equivale a uma acrescida aquisição de conhecimento e conseqüentemente de poder. O empregador é, hoje em dia, detentor de um poder quase inimaginável sobre os seus trabalhadores. Mas até que ponto ser-lhe-á legítimo exercer um poder de controlo de natureza “inspectiva” sobre o trabalhador?

Questões determinantes para o presente trabalho, consistem, então, em apurar quando e quanto pode o empregador, dentro do poder directivo que a lei lhe confere, exercer um poder de controlo específico, e de natureza “inspectiva”, do acesso e do uso do *e-mail* e da internet por parte do trabalhador. Esta questão torna-se pertinente se considerarmos que, quotidianamente, o trabalhador utiliza esses meios electrónicos quer a nível profissional, como ferramenta de trabalho, quer a nível pessoal. De facto, actualmente, embora o *e-mail* e a internet constituam a ferramenta de trabalho, por excelência, no âmbito das actividades económicas do sector terciário, não podemos deixar de considerar que os mesmos têm, igualmente, uma importante e imprescindível utilização pessoal e social.

⁽²⁾ Segundo José de Oliveira Ascensão, in “A Sociedade da Informação” in “Direito da Sociedade da Informação”, Volume I, Coimbra Editora, 1999, pp. 163-184, “«Sociedade da Informação» não é um conceito técnico: é um *slogan*. Melhor se faria até em *sociedade da comunicação*, uma vez que o que se pretende impulsionar é a comunicação, e só num sentido muito lato se pode qualificar toda a mensagem como informação”.

⁽³⁾ O “Livro Verde para a Sociedade de informação em Portugal” (disponível em <http://www.acessibilidade.gov.pt/docs/lverde.htm>), da responsabilidade da Missão para a Sociedade da Informação, aprovado pelo Conselho de Ministros no dia 17 de Abril de 1997 e publicado pelo Ministério da Ciência e da Tecnologia, refere-se a um “modo de desenvolvimento social e económico em que a aquisição, armazenamento, processamento, valorização, transmissão, distribuição e disseminação de informação conducente à criação de conhecimento e à satisfação das necessidades dos cidadãos e das empresas, desempenham um papel central na actividade económica, na criação de riqueza, na definição da qualidade de vida dos cidadãos e das suas práticas culturais.

Torna-se óbvio que esta nova sociedade é controlada pela informação, que se assume como a matéria-prima essencial do processo produtivo, tal como a energia assumia este mesmo papel no modelo da sociedade do passado, que está ainda muito recente e para muitas pessoas presente. Alguns preferem chamar-lhe «Estado Digital», dominado pela informação e pelas tecnologias associadas, as Tecnologias de Informação e de Comunicações”.

Centrando-nos no caso específico das relações jurídicas decorrentes de um contrato individual de trabalho, constatamos que estes novos meios de comunicação são, tendencialmente, os meios exclusivos de comunicação quer interna quer externa, bem como as fontes de recolha e de produção de informação, o que torna necessárias normas que claramente prevejam e resolvam situações de possíveis conflitos de direitos.

É indiscutível que as novas tecnologias de informação têm um carácter ambivalente: simultaneamente, servem como instrumento para desempenhar a actividade produtiva e como mecanismo de controlo da prestação de trabalho executada pelo trabalhador. Este poder de controlo e vigilância do empregador configura-se tradicionalmente como uma manifestação do poder directivo. Mas se o controlo por parte do empregador não é novo nem proibido, a novidade provém do facto de surgirem novas tecnologias que têm uma maior efectividade de controlo e uma maior capacidade de recolher dados que, por vezes, parece não ter limites. As novas tecnologias criaram, pois, formas mais sofisticadas e efectivas de controlar os trabalhadores, permitindo, ao contrário da vigilância tradicional, um controlo total, ou quase total, de todos os seus movimentos, tornando-se quase “transparentes” para os seus empregadores.

Não nos referimos apenas ao controlo da localização física do trabalhador, mas sim do próprio processo de trabalho, a um controlo que poderá permitir ao empregador um conhecimento do modo de pensar daquele, para além do que lhe é legítimo, ultrapassando a barreira da privacidade.

A introdução das novas tecnologias de informação na sociedade actual permitiu, pois, ao empregador ter acesso a um conjunto de informação obtida através de meios céleres e de baixo custo, os quais lhe dão acesso à reconstrução de um “perfil” dos seus trabalhadores, o qual poderá não corresponder inteiramente à realidade. Mas será esse o cerne do controlo pelo empregador, ou melhor, será que estaremos, ainda, no âmbito do poder de controlo? Até que ponto os objectivos, nomeadamente, económicos das empresas e a assunção do risco por parte das mesmas legitimam o empregador a tornar o trabalhador transparente aos seus olhos?

Mais à frente tentaremos resolver a questão da legitimidade e do âmbito em que o empregador pode exercer esse controlo. De todo o modo, parece-nos poder concluir-se que, hoje em dia, o empregador tem, no plano fáctico, a possibilidade de exercer um controlo total, ou quase total, sobre o trabalhador, ainda que, no plano jurídico, esteja impedido de o fazer. Ainda que o empregador tenha de obedecer a regras aquando do seu poder de controlo sobre o trabalhador, a lei não tem como o impedir de extrapolar esse controlo. Por outro lado, a CNPD tem uma natureza regulamentar mas não inspectiva.

Note-se que o carácter imperceptível desta forma de controlo, sem que os trabalhadores estejam conscientes da mesma, aliado ao facto de o empregador ter a possibilidade de ordenar que se reproduza, no seu próprio computador, uma cópia exacta dos conteúdos que um determinado trabalhador visualize, seguindo todos os seus movimentos, dificulta bastante a protecção dos direitos legalmente tutelados.

Vivemos, de facto, numa época de vigilância, de controlo, de um certo *Big Brother*, de um ambiente “fechado”, desconfiado, com o objectivo supremo da segurança e da prossecução dos objectivos económicos da empresa. Mas até que ponto poderá esta tão aclamada segurança sobrepor-se à privacidade? Até que ponto o direito à segurança (e a própria competitividade da empresa) defendido pelo empregador imporá um afastamento do direito à privacidade?

Este tema do controlo à distância levanta, certamente, inúmeras questões, nomeadamente as relacionadas com a videovigilância. No entanto, o presente trabalho cingir-se-á ao controlo electrónico efectuado no âmbito das relações laborais, no seio de uma empresa, tendo em consideração a relação empregador-trabalhador.

Sabemos que as tecnologias de informação evoluem de forma bastante mais célere do que o próprio Direito, pelo que se torna necessário compreendermos em que medida pode o empregador socorrer-se dos instrumentos tecnológicos que tem ao seu alcance por forma a detectar eventuais incumprimentos ou ilegalidades praticadas pelos seus trabalhadores.

A questão em análise no presente estudo prende-se, pois, com a identificação dos limites dos poderes do empregador (poder directivo, poder disciplinar e poder regulamentar) e dos limites do direito à privacidade, como direito fundamental, intimamente ligado à dignidade da pessoa humana.

Nesta medida, o âmago do presente estudo consiste em estabelecer-se quais os meios idóneos para que o empregador possa dar sequência à satisfação das suas pretensões de controlo electrónico sem que sejam feridos os direitos legalmente tutelados dos trabalhadores. Ou seja, é objectivo desta tese perceber-se, face à lei vigente, se a disponibilização a um trabalhador de meios electrónicos, como sucede no caso do *e-mail* e da internet, permite ou não que o seu empregador possa, a todo o momento, e sem restrições, controlar, visualizar os acessos e o uso que aquele faz dessas ferramentas.

Esta matéria do controlo electrónico do trabalhador é bastante extensa, e com inúmeras questões por explorar. Porém, o que propomos, neste trabalho, é um olhar actual e atento à admissibilidade da prova obtida através da visualização da correspondência trocada pelo trabalhador mesmo via *e-mail* e das consultas efectuadas na Internet.

CAPÍTULO I

ASSENTO LEGAL

I. AS PRINCIPAIS DISPOSIÇÕES INTERNACIONAIS E EUROPEIAS ⁽⁴⁾

O desenvolvimento e o aperfeiçoamento das novas tecnologias e a aplicação das suas potencialidades no controlo dos trabalhadores têm suscitado um grande debate quer ao nível das Organizações Internacionais quer ao nível dos vários Estados da União Europeia. “Não havendo, em regra, disposições legais expressas que estabeleçam as condições de utilização e controlo dos meios que a empresa coloca à disposição do trabalhador – tanto mais que se trata de instrumentos que são propriedade do empregador – tem havido uma preocupação em compatibilizar os legítimos interesses e poderes da entidade empregadora com uma certa autonomia, iniciativa e prudente utilização dos meios da empresa por parte dos trabalhadores” ⁽⁵⁾.

Analisada a questão no âmbito das disposições patentes no Direito Internacional, verificamos que o direito à privacidade tem um reconhecimento relativamente recente, principalmente a partir do final da II Guerra Mundial. O primeiro registo data de 2 de Maio de 1948, com a Declaração Americana dos Direitos e Deveres do Homem. Mais tarde, ainda no ano de 1948, surgiu a Declaração Universal dos Direitos do Homem, cujas disposições, embora não tendo carácter vinculativo, influenciaram outros diplomas normativos internacionais.

Os principais documentos de Direito Internacional relativos à protecção dos Direitos do Homem (Declaração Universal dos Direitos do Homem e Pacto Internacional relativo aos Direitos Cívicos e Políticos) ainda não contêm referências expressas relativamente à protecção de dados pessoais, não obstante protejam expressamente a privacidade. No entanto, a sua interpretação ao longo do tempo acabou por se estender igualmente àquela protecção.

⁽⁴⁾ Os principais instrumentos normativos, a nível internacional e europeu, encontram-se sistematizados no Anexo I deste trabalho.

⁽⁵⁾ Amadeu Guerra, *in* “A privacidade no Local de Trabalho – As Novas Tecnologias e o Controlo dos Trabalhadores através de Sistemas Automatizados – Uma abordagem ao Código do Trabalho”, Almedina, 2004, p. 299.

Organizações internacionais

Também as Organizações internacionais adoptaram instrumentos protectores do cidadão relativamente ao tratamento de dados pessoais: a OCDE ⁽⁶⁾ aprovou um conjunto importante de Linhas directrizes; as Nações Unidas aprovaram igualmente Linhas directrizes nesta matéria; o Acordo de *Schengen* ⁽⁷⁾ e a respectiva Convenção de Aplicação ⁽⁸⁾; as disposições da OMC ⁽⁹⁾; e as disposições da OIT ⁽¹⁰⁾.

Todos estes instrumentos contribuíram para a legislação nacional em matéria de protecção de dados pessoais.

DIREITO EUROPEU

O Tribunal Europeu dos Direitos do Homem tem entendido, de forma pacífica, que a protecção da “vida privada”, com assento no artigo 8.º da Convenção Europeia dos Direitos do Homem (Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais), não se confina à habitação, podendo ser aplicável, igualmente às relações estabelecidas no local de trabalho.

O direito europeu mais recente [Convenção para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal (Convenção 108 do Conselho da Europa)] já prevê a protecção da privacidade na perspectiva do seu tratamento. Nesta Convenção foram consagrados princípios fundamentais de protecção dos dados pessoais que vieram, posteriormente, a ser integrados na Directiva 95/46/CE, tais como os princípios da finalidade, da adequação e da pertinência, ou garantias como a da informação e da rectificação dos dados, bem como regras para os fluxos transfronteiras de dados.

O principal elemento de regulação desta matéria consiste na Directiva 95/46/CE, do Parlamento e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Da sua transposição, resultou a Lei n.º 67/98, de 26 de Outubro, Lei da Protecção de Dados Pessoais.

⁽⁶⁾ Organização para a Cooperação e Desenvolvimento Económico.

⁽⁷⁾ Assinado no Luxemburgo, em *Schengen*, a 14 de Junho de 1985.

⁽⁸⁾ De 19 de Junho de 1990.

⁽⁹⁾ Organização Mundial do Comercio.

⁽¹⁰⁾ Organização Internacional do Trabalho. Em 7 de Outubro de 1996, a Organização Internacional do Trabalho fez uma recolha de directivas práticas, as quais tinham como objectivo fundamental fornecer orientações sobre a protecção de dados pessoais dos trabalhadores.

II. AS PRINCIPAIS DISPOSIÇÕES NACIONAIS – A PROTECÇÃO DA PRIVACIDADE NO ORDENAMENTO JURÍDICO PORTUGUÊS ⁽¹¹⁾

Para se falar em protecção da privacidade, temos, em primeiro lugar, de concluir se esta é necessária, ou seja, se, perante um efectivo controlo e vigilância do empregador, subsiste a necessidade de protecção da privacidade do trabalhador. Há, pois, que resolver, em primeira instância, a questão de saber se esse poder de controlo e vigilância cabe ou não dentro do poder directivo conferido ao empregador. E, só posteriormente, resolver a questão dos limites desse poder directivo, no sentido de ser um direito que possa afastar ou limitar o direito à reserva da intimidade da vida privada.

Por um lado, parece pacífico concluir-se que é legítimo ao empregador verificar se as suas ordens estão a ser cumpridas correctamente e se os instrumentos de trabalho facultados ao trabalhador estão a ser utilizados da forma expectável. Mas em qualquer circunstância?

Sabemos que o poder de controlo e vigilância do empregador sobre a actividade prestada pelo trabalhador é uma manifestação do seu poder directivo, sem o qual este seria esvaziado de sentido, que tem uma existência legitimada constitucional, legal e contratualmente, e que constitui um elemento natural e próprio da relação de trabalho, atribuindo ao empregador a faculdade de verificar se as suas ordens e instruções estão a ser cumpridas correctamente. Ao contrário do contrato de prestação de serviços, em que existe uma obrigação de resultado, no contrato de trabalho, está em causa a própria actividade do trabalhador, e o cumprimento adequado da mesma. Mas quais os limites deste poder de controlo? Esta questão toma uma dimensão acrescida quando temos actualmente um conjunto de novas tecnologias que têm uma enorme efectividade de controlo e de recolha de dados.

Por outro lado, o direito à reserva sobre a intimidade da vida privada está directamente relacionado com o direito à dignidade da pessoa humana (artigo 1.º da CRP) e com os direitos da personalidade. Nos termos do artigo 18.º, n.º 1 da CRP, os “direitos, liberdades e garantias” “são directamente aplicáveis e vinculam entidades públicas e privadas”. Ora, a CRP contém preceitos que prevêm outros direitos fundamentais que se relacionam com aqueles, como o direito à inviolabilidade do domicílio e da correspondência (artigo 34.º), a proibição do tratamento informático de dados referentes à vida pessoal (artigo 35.º), a nulidade da prova obtida mediante intromissão abusiva na vida privada, no domicílio, na correspondência ou nas telecomunicações (artigo 32.º, n.º 8), e a restrição em matéria de

⁽¹¹⁾ Os principais normativos internos nesta matéria encontram-se sistematizados no Anexo I deste trabalho.

intimidade das pessoas, relativa ao direito de acesso aos arquivos e registo administrativos (artigo 268.º, n.º 2).

Portugal foi o primeiro Estado europeu que reconheceu de forma expressa no seu texto constitucional um direito à protecção de dados pessoais, distinto do direito à reserva sobre a intimidade da vida privada. Com efeito, desde a sua versão originária de 1976, que a CRP consagra, no seu artigo 35.º, um direito à autodeterminação informativa.

Por sua vez, o direito ao sigilo da correspondência e de outras comunicações privadas, previsto no artigo 34.º da CRP abrange as correspondências efectuadas por meio das telecomunicações. A protecção deste direito diz respeito não só ao conteúdo da correspondência mas também ao próprio tráfego, ou seja, à espécie, hora, duração e intensidade da utilização.

Por sua vez, o Código Civil consagra o direito à privacidade desde 1966.

No entendimento de Teresa Coelho Moreira⁽¹²⁾, que perfilhamos, “o art. 80.º, n.º 1 do Código Civil não pode ser entendido como proibindo apenas a divulgação de aspectos da vida privada. Há também que considerar-se interdito o acesso a estas informações e a intromissão abusiva na vida privada. A reserva sobre a intimidade da vida privada pode ser violada tanto pela entrada dos outros no seu domínio particular, invadindo-o, como pela divulgação de informações, ou seja, «por se arrancar a pessoa àquela área de intimidade e se expor, assim, na «praça pública», a ela e àquilo que é seu»⁽¹³⁾. Especial relevância neste acesso tem a informática, de importância crescente na nossa sociedade, que possibilita, por vezes, uma invasão da privacidade das pessoas. O legislador português não foi alheio a esta nova realidade e legislou neste sentido, primeiro através da L. n.º 19/91, de 29 de Abril, de protecção dos dados pessoais face à informática, revogada e substituída pela L. n.º 67/98, de 26 de Outubro, Lei da Protecção de Dados Pessoais, que transpôs para o nosso ordenamento jurídico a Directiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à sua livre circulação”.

⁽¹²⁾ In Teresa Coelho Moreira, *op. cit.*, p. 322.

⁽¹³⁾ Teresa Coelho Moreira, *op. cit.*, p. 322, *apud* Paulo Mota Pinto, in “O direito à reserva sobre a intimidade da vida privada”, BFDUC, n.º 69, 1993, pp. 533-534.

A Lei n.º 67/98, de 26 de Outubro aplica-se não só a tratamentos de dados pessoais quando realizados por meios automatizados ou parcialmente automatizados, mas também aos tratamentos realizados por meios não automatizados, contidos em ficheiros manuais.

O princípio geral que deve reger o tratamento de dados pessoais encontra-se no artigo 2.º desta Lei, segundo o qual “o tratamento de dados pessoais deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais.”

No que respeita à utilização e controlo das NTIC, nomeadamente do *e-mail* e da Internet, no local do trabalho, existe, no ordenamento jurídico português, uma norma específica: o artigo 22.º do CT.

A regulação prevista no CT “resulta também das necessidades sentidas actualmente, onde o grande desafio do Direito do Trabalho é o de conseguir encontrar um modo de compatibilizar a competitividade das empresas com os direitos de cidadania e a dignidade dos trabalhadores, tendo em atenção que um certo grau de controlo e de tratamento de dados pessoais constitui uma normal e indispensável característica do contrato de trabalho.”⁽¹⁴⁾. É indiscutível que o empregador tem necessidade de ter acesso, regularmente, a determinadas informações, de saber como se está a desenvolver a relação de trabalho e se está a ser realizada de acordo com as directrizes por si definidas. Mas também não podemos esquecer que os direitos de personalidade do trabalhador são fundamentais na dignidade da pessoa humana e não deixam de existir só pelo facto de estarmos perante uma relação de trabalho” Nessa relação de trabalho, naturalmente que o empregador tem uma posição de supremacia em relação ao trabalhador, que se encontra subordinado aos poderes daquele. Ao inserir-se na organização produtiva empresarial, hierárquica, o trabalhador abdica necessariamente de alguma da sua liberdade individual. É neste ponto que o Direito do Trabalho é essencial no sentido de delimitar os limites aos poderes do empregador sobre o trabalhador, considerado por natureza a parte mais dependente e mais fragilizada da relação de trabalho.

Mas o poder do empregador não é absoluto, No âmbito da relação de trabalho, existem, de facto, alguns requisitos para o exercício do poder de direcção do empregador. Assim, por exemplo, o trabalhador poderá recusar legitimamente cumprir uma ordem que seja contrária aos seus direitos de personalidade, podendo igualmente interpor uma acção judicial

⁽¹⁴⁾ In Teresa Coelho Moreira, *op. cit.*, p. 338.

fundamentada em tal ordem, ou em ordem cujo cumprimento tenha como consequência a existência de um perigo para a sua saúde. Neste sentido, o artigo 128.º, n.º 1, alínea e) do CT prevê como dever do trabalhador a obediência a ordens “respeitantes à execução ou disciplina do trabalho, bem como a segurança e saúde no trabalho que não sejam contrárias aos seus direitos ou garantias”. Este preceito prevê também a desobediência legítima a ordens ilegítimas ou contrárias à lei, tendo o trabalhador o direito de chamar a atenção do empregador e manifestar-lhe que não pretende cumprir tal ordem. Deste modo, se o empregador sancionar o trabalhador pelo não cumprimento de tais ordens, tal sanção é considerada abusiva [cfr. artigo 331.º, n.º 1, alínea b) do CT]. No mesmo sentido dispõe o artigo 21.º da CRP. Existindo tal sanção, considerada abusiva nos termos legais, e, por tal, ferida de nulidade, deverá o empregador repor a situação tal como se ela não tivesse existido, tendo ainda o trabalhador o direito de resolução do contrato de trabalho com justa causa, de acordo com o disposto no artigo 394.º, n.º 2, alíneas c) e f) do CT, bem como o direito a uma indemnização calculada nos termos do artigo 396.º, n.º 1 do CT.

CAPÍTULO II

“PRINCÍPIOS SOBRE A PRIVACIDADE NO LOCAL DE TRABALHO” – Comissão Nacional de Protecção de Dados (CNPd) ⁽¹⁵⁾

No âmbito do exercício das suas competências, entre as quais se destacam a divulgação e o esclarecimento dos direitos relativos à protecção de dados [alínea p) do n.º 1 do artigo 23.º da Lei n.º 67/98], a Comissão Nacional de Protecção de Dados, órgão de controlo do respeito pelas disposições em matéria de protecção de dados pessoais, aprovou, em sessão plenária de 29/10/2002, um documento intitulado “Princípios sobre a privacidade no local de trabalho”, referente ao tratamento de dados em centrais telefónicas, ao controlo do *e-mail* e do acesso à Internet, cujo conteúdo se encontra publicitado no seu *site* da Internet (www.cnpd.pt).

Embora não tendo a natureza de normas legais, estes “Princípios” têm uma função orientadora para as empresas que pretendem proceder ao tratamento de dados pessoais.

No Anexo II deste trabalho, podemos observar alguns dos princípios gerais que esta Comissão tem identificado, designadamente no que respeita à utilização e controlo de *e-mail* e de Internet.

Cumpre-nos referir que aquela Comissão aprovou, na sua sessão plenária de 16 de Julho, a Deliberação n.º 1638/2013, que veio rever o documento *supra* mencionado sobre a mesma matéria, e cujo texto foi apenas divulgado no passado dia 14 de Novembro.

Ora, não obstante assinalarmos as novas orientações determinadas pela CNPD, em Adenda a este trabalho, é de ter em atenção que não foram as mesmas consideradas ao longo do mesmo, dada a respectiva publicação ter ocorrido em data coincidente com o momento final da entrega deste.

⁽¹⁵⁾ Por uma razão de simplificação, ao longo da exposição que se segue, a alusão a estes “Princípios sobre a Privacidade no Local de Trabalho” será efectuada pela expressão “Princípios da CNPD”.

CAPÍTULO III

DADOS PESSOAIS E TRATAMENTO DE DADOS PESSOAIS

As operações de tratamento, especialmente quando afectam alguns direitos dos trabalhadores (v.g. a sua intimidade ou privacidade), devem assentar em disposições legais. Mas o CT contém disposições demasiado genéricas nesta matéria, tendo o nosso legislador, ainda, um longo percurso pela frente.

As operações que consistem no tratamento de dados pessoais [ou seja, “qualquer operação ou conjunto de operações sobre dados pessoais, efectuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição”, cfr. dispõe o artigo 3.º, al. b) da Lei n.º 67/98, de 26 de Outubro] estão sujeitas, por via de regra, a uma notificação à Comissão Nacional de Protecção de Dados (cfr. dispõe o artigo 27.º, n.º 1 da Lei n.º 67/98, de 26 de Outubro), isto é, o tratamento dos dados tem de ser levado ao conhecimento desta entidade, mediante envio de um formulário de legalização devidamente preenchido.

“A criação e a manutenção de um conjunto estruturado de dados pessoais, pelos perigos que pode constituir para os titulares dos dados, é uma tarefa de responsabilidade. Todos os que pretendam realizá-la ficam sujeitos a obrigações importantes de cujo incumprimento resultam várias sanções. Para que se possa saber quais os tratamentos que estão sujeitos a notificação é desde logo necessário saber o que são dados pessoais. Depois, identificar-se-ão os tratamentos de dados que estarão isentos dessa notificação, bem como os que, segundo a lei, não são abrangidos pelo regime jurídico de protecção de dados especialmente previsto”⁽¹⁶⁾.

Dispõe a Lei n.º 67/98, de 26 de Outubro [artigo 3.º, al. a)], que “para efeitos da presente lei, entende-se por: a) «Dados pessoais»: qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável a pessoa que possa ser identificada directa ou indirectamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social”.

Assente-se que quando os dados não permitam identificar uma pessoa, mesmo que sejam

⁽¹⁶⁾ Catarina Sarmiento e Castro, *in* “Direito da Informática, Privacidade e Dados Pessoais”, Almedina, 2005, p. 65.

dados que se referem, em abstracto, a pessoas, não são dados pessoais: é o caso dos dados estatísticos que não permitem “voltar” a saber a quem se referiam.

Nos termos da Directiva 95/46/CE e da Lei da Protecção de Dados Pessoais, são exemplos de dados pessoais, naturalmente, o nome, mas também a morada e outros dados de identificação, tais como o número de segurança social, o número de contribuinte, o número de Bilhete de Identidade, de passaporte, ou até de cliente de estabelecimento comercial, assim como o número de telefone, o *e-mail*, uma chapa de matrícula, o valor de uma retribuição, o som da voz registada para permitir o acesso a uma conta bancária, desde que, por estarem associados a uma pessoa, estes permitam identificá-la. “É também o caso de uma impressão digital, de uma imagem biométrica do rosto, de uma imagem recolhida através do uso de uma câmara, como nos casos da videovigilância, ou de um conjunto de fotografias divulgadas na Internet. São dados pessoais, quando permitam identificar uma pessoa – desde logo se surgem associados a nome – as suas classificações escolares e *curriculum*, a sua história clínica, as suas dívidas e créditos, as compras que efectua, o registo dos meios de pagamento que utiliza, etc.”⁽¹⁷⁾.

Apercebido que está o conceito de “dados pessoais”, cumpre atentar que, de entre os dados pessoais, a Lei distingue os denominados “dados sensíveis”, quando, no artigo 7.º daquele diploma, sob a epígrafe “Tratamento de dados sensíveis”, estabelece uma proibição de tratamento relativamente a dados pessoais referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, bem como o tratamento de dados relativos à saúde e à vida sexual, incluindo os dados genéticos. Com efeito, a CRP, a Directiva 95/46/CE e a Lei da Protecção de Dados Pessoais, embora admitindo excepções, consagram uma proibição geral de tratamento de dados que revestem uma especial sensibilidade, sendo, por isso, considerados dados sensíveis.

Desde logo, o artigo 35.º, n.º 3 da CRP, estabelece igualmente a proibição desse tratamento de dados, quando referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.

Também a Directiva se referiu a categorias específicas de dados pessoais, proibindo, no seu

⁽¹⁷⁾ Catarina Sarmento e Castro, *op. cit.*, p. 74.

artigo 8.º o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde ou à vida sexual. Apesar desta Directiva não ter previsto expressamente a protecção da vida privada, no texto desse preceito, secundando as palavras de Catarina Sarmiento e Castro, “a explicação possível para a solução adoptada parece ser esta: os dados de saúde, os dados relativos à vida sexual, os dados genéticos, que a Lei também inclui entre os dados sensíveis, são, todos eles, dados acerca da vida privada.”⁽¹⁸⁾.

Sucedem que “muitas vezes, um tratamento de dados pode estar estruturado de modo a, aparentemente, não constituir um tratamento de dados sensíveis. Imagine-se uma listagem de nomes de alguns habitantes de uma cidade, à primeira vista inócua. Mas se essa listagem for constituída apenas pelos nomes que possam ser associados a uma certa origem étnica, o uso que do nome se faz permite qualificar uma tal listagem como um conjunto de dados sensíveis, ainda que deles apenas conste o nome. Apesar de o nome, em si mesmo, não ser um dado sensível, em certas circunstâncias torna-se idóneo para revelar certas características de especial sensibilidade que podem ser utilizadas como factor de discriminação, pelo que, nessas circunstâncias, o seu tratamento deve ser considerado proibido, salvo nos casos excepcionais previstos na Lei”⁽¹⁹⁾. É, pois, crucial entendermos que, não obstante uma recolha de dados ser aparentemente “inofensiva” a título de tratamento de dados pessoais, poderemos estar, designadamente, perante um conjunto de dados que, na realidade, têm como objectivo a identificação de um grupo étnico ou racial, pelo que qualquer tratamento de dados (como por exemplo uma simples recolha, destruição ou consulta de nomes de pessoas) deverá ser objecto da maior atenção por parte de quem faz esse tratamento, pois poderá estar-se perante uma proibição legal sancionada com pena de prisão ou multa (como veremos mais à frente).

Qualquer operação de tratamento de dados pessoais dos trabalhadores, efectuada pelo empregador, para exercer qualquer forma de controlo - por mínimo ou pontual que seja - está sujeita à observância, em toda a sua plenitude, da Lei n.º 67/98, assumindo aquele a qualidade de responsável, na acepção do artigo 3.º, al. d), uma vez que é quem determina as finalidades e os meios afectos ao tratamento.

⁽¹⁸⁾ Catarina Sarmiento e Castro, *op. cit.*, p. 96.

⁽¹⁹⁾ Catarina Sarmiento e Castro, *op. cit.*, p. 89.

No entanto, “nem todas as formas de tratamento se podem revelar ajustadas ao cumprimento da finalidade que a empresa se propõe realizar. Pode ser suficiente o registo generalizado dos dados, sem que se revele necessária a consulta específica dos dados pessoais.”⁽²⁰⁾. Por exemplo, poderá ser suficiente para o empregador satisfazer a sua necessidade de controlo sobre a actividade prestada pelo trabalhador a verificação do número de chamadas telefónicas feitas por uma determinada extensão, do número de *e-mails* enviados por um determinado endereço electrónico, do valor global gasto em determinado período com o telemóvel cedido por aquele, do tempo gasto em consultas na Internet.

É, ainda, de atentar que, não obstante a regra de notificação dos tratamentos prevista no artigo 27.º da Lei n.º 67/98, a mesma Lei prevê que a CNPD possa isentar desta notificação certos tratamentos de dados pessoais, quando, atendendo aos dados a tratar, não sejam aqueles susceptíveis de pôr em causa os direitos e liberdades dos titulares dos dados. Fundamento de tais isenções será também a necessidade de celeridade, economia e eficiência.

As seis isenções de notificação actualmente previstas foram publicadas no Diário da República n.º 22, 2.ª Série, de 22 de Janeiro de 2000, e foram estabelecidas ao abrigo do n.º 2 do art.º 27.º. Nos termos das isenções, estão dispensados de notificação:

- O processamento de retribuições, prestações, abonos de funcionários ou empregados;
- A gestão de utentes de bibliotecas e arquivos;
- A facturação e gestão de contactos com clientes, fornecedores e prestadores de serviços;
- A gestão administrativa de funcionários, empregados e prestadores de serviços;
- O registo de entradas e saídas de pessoas em edifícios;
- A cobrança de quotizações em associações e contactos com os respectivos associados.

Note-se, contudo, que um tratamento de dados apenas poderá considerar-se isento de notificação quando respeite os limites previstos no texto da isenção, mantendo-se as obrigações nele mencionadas, desde logo, *v.g.*, a garantia do direito de informação do titular dos dados pessoais.

A publicidade imposta a qualquer tratamento de dados obriga a que mesmo no caso em que um tratamento de dados esteja isento de notificação, deva o responsável pelo mesmo prestar a qualquer pessoa que lho solicite, informação adequada (artigo 31.º, n.º 3 da Lei da Protecção de Dados) sobre:

⁽²⁰⁾ Amadeu Guerra, *op. cit.*, p. 60-61.

- a)* O responsável do ficheiro e, se for caso disso, o seu representante;
- b)* As categorias de dados pessoais tratados;
- c)* As finalidades a que se destinam os dados e as categorias de entidades a quem podem ser transmitidos;
- d)* A forma de exercício do direito de acesso e de rectificação;
- e)* Eventuais interconexões de tratamentos de dados pessoais;
- f)* Transferências de dados previstas para países terceiros.

Note-se que o não cumprimento desta obrigação e publicidade faz incorrer o responsável pelo tratamento na prática da contra-ordenação prevista no artigo 38.º, n.º 1 da Lei n.º 67/98, de 26 de Outubro.

CAPÍTULO IV

O PODER DE CONTROLO ELECTRÓNICO E OS PODERES DE DIRECÇÃO, DISCIPLINAR E REGULAMENTAR DO EMPREGADOR

Os poderes do empregador assumem várias vertentes: o poder de direcção (como o poder de comando sobre os subordinados por ocasião do trabalho, o poder determinativo das suas funções), o poder regulamentar (como o direito de elaborar o regulamento interno) e o poder disciplinar (como a faculdade de aplicar determinadas sanções aos seus trabalhadores).

Dentro do poder de direcção, o poder organizativo, que se revela de todo o interesse para esta exposição, é determinante na delimitação dos objectivos e da política empresarial e na estruturação e rentabilidade dos factores de produção. Nele se inclui, ainda, a escolha do tipo de serviços e a arquitectura de telecomunicações a adoptar, a forma de estruturação do sistema de informação, a definição da segurança física, a definição de políticas de publicitação da actividade da empresa ou de comunicação com o exterior. No âmbito deste poder, é ainda ao empregador que cabe definir os meios de tratamento de dados pessoais e as finalidades determinantes do mesmo [cfr. artigo 3.º, al. d) da Lei n.º 67/98].

Para além da necessidade e interesse em saber se o trabalhador dedica as suas horas de trabalho à prestação de trabalho para que foi contratado ou a actividades extra-laborais que o distraem dos objectivos pretendidos pela empresa, bem como o tempo direccionado a tais actividades, e da necessidade e interesse em saber se as suas ordens e instruções estão a ser integralmente cumpridas por aquele trabalhador (o que permitirá efectuar uma melhor avaliação de desempenho daquele, e abrir-lhe á caminho à aplicação de medidas atinentes à alteração das suas funções, ou no limite, ao seu despedimento, por incumprimento dos deveres laborais a que legalmente está vinculado), o empregador pode ter ainda outros legítimos interesses em pretender controlar o uso destes novos meios de informação e comunicação por parte dos trabalhadores, desde logo porque a existência de Internet numa empresa coloca sérios riscos para o empregador, exponencialmente elevados com a facilidade e rapidez de transmissão que aquela oferece, começando com os relacionados com a espionagem industrial, a transmissão de informações confidenciais, bem como o aumento da vulnerabilidade da empresa que fica exposta a uma série de possíveis ataques externos. Amadeu Guerra defende que “a divulgação de um segredo comercial ou industrial, a revelação de informações que possam lesar interesses patrimoniais sérios da empresa ou a produção e difusão de mensagens injuriosas em relação aos superiores hierárquicos e à

entidade patronal podem comprometer a subsistência da relação laboral e, por isso, integrar justa causa de despedimento (cfr. artigo 396.º do CT)”⁽²¹⁾.

Para além desse aspecto, “as empresas podem ainda alegar razões de funcionamento para fazerem uso destas novas possibilidades de controlo, na medida em que o correcto e eficiente funcionamento do sistema informático pode ver-se alterado como consequência de determinadas actividades dos trabalhadores, sendo que o uso destes meios informáticos para fins privados ainda pode aumentar mais esta possibilidade, pois pode originar problemas no funcionamento da rede, ou uma redução da velocidade do sistema, assim como da sua capacidade.

Por outro lado, outro motivo de preocupação está também relacionado com determinadas situações que podem colocar em causa a «imagem pública» da empresa, na medida em que as circunstâncias em que se definem estes novos sistemas fazem com que se tornem canais especialmente aptos para certas condutas que fazem quase desaparecer certos bens considerados fundamentais, quer seja por difamação ou discriminação ou, simplesmente, porque se trata de comunicações que podem ofender certas pessoas por razões, *v.g.* de raça, sexo, orientação sexual, idade, deficiência e religião. E se o *e-mail* é o da empresa, este uso pode afectar a sua imagem, principalmente se o trabalhador utiliza este *e-mail* para enviar mensagens com certo conteúdo. Não nos podemos esquecer que, ao enviar um *e-mail* com o endereço electrónico que lhe foi fornecido pela empresa, é como se o trabalhador estivesse a utilizar o logótipo da empresa. Nestes casos o nome da empresa vê-se directamente relacionado com as opiniões difundidas que, em função do seu conteúdo, podem prejudicá-lo comercialmente e causar danos à sua imagem externa, podendo, igualmente, criar um ambiente de trabalho desagradável ou repercutir-se negativamente na normal convivência de quem presta serviços à empresa”⁽²²⁾.

O problema essencial reside na diferenciação que, a nosso ver, tem de ser imposta ao trabalhador: a diferenciação entre a sua vida pessoal e a sua vida profissional. A distinção entre as horas de trabalho e as horas de lazer.

É, pois, problemática a questão de saber se a entidade patronal pode, e em que circunstâncias, ter acesso ao conteúdo do *e-mail* utilizado pelo trabalhador. Não ignoramos, porém, que o conteúdo de um *e-mail* possa ser decisivo em relação à escolha da sanção disciplinar a aplicar

⁽²¹⁾ *Op. cit.*, p. 390.

⁽²²⁾ Teresa Coelho Moreira, *op. cit.*, pp. 618-619.

a um trabalhador, nomeadamente quando a entidade patronal verifica que o número de *e-mails* expedidos é significativo em relação ao “grau de tolerância” permitido, quando permitido. É de salientar que, para além do dever de obediência, o trabalhador deve “velar pela conservação e boa utilização dos bens relacionados com o seu trabalho que lhe forem confiados pelo empregador” [artigo 128.º, n.º 1, al. g) do CT].

No âmbito do seu poder de direcção, “compete ao empregador estabelecer os termos em que o trabalho deve ser prestado, dentro dos limites decorrentes do contrato e das normas que o regem” (artigo 97.º do CT).

Em anotação a esse preceito legal, *in* “Código do Trabalho Anotado”⁽²³⁾, Pedro Madeira de Brito menciona Maria do Rosário Palma Ramalho (“Direito do Trabalho”, II, 3.ª Edição Coimbra, 2010, p. 685 e segs.), segundo a qual “o conteúdo do poder de direcção tem três manifestações essenciais: a de determinação da função do trabalhador, a conformação da actividade laboral em concreto e o poder de vigilância ou de controlo do modo de cumprimento da prestação do trabalho.” Na perspectiva da autora, estas manifestações do poder directivo encontrar-se-iam respectivamente nos artigos 115.º, n.º 1 e 2 (sob a epígrafe “Determinação da actividade do trabalhador”), 97.º (ao prever que compete ao empregador estabelecer os termos em que o trabalho deve ser prestado, dentro dos limites decorrentes do contrato e das normas que o regem) e sem norma expressa quanto ao poder de fiscalização.

Ora, sendo a obrigação de prestar trabalho subordinado uma obrigação de conteúdo indeterminado, tal indeterminação é resolvida com recurso ao poder de direcção do empregador, enquanto expressão característica da posição ocupada pelo empregador na situação jurídica laboral, que administra a relação de trabalho, concretiza a actividade do trabalhador resolvendo tal indeterminação e adapta a sua prestação, dentro dos limites fixados no contrato.⁽²⁴⁾

Ora, a definição da actividade contratada pode ser feita por remissão, tal como prevê o n.º 2 do citado artigo 115.º do CT., para instrumento de regulamentação colectiva de trabalho ou para regulamento interno de empresa.

⁽²³⁾ “Código do Trabalho Anotado”, Almedina, 2013, de Pedro Romano Martinez, Luís Miguel Monteiro, Joana Vasconcelos, Pedro Madeira de Brito, Guilherme Dray e Luís Gonçalves da Silva,

⁽²⁴⁾ Em anotação ao artigo 115.º do CT, Pedro Madeira de Brito, *op. cit.*, adopta, neste sentido, o entendimento de Bernardo da Gama Lobo Xavier (“A mobilidade funcional e o artigo 22.º da LCT”, RDES, 1997, 1/2/3, 51-130).

Paralelamente ao poder de direcção, o empregador tem o poder de disciplinar sobre o trabalhador ao seu serviço, enquanto vigorar o contrato de trabalho. Com a versão de 2009 do CT, este poder deixou de estar inserido no Capítulo referente ao incumprimento do contrato de trabalho (como sucedia na sua versão de 2003), como um poder existente apenas no âmbito de um incumprimento contratual por parte do trabalhador, gerador de infracção disciplinar, para estar inserido dentro do Capítulo referente ao contrato de trabalho e, mais especificamente, ao empregador e à empresa, o que sugere que o seu conteúdo não se limita a sancionar incumprimentos contratuais, mas também a poder prever, disciplinar comportamentos do trabalhador que revelem incumprimentos de regulamentos internos, por exemplo.

Complementarmente ao poder regulamentar, este poder do empregador possibilita-lhe a elaboração de normas e a previsão e aplicação de sanções decorrentes da violação das mesmas, nomeadamente quando decorrentes de um regulamento interno de empresa, nos termos consignados no artigo 99.º do CT, segundo a qual a sua eficácia depende actualmente do conhecimento do seu conteúdo por parte dos trabalhadores (ao contrário do que se verificava antes da entrada em vigor da Lei n.º 23/2012, de 25 de Junho, em que era condição de eficácia daquele o seu envio à ACT). Segundo Pedro Madeira de Brito ⁽²⁵⁾, “o poder regulamentar existe na justa medida em que o contrato de trabalho e as normas que o regem o permitem, e tem fundamento na existência de uma relação laboral e versa sobre a organização e disciplina do trabalho. Tratam-se fundamentalmente de disposições que emanam do poder de organizar a empresa e portanto correspondem a regras de natureza organizatória, bem como a regras de disciplina. Maria do Rosário Palma Ramalho ⁽²⁶⁾ entende que o poder regulamentar é reconduzido a uma manifestação do poder directivo, mas igualmente do poder disciplinar.

Entendemos que o poder de controlo electrónico do empregador fundamenta-se nestes poderes que elencámos, numa perspectiva de decorrência do conjunto desses três poderes. O poder de vigilância ou de controlo do modo de cumprimento da prestação do trabalho, como manifestação do poder directivo, fundamenta a sua legitimidade igualmente no poder disciplinar, e encontra a sua consagração mais evidente no poder regulamentar, na emissão de regras de conduta para os trabalhadores.

⁽²⁵⁾ In “Código do Trabalho Anotado”, *op. cit.*, p. 276.

⁽²⁶⁾ In “Direito do Trabalho – Parte II – Situações Laborais Individuais, Almedina, Coimbra, 2006, p. 589.

O n.º 4 do artigo 99.º ao dispor que “a elaboração de regulamento interno de empresa sobre determinadas matérias pode ser tornada obrigatória por instrumento de regulamentação colectiva de trabalho negocial” poderá tornar-se, julgamos, um forte aliado na protecção dos interesses do empregador e, igualmente, do trabalhador, no âmbito do poder electrónico efectivado sobre a utilização do *e-mail* e o acesso à Internet, protegendo ambas as partes da relação contratual contra a indeterminação dessa utilização e acesso.

Ainda, nos termos do n.º 3 do referido artigo 115.º do CT, o contrato de trabalho confere automaticamente ao trabalhador os poderes de representar o empregador, salvo quando a lei exija instrumento especial. Assim sendo, o trabalhador não necessita de invocar que age em nome empregador nem os seus actos necessitam de ratificação por parte deste (conforme poderia resultar do artigo 1180.º do Código Civil). Ora, a imposição de elaboração de um regulamento interno de empresa, tornada obrigatória por um instrumento de regulamentação colectiva de trabalho negocial simplificaria a defesa do empregador perante uma eventual responsabilidade do empregador por actos praticados pelo trabalhador, no âmbito da relação comitente-comissário, isto é, uma responsabilidade do empregador por actos praticados pelos seus trabalhadores (cfr. artigo 500.º do Código Civil). Como vimos anteriormente, existem vários requisitos para a verificação desta responsabilidade: a existência de uma comissão (o contrato de trabalho); a prática do acto ilícito no exercício da função (independentemente de ter sido intencional ou contra as instruções do empregador). Mas se, perante tais circunstâncias, o empregador provar que o trabalhador praticou o facto danoso fora das suas funções, ou seja, por ocasião das mesmas e não no seu exercício, a sua responsabilidade ficará afastada, e a consagração de um regulamento interno de empresa que determine as condições e consequências do uso daqueles meios de comunicação facilitaria, em muito, a salvaguarda da sua posição. Do lado do trabalhador, também este beneficiaria com tal regulamentação, com a determinação e informação das regras de conduta a que está adstrito e com a previsão da possibilidade de controlo sobre *e-mails* determinados.

No Acórdão do Tribunal da Relação do Porto, de 08/02/2010, processo número 452/08.0TTVFR.P1, em que foi relatora a Juíza Desembargadora Paula Leal de Carvalho e publicado em www.dgsi.pt, encontramos uma citação de Joana Vasconcelos ⁽²⁷⁾, segundo a qual o empregador pode, em geral, estabelecer regras quanto à utilização de meios de

⁽²⁷⁾ In “O Contrato de Trabalho; 100 Questões”, Universidade Católica Editora, 3.ª Edição, 2010, pp.103 a 104“.

comunicação (telefone; fax; telemóvel; correio electrónico) e de tecnologias de informação (ligações à Internet), pertencentes à empresa, sendo que a existência de tais regras, bem como o controlo do seu respeito pelos trabalhadores, não afecta o direito à reserva e à confidencialidade que a nossa lei garante relativamente a mensagens pessoais e à informação não profissional que o trabalhador receba, consulte ou envie, designadamente através de correio electrónico.

O artigo 22.º, n.º 2 do CT não estabelece a forma pela qual tais regras devem ser concebidas e comunicadas, pelo que “vigora o princípio do consensualismo: qualquer meio utilizado será lícito, desde que se revele adequado para que se torne possível o seu conhecimento por parte dos trabalhadores da empresa. Admite-se, porém, que o regulamento da empresa se afigure o meio por excelência a adoptar para o efeito.”⁽²⁸⁾”

Do documento aprovado pela Comissão Nacional de Protecção de Dados (CNPd), na sessão plenária de 29 de Outubro de 2002, no âmbito dos “Princípios gerais relativos à utilização e controlo do *e-mail* e Internet”, salientamos o seguinte:

“A entidade empregadora deverá analisar todos os factores – a salvaguarda da liberdade de expressão e de informação, a formação, o livre desenvolvimento e iniciativa do trabalhador, a sua sensibilização para acesso às redes públicas, os custos para a empresa, as políticas de segurança, de privacidade e o grau de utilização destes meios, o tipo de actividade e grau de autonomia dos seus funcionários, bem como as suas necessidades concretas e pessoais – para definir regras claras e precisas em relação à utilização do correio electrónico e da Internet para fins privados”; “Estas regras – que não podem ser desenquadradas da prática institucionalizada e das necessidades particulares dos trabalhadores - devem assentar nos princípios da adequação, da proporcionalidade, da mútua colaboração e da confiança recíproca”.

Deverá, pois, o empregador elaborar um documento que vise regular o âmbito de acesso e utilização da Internet e dos meios de comunicação de correio electrónico, indicando-se quais

⁽²⁸⁾ Anotação de Guilherme Dray ao artigo 22.º do CT, in “Código do Trabalho Anotado”, Almedina, 2013, de Pedro Romano Martinez, Luís Miguel Monteiro, Joana Vasconcelos, Pedro Madeira de Brito, Guilherme Dray e Luís Gonçalves da Silva.

os métodos de controlo a estabelecer (tendo por base os “Princípios da CNPD”), e que deverá ser sujeito à apreciação dessa Comissão.

Este documento deverá identificar, em concreto, quais são as formas de controlo existentes, bem como qual é a margem de acesso que é consentida ao trabalhador para uso privado.

Deverá expressamente prever que o empregador poderá, a todo o tempo, proceder a alterações do seu clausulado, cabendo-lhe contudo informar, prévia e posteriormente, o trabalhador das alterações introduzidas.

É ainda essencial que neste documento se prevejam mecanismos para situações de ausências dos trabalhadores – nomeadamente, em caso de férias, suspensões do contrato por doença e licenças – em que pode ser necessário, sob pena de informações importantes não poderem ser recebidas em tempo útil, que o empregador aceda ao correio electrónico dos trabalhadores: convém, porém, que os trabalhadores visados sejam previamente alertados para essa possibilidade e que, preferencialmente, tenham dado o seu consentimento prévio.

O empregador pode, portanto, regulamentar o uso destes meios estabelecendo uma política clara sobre o uso correcto e incorrecto destes novos meios de comunicação electrónica, determinando nomeadamente quanto tempo os trabalhadores poderão utilizá-los e sancionando disciplinarmente quem exceda esses limites. Todavia, não fica legitimado para controlar as páginas visitadas, como já vimos anteriormente, atenta a protecção do direito à privacidade em sentido amplo.

É igualmente assente que o empregador pode restringir o acesso da consulta da Internet através da filtragem de determinados *sites*.

Não tendo o empregador regulado a utilização do correio electrónico para fins pessoais, conforme possibilita o artigo 22.º, n.º 2, o envio de mensagens de carácter pessoal não integra infracção disciplinar, no que respeita ao não cumprimento de tal regulamentação, não obstante poder configurar uma infracção disciplinar caso tal envio exceda os limites legais afectos ao cumprimento da prestação por parte do trabalhador, como sejam, a boa fé, o zelo e diligência, a lealdade, a promoção e execução de actos tendentes à melhor e maior produtividade da empresa, enfim o dever de obediência a que está obrigado.

CAPÍTULO V

CARACTERIZAÇÃO DA POSIÇÃO JURÍDICA – BALANÇO DOS INTERESSES PROCEDIMENTAIS – OS INTERESSES DO EMPREGADOR E OS DIREITOS DO TRABALHADOR

Quer na utilização da Internet quer na utilização do *e-mail* profissional, vários são, pois, os argumentos de que o empregador se socorre para fazer valer a legitimidade do controlo electrónico exercido sobre o trabalhador, efectivado através do acesso e da visualização do tipo e do número de *e-mails* que aquele envia, da hora a que os envia, do acesso ao conteúdo dos mesmos.

Estes argumentos relacionam-se, pois, maioritariamente, com a propriedade do sistema informático, os custos envolvidos, a segurança do sistema informático e a eventual responsabilidade do empregador por actos praticados pelo trabalhador.

No que respeita à propriedade do sistema informático, é nosso entendimento que este não é um argumento que habilite os empregadores a violarem, sem mais, o direito fundamental do trabalhador à privacidade. A titularidade do meio utilizado não justifica o acesso às comunicações electrónicas realizadas através da empresa. De facto, nenhum motivo permite ao empregador fazer aquilo que nem as autoridades policiais podem fazer sem autorização judicial. Pelo que, o empregador não pode, pois, aceder ao conteúdo dos *e-mails* pessoais dos trabalhadores.

Outro argumento utilizado pelos empregadores prende-se com os custos que o uso extralaboral dos meios informáticos representa, podendo haver danos patrimoniais ou afectação da prestação de trabalho. No entanto, actualmente, as empresas celebram contratos que lhes permitem um uso permanente destes meios, sendo insignificante, a nível de custos monetários dos mesmos, o uso privado que o trabalhador lhes dê. O custo monetário da utilização destes meios é inferior, aliás, ao uso de telefones ou de viaturas da empresa. O que o empregador poderá invocar serão, sim, lucros cessantes, por poder haver uma falta de prestação efectiva da actividade laboral. Conforme o entendimento de Amadeu Guerra ⁽²⁹⁾, que partilhamos, estando em causa razões de custos ou de produtividade, o controlo pelo empregador deverá ser feito, em primeiro lugar, através da contabilização do número de *e-mails* enviados pelo trabalhador, sendo que, se se verificar que houve uma utilização desproporcionada deste meio

⁽²⁹⁾ *Op. cit.*, pp. 389-390.

de comunicação – que deverá ser comparada com a natureza e tipo de actividade desenvolvida – deve seguir-se um aviso do trabalhador e, se possível, o controlo através de outros meios alternativos e menos intrusivos.

Um outro argumento frequentemente invocado pelos empregadores é a segurança do sistema informático e o risco de transmissão de vírus. No entanto, no nosso ponto de vista, este risco também existe quando os trabalhadores acedem à Internet por razões profissionais. A solução para este tipo de problemas consistirá apenas em o empregador acautelar estas situações e preveni-las, instalando programas anti-vírus e realizando regularmente cópias de segurança. Este argumento não colhe, igualmente, pois, inclusivamente, muitas vezes as empresas recebem *e-mails* de *spam*, sem que o trabalhador tenha nisso qualquer responsabilidade. A solução passa, portanto, por o empregador utilizar filtros que sejam eficazes. Com efeito, “a vulnerabilidade invocada (...) não decorre da forma como os trabalhadores utilizam os computadores, mas da insuficiência de medidas ou de políticas de segurança que fragilizam muitas empresas e as expõem a «ataques» externos”⁽³⁰⁾. Segundo o entendimento deste Autor, que secundamos, existem programas anti-vírus, que devem estar actualizados, devendo a entidade empregadora adoptar procedimentos regulares de *backup* para evitar a perda da informação, definir políticas de “gestão de quotas de disco”, sistemas de alarme e registo de tentativas de intrusão no sistema da empresa ou, até, mecanismos *anti-cookie*, sendo os sistemas de *firewall* os mais eficazes para proteger a empresa contra a intrusão exterior. Efectivamente, este sistema de *firewall* pode ser especialmente eficaz se forem adoptados mecanismos complementares à filtragem do tráfego, nomeadamente através da especificação de *sites* interditos, da criação de *software* que permita a identificação de “palavras-chave” que sejam determinantes para negar o acesso aos internautas quando essas palavras são utilizadas e mesmo através do estabelecimento de mecanismos de bloqueamento de tráfego em relação à natureza e formato de certos ficheiros (v.g. .exe, imagens ou mp3).

Existem ainda argumentos de funcionalidade da empresa, nomeadamente quando o trabalhador se encontre ausente, aspectos estes que podem, no nosso ponto de vista, ser colmatados perante a elaboração de normas regulamentares dirigidas a este efeito. Considerámos, pois, que se existir uma política clara sobre o uso do *e-mail* que seja conhecida dos trabalhadores, a sua utilização significará que o trabalhador está a consentir no controlo

⁽³⁰⁾ Amadeu Guerra, *op. cit.*, p.395.

das mensagens profissionais e pessoais mas, quanto a estas, apenas para determinar a sua natureza pessoal ou profissional e não o seu conteúdo.

Não defendemos, no entanto, uma liberdade, sem mais, de utilização da Internet pelo trabalhador. Afastamos, somente, a pretensão da realização de um controlo absoluto da actividade do trabalhador baseado neste tipo de argumento, que, salientamos, consideramos falível.

O próximo argumento que descreveremos no sentido do controlo electrónico do empregador sobre o trabalhador relaciona-se com o disposto no artigo 500.º do Código Civil, ou seja, com a eventual responsabilidade do empregador por actos praticados pelo trabalhador, no âmbito da relação comitente-comissário, isto é, a responsabilidade do empregador por actos praticados pelos seus trabalhadores.

Ao abrigo do artigo 500.º do Código Civil, e da relação comitente – comissário aí prevista, o empregador responde civilmente pelos actos praticados pelos seus trabalhadores, tendo direito de regresso caso não exista culpa sua (cfr. n.º 3 deste artigo). Ora, nos termos deste preceito, existem vários requisitos para a verificação desta responsabilidade: a existência de uma comissão (o contrato de trabalho); a prática do acto ilícito no exercício da função (independentemente de ter sido intencional ou contra as instruções do empregador).

Na verdade, pode tornar-se difícil imputar-se a responsabilidade num sistema em que o indivíduo se dilui. Mas, a nosso ver, o empregador tem aqui a possibilidade de afastar a sua responsabilidade se provar que o trabalhador praticou o facto danoso fora das suas funções, ou seja, por ocasião das mesmas e não no seu exercício ⁽³¹⁾. Consideramos que a prevenção desta responsabilidade passará pela adopção por parte do empregador de um regulamento com regras próprias sobre a utilização da Internet, prevendo, nomeadamente, a proibição do seu uso para fins ilícitos.

⁽³¹⁾ Helena Moniz, in “Internet e Globalização – Problemas Jurídico-Penais” in “As Telecomunicações e o Direito na Sociedade da Informação”, Coimbra, 1999, p. 383, afirma: “De quem é a responsabilidade pelas mensagens transmitidas na *internet*? Parece-nos que é de quem as divulga, não tendo o servidor qualquer responsabilidade (embora alguns autores considerem que deve ser feita uma equiparação do servidor ao director do jornal, o que quanto a nós é excessivo uma vez que o administrador do servidor não tem a direcção da informação que nele circula). Quando se trata de transmissão de informações pela *www* (*world wide web*), através de *newsgroup* ou simplesmente por correio electrónico, o autor destas informações é que será o responsável; poderá verificar-se alguma dificuldade na identificação do autor do crime enquanto pessoa física, todavia isto não constitui obstáculo para o traficante de droga, o mensageiro de uma carta armadilhada, etc. (...) No entanto, o servidor não pode assumir a posição de garante relativamente às informações que *passam* por ele”.

É, pois, determinante a imposição de regras quanto ao acesso e ao uso que o trabalhador faz dos meios electrónicos que a empresa lhe coloca ao dispor. Apenas com o estabelecimento daquelas, ficará o empregador legitimado para actuar perante as ocorrências. Mas mesmo existindo uma definição de tais regras, entendemos que o acesso ao *e-mail* deverá ser o último recurso a utilizar pelo empregador (salvo se previamente for estabelecida a proibição total da utilização pessoal daquele), sendo preferível que tal se processe na presença do trabalhador visado e na presença de um representante da comissão de trabalhadores. Esta intervenção das comissões de trabalhadores visaria, em certa medida, comprovar que o controlo não se revelaria abusivo e desproporcionado em relação à finalidade a atingir. Entendemos, assim, que este acesso deve limitar-se à visualização dos endereços dos destinatários, do assunto, data e hora do envio, podendo o trabalhador – se for o caso – especificar a existência de alguns *e-mails* de natureza privada, que não pretende que sejam lidos pela entidade patronal. Ora, em face dessa oposição do trabalhador, o empregador deverá então abster-se de consultar o conteúdo do *e-mail*, tendo, no entanto, a faculdade de tomar as medidas que considere adequadas ao caso (entre elas o procedimento disciplinar - se considerar haver fundamento para o efeito).

Tal regulamentação poderá conter normas sobre a duração da utilização da Internet para fins pessoais, prevendo sanções em caso de violação. No entanto, entendemos que a visualização do próprio conteúdo dos *sites* consultados já excede o seu poder de controlo. Não esqueçamos que o empregador tem, também, a faculdade de impedir o acesso a determinados *sites*, *sites* ilícitos, de jogo, de *chat*, como medida de prevenção, devendo tal ser objecto de informação aos trabalhadores. Da mesma maneira, existem estas restrições relativamente a chamadas para telemóveis ou internacionais.

Na verdade, se existir um regulamento interno que defina em que condições podem ser utilizadas as novas tecnologias, o empregador poderá valer-se do mesmo para prevenir uma eventual responsabilidade por actos praticados pelos trabalhadores.

Mas se, por um lado, temos de ter em consideração os interesses do empregador, nomeadamente no que respeita à propriedade, à segurança (v.g. introdução de vírus), aos custos com a navegação na Internet, à rentabilidade e à produtividade da empresa, bem como à responsabilização do empregador por factos praticados pelo trabalhador (v.g. crimes), por outro lado, não podemos deixar de atender ao direito à privacidade do trabalhador e ao direito ao sigilo das comunicações, previsto no artigo 34.º da CRP.

Um dos efeitos adversos da utilização das novas tecnologias de informação é, pois, que da mesma forma como concedem ao trabalhador liberdade no acesso a qualquer tipo de informação de uma forma veloz e instantânea, facilitam também ao empregador uma entrada de tal maneira invasiva na sua vida que lhe é difícil impedir a disseminação de informações que pretenda manter em sigilo, diminuindo igualmente a liberdade da sua esfera privada. Para além disso, permitem que o empregador efectue um tratamento global às informações obtidas, de forma invisível, interconectando-se os dados considerados individualmente para a criação de um autêntico perfil do trabalhador, traçado informaticamente, perfil esse que poderá, por vezes, não corresponder à realidade de facto. A visualização pelo empregador do conteúdo dos *e-mails* do seu trabalhador, bem como das informações visualizadas por este nas suas pesquisas efectuadas através da Internet, tornam o trabalhador “transparente” face ao seu empregador, permitindo-lhe a construção de interligações que o levam à assunção de um perfil pessoal daquele, da presunção dos seus gostos, interesses, ligações pessoais e familiares, possíveis problemas de saúde, viagens.

Há quem entenda, como Amadeu Guerra, que, neste contexto, “está a surgir um novo direito fundamental do trabalhador – «direito à intimidade informática» – e que lhe confere a faculdade de conhecer e de controlar quantas transacções e operações se realizam com os seus dados de carácter pessoal, assim como a faculdade de decidir sobre as referidas operações através da concessão do direito ao consentimento informado, colocando nas suas mãos os instrumentos válidos para uma defesa prévia, convertendo o próprio trabalhador, titular dos dados, no mais eficiente garante da sua privacidade. Este direito assume, no domínio laboral, particular relevância, pelas razões já evidenciadas e que se relacionam com os princípios da «mutua colaboração» e da «confiança recíproca», sem esquecer que a realização de tratamentos sem informação dos trabalhadores não contribui, de forma alguma, para atenuar a «conflitualidade» inerente ao desenvolvimento da relação de trabalho. Para além de a falta de informação aos titulares dos dados ser susceptível de integrar uma violação da Lei n.º 67/98, não havendo razão jurídica para negar aos trabalhadores esse direito, tal omissão tem implicações evidentes no domínio da *validade da prova*”⁽³²⁾. De facto, a prova obtida por meios ilegais não é admissível de ser utilizada pelo empregador contra o trabalhador.

⁽³²⁾ Amadeu Guerra, *op. cit.*, p. 54.

CAPÍTULO VI

VANTAGENS DA UTILIZAÇÃO DA INTERNET E DO *E-MAIL* PARA FINS PESSOAIS E ADOÇÃO DE NORMAS REGULAMENTARES

Antes de avançarmos mais na matéria do controlo electrónico propriamente dito, é de notar que, para evitar os riscos *supra* mencionados, algumas empresas suprimem o uso destes meios para fins não profissionais. No nosso entendimento, esta solução, não obstante poder traduzir-se num factor de desmotivação dos trabalhadores, poderá ser uma forte aliada do empregador. É verdade que o trabalhador despende a maior parte do seu dia no local de trabalho, mas a lei prevê que falte justificadamente ao trabalho quando necessita de cumprir algumas necessidades consideradas relevantes, como sejam a visualização de informações relacionadas com a educação e estabelecimento escolar dos filhos,

Antes de reflectirmos sobre até que ponto a utilização pessoal destes meios electrónicos, em ambiente profissional, é desejada, vejamos as vantagens que os mesmos consagram em geral. Por um lado, a utilização do *e-mail* oferece inúmeras vantagens: a facilidade de uso, a permanência ou armazenamento das mensagens, a rapidez de envio de mensagens e a várias pessoas em simultâneo, a possibilidade de rever o conteúdo da mensagem antes de ser enviada, a possibilidade de ler a mensagem em qualquer altura. Os *e-mails* têm vindo a substituir, quase por completo, os tradicionais meios de comunicação.

Por sua vez, a Internet oferece inúmeras vantagens em termos de aprendizagem do trabalhador. Tendo em conta a importância, a difusão e a quantidade de informações que este meio de comunicação oferece actualmente, entendemos que a Internet melhora bastante a capacidade dos trabalhadores exercerem a sua actividade.

No entanto, a sua utilização, em horário de trabalho, para fins pessoais, deixa muito a desejar. Com efeito, para além dos argumentos já aduzidos no Capítulo anterior, formulados do ponto de vista da entidade empregadora, a “a generalidade dos estudos aponta no sentido de que os internautas gastam mais tempo e dinheiro *on line* quando estão no trabalho do que quando estão no seu domicílio” ⁽³³⁾. As compras, o pagamento de contas diversas, a pesquisa de informações relacionadas com viagens de lazer, com produtos a adquirir, com informações de saúde, por exemplo, são efectuadas, na maioria das vezes, *online* e durante o horário de trabalho, o que provoca inúmeras distrações ao trabalhador, desviando-o da sua expectável dedicação profissional. Pelo que, perfilhando a opinião de Amadeu Guerra, entendemos que a

⁽³³⁾ Amadeu Guerra, *op. cit.*, p. 366.

entidade empregadora deverá “analisar todos os factores – a salvaguarda da liberdade de expressão e de informação, a formação, o livre desenvolvimento e iniciativa do trabalhador, a sua sensibilização para acesso às redes públicas, os custos para a empresa, as políticas de segurança, de privacidade e o grau de utilização destes meios, o tipo de actividade e grau de autonomia dos seus funcionários, bem como as suas necessidades concretas e pessoais – para definir regras claras e precisas em relação à utilização do correio electrónico e da Internet para fins privados. É essa opção do CT quando, no seu artigo 21.º, n.º 2, confere à entidade empregadora a faculdade de «estabelecer regras de utilização dos meios de comunicação da empresa», em particular em relação à utilização do correio electrónico”⁽³⁴⁾. Julgamos que esta regulamentação é, pois, essencial, servindo como linha de orientação e actuação dos trabalhadores e como mecanismo de salvaguarda dos interesses do empregador, mormente numa situação de eventual desrespeito pelas mesmas. Naturalmente que o caminho seria mais facilitado se as empresas entendessem prever, pura e simplesmente, uma absoluta interdição do uso pessoal daqueles meios de comunicação.

Em nosso entendimento, tais regras deveriam obedecer aos princípios da necessidade, da proporcionalidade, da mútua colaboração e da confiança recíproca, os quais estão subjacentes ao contrato de trabalho. As mesmas deveriam ser submetidas à consideração dos trabalhadores e dos seus órgãos representativos e respeitar os direitos de personalidade dos trabalhadores, e ser publicitadas.

O empregador tem, portanto, a possibilidade de regulamentar a utilização destes meios, através da elaboração e publicitação de um regulamento interno aplicável a todos os trabalhadores, proibindo um uso extra-laboral abusivo e contrário, nomeadamente, ao princípio da boa fé, e estabelecendo políticas claras sobre a utilização destes meios de comunicação.

O estabelecimento de regras claras deve, pois, constar de regulamentos internos. Em tais regras, poderá ser estabelecido que os *e-mails* pessoais enviados devem ser legais e não conterem elementos difamatórios, elementos de assédio, elementos ofensivos baseados no género, idade, sexualidade, raça, incapacidade ou aparência das pessoas; poderá também ser definido que os *e-mails* pessoais devem conter uma cláusula de responsabilidade que esclareça que o conteúdo da mensagem é da exclusiva responsabilidade do seu autor, não reflectindo o ponto de vista do empregador; e poderá, ainda, ser estabelecido que a utilização do *e-mail* profissional para fins pessoais deverá ser efectuado apenas em casos de absoluta

⁽³⁴⁾ Amadeu Guerra, *op. cit.*, p. 366.

necessidade, impondo-se, pois uma regra proibitiva dos mesmos. Também poderá estar definido o tipo de anexos permitido, os limites de tempo e as políticas de acesso quando os trabalhadores estão temporariamente ausentes (quer por motivo de doença quer por motivo de gozo de férias, em que o empregador poderá ter de aceder à caixa de correio electrónico dos trabalhadores, convindo que estes sejam previamente informados dessa possibilidade e que tenham dado o seu consentimento prévio - embora o empregador continue a não poder aceder ao conteúdo dos *emails* pessoais, a existirem). Para evitar eventuais aberturas de *e-mails* pessoais, é preferível a separação entre caixas de correio pessoais e caixas de caixas de correio profissionais ou poderá ser previsto que estes, a existirem, devem ser guardados numa pasta pessoal dentro da caixa de correio electrónico profissional, sendo o trabalhador obrigado a classificar os *e-mails* pessoais e os profissionais, e devendo o empregador presumir como profissional o correio que não é qualificado como pessoal.

Deverá ainda ser estabelecido, como regra interna da empresa, que, durante a ausência do trabalhador, deverá o mesmo criar, como resposta a *e-mails* recepcionados, uma mensagem instantânea de aviso da sua ausência e de informação do responsável para onde os *e-mails* deverão ser reencaminhados.

Como vimos, o empregador pode estabelecer regras de utilização das tecnologias e restringi-los ao uso profissional se assim o entender. Tais regras terão, pois, como objectivo a segurança do sistema, a necessidade de evitar problemas de responsabilidade imputáveis ao empregador e garantir a possibilidade de se controlar a produtividade e a disciplina do trabalhador durante as suas horas de trabalho. A adopção de um regulamento interno de empresa é, no nosso entendimento, a forma mais eficaz para a regulação de todas as situações que possam constituir preocupações do empregador.

É de notar que, com as mais recentes alterações a nível laboral, o regulamento interno não tem já de ser enviado à Autoridade para as Condições do Trabalho (ACT) para produzir os seus efeitos. Com efeito, a Lei n.º 23/2012, de 25 de Junho alterou o n.º 3 do artigo 99.º do CT, aprovado pela Lei n.º 7/2009, de 12 de Fevereiro, pelo que é actualmente muito mais facilitada e célere a adopção destas regras.

CAPÍTULO VII

O CONTROLO ELECTRÓNICO EFECTUADO PELO EMPREGADOR

O facto de o empregador optar pela adopção de uma regulamentação nos moldes *supra* descritos, não o legitima a aceder ao conteúdo dos *e-mails* pessoais ou ao conteúdo das páginas da Internet visitadas, tendo de observar o limite imposto pelo direito à privacidade. Ademais, na maioria das situações, não existe sequer necessidade, no que se refere à utilização da Internet, de se controlar o conteúdo dos *sites* visitados, bastando atender ao tempo despendido ou o controlo dos *sites* mais visitados, por forma a aferir da correcta utilização destes meios, já configurando este um controlo licitamente realizado pelo empregador.

Note-se que o empregador deve ter em consideração a possibilidade de visitas a *sites* efectuadas inadvertidamente, nomeadamente por anúncios ou erros de escrita, em que os trabalhadores são redireccionados para *sites* que não procuraram.

Quanto à possibilidade de sancionar o trabalhador pela utilização pontual da Internet, consideramos que tal não é causa suficiente para a aplicação de uma sanção disciplinar. Diferente, no entanto, será o caso do trabalhador utilizar indevidamente a Internet, nomeadamente para descarregar filmes, provocando o engarrafamento do servidor. Para se aplicar uma infracção disciplinar, é necessário verificar-se uma efectiva diminuição da produtividade ou um dano patrimonial da empresa.

Qualquer decisão sobre a realização de controlo deverá ser criteriosa, evitando-se que os benefícios que a entidade empregadora pretende obter sejam desproporcionados em relação ao grau de lesão que vai ser causada à privacidade e à autonomia dos empregados. Devem, pois, ser consideradas as vantagens – quer para a empresa quer para os trabalhadores – que o acesso à Internet traz para o desenvolvimento da capacidade de investigação, autonomia e iniciativa do trabalhador, aspectos que podem ser capitalizados em benefício da empresa se as pesquisas efectuadas *online* pelo trabalhador se cingirem exclusivamente para fins profissionais.

A entidade empregadora pode, pois, exercer um controlo electrónico dos trabalhadores, o qual deverá estar salvaguardado por normas regulamentares inseridas num regulamento interno. No âmbito da execução desse controlo, a entidade empregadora deve escolher metodologias de controlo não intrusivas, que estejam de acordo com os princípios previamente definidos e que sejam do conhecimento dos trabalhadores.

Face à posição da CNPD, resulta que esta entidade, dotada de poderes de autoridade, é claramente protectora dos interesses dos trabalhadores, quase que vedando as formas de controlo que o empregador possa querer exercer relativamente às ferramentas electrónicas que coloque à sua disposição. Refira-se que, neste caso, as cautelas e limitações que a CNPD tem proferido reportam-se apenas aos acessos e utilização de telefones, Internet e meios de comunicação de correio electrónico e têm subjacente o facto de efectivamente se admitir como legítimo o exercício de controlo dessas situações. O que legitima tal controlo é a observância de que os respectivos métodos devem ser do conhecimento dos trabalhadores que claramente deverão saber o grau de tolerância que o empregador possa dar à utilização dos meios e o grau de intrusão a que estão sujeitos no que respeita à utilização de *e-mail*, informações estas que deverão constar de um documento escrito (v.g. Regulamento Interno). O que legitima tal controlo é, também, o dever que impende sobre o trabalhador de velar pela boa conservação e utilização dos bens relacionados com o seu trabalho, que lhe foram confiados pela entidade empregadora. O que legitima tal controlo é, ainda, o dever de obediência às ordens e instruções emanadas pelo empregador, o dever de realizar o seu trabalho com zelo e diligência, o dever de guardar lealdade ao empregador, de promover ou executar os actos tendentes à maior e melhor da produtividade da empresa, o dever de proceder de boa fé no exercício dos seus direitos e obrigações (como prevêm os artigos 126.º e seguintes do CT). Não podemos, em momento algum, olvidar que o trabalhador assinou um contrato de trabalho, tendo-se obrigado, mediante o pagamento de uma retribuição, a prestar a sua actividade a outra pessoa, no âmbito da organização e sob a autoridade desta (é este, na verdade, o conceito legal de contrato de trabalho). O trabalhador preencheu, portanto, um lugar dentro da estrutura organizativa da empresa, tendo o empregador a expectativa lógica de obtenção de resultados positivos por parte daquele, sem distrações que desviem a sua atenção do objectivo para que foi contratado e para o qual auferirá uma retribuição em contrapartida.

Atentando ao poder de direcção do empregador, é nosso entendimento que um documento que vise regular o acesso e a utilização das ferramentas electrónicas deverá indicar quais os métodos de controlo a estabelecer, tendo por base os “Princípios da CNPD”, e ser sujeito à apreciação dessa Comissão, tendo em atenção que, e perfilhando as recomendações da CNPD, o acesso sistemático ao registo das comunicações electrónicas – para além de se poder revelar desproporcionado ao objectivo de controlo e atentar contra a dignidade do trabalhador – pode não se revelar eficaz e necessariamente produtivo, pelo “clima de angústia e tensão” que todos estes métodos podem criar no seio da empresa. Pelo que, a entidade empregadora não deve

fazer um controlo permanente e sistemático do *e-mail* dos trabalhadores. O controlo deve ser, pois, pontual e direccionado para as áreas e actividades que apresentem um maior “risco” para a empresa. O dever de respeitar e tratar o trabalhador com urbanidade e probidade legalmente estipulado, o valor da dignidade da pessoa humana constitucionalmente previsto são fundamentos impeditivos do exercício de um controlo quase ditatorial sobre o trabalhador. De facto, embora tendo assinado um contrato de trabalho, tal não habilita a outra parte a invadir legalmente a sua vida pessoal.

O controlo em relação ao tempo de acesso diário e aos *sites* consultados por cada trabalhador só deverá ser realizado em circunstâncias excepcionais, nomeadamente quando, no contexto da sua advertência, o trabalhador duvidar das indicações da empresa e quiser conferir a realização de tais acessos. Julgamos que a diminuição da produtividade do trabalhador ou o surgimento crescente de vírus no sistema operativo alerte o empregador para a sua origem, configurando as mesmas circunstâncias excepcionais para o exercício do poder de controlo do empregador.

Decorre das recomendações dos “Princípios da CNPD” que o grau de autonomia do trabalhador e a natureza da actividade desenvolvida, bem como as razões que levaram à atribuição de um *e-mail* ao trabalhador devem ser tomadas em conta, decisivamente, em relação à forma como vão ser exercidos os poderes de controlo. Acresce que o segredo profissional específico que impende sobre o empregado deve ser preservado.

Para além disso, os meios utilizados deverão ser ajustados à organização da empresa, ao desenvolvimento da actividade produtiva e ser compatíveis com os direitos e obrigações dos trabalhadores consignados na legislação de trabalho, correspondendo a um «interesse empresarial sério» que não se revele abusivo e desproporcionado em relação ao grau de protecção da esfera privada do trabalhador.

Resulta igualmente daqueles “Princípios” que quando, na qualidade de empregador, este proceda a um controlo da actividade, deve privilegiar metodologias genéricas (por exemplo, uma mera amostragem), evitando a consulta individualizada de dados pessoais, através das quais se obtenha o número de *e-mails* enviados, tempo gasto em consultas na Internet, entre outros.

Não obstante o empregador encontrar-se proibido de aceder ao conteúdo dos *sites* consultados, existindo um Regulamento Interno sobre a utilização da Internet, aquele, face à constatação da utilização desproporcionada deste meio de comunicação – que será comparada com a natureza e tipo de actividade desenvolvida – deve proceder a um aviso ao trabalhador e, se possível, ao controlo através de outros meios alternativos e menos intrusivos.

Há, no entanto, que considerar que a utilização indevida da Internet poderá decorrer, não da forma como os trabalhadores utilizam os computadores, mas da insuficiência de medidas ou de políticas de segurança que fragilizam muitas empresas e as expõem a “ataques” externos. Tal sucederá se, por exemplo, a empresa não tiver instalado um bom programa de anti-vírus. Como defendemos *supra*, julgamos ser razoável que a empresa consinta na utilização particular do correio electrónico, desde que tal não impeça o normal funcionamento das funções e do bom funcionamento da caixa de correio. Consideramos também adequado que a empresa permita que o trabalhador consulte, via Internet, *sites* que se destinem a auxiliar a sua vida privada, nomeadamente quando o acesso aos mesmos se revele importante ou como forma prática para se inteirar de assuntos de âmbito familiar, da vida escolar dos seus filhos, verificação da conta bancária, pagamento de serviços, transferências e outras operações de idêntica natureza, desde que tais operações sejam pontuais, excepcionais, e não interfiram com a prestação do trabalho contratada. Tais operações seriam, do nosso ponto de vista, realizáveis, fora do período normal de trabalho a que o trabalhador se encontra obrigado, nomeadamente num intervalo de descanso.

É também admissível que do documento que regule a utilização destes meios electrónicos conste uma cláusula sobre a responsabilidade disciplinar e civil do trabalhador que não respeite os deveres indicados no mesmo.

A violação dessas regras de utilização dos meios de comunicação da empresa não permite, no entanto, repita-se, que o empregador efectue qualquer violação da confidencialidade das comunicações efectuadas pelo trabalhador. Com efeito, a indevida utilização do correio electrónico ou Internet pode ser detectada sem ter que se determinar o conteúdo das comunicações ou quais os *sites* visitados.

Se o trabalhador utilizar estes meios ilicitamente, caberá ao empregador provar tal incumprimento, alegando e provando a violação do dever de lealdade (previsto no artigo 128.º, nº 1, alínea f) do CT), ou seja, que tal incumprimento comprometeu a actividade do trabalhador e/ou a produtividade da empresa e/ou a imagem da mesma.

PRINCÍPIOS GERAIS NA EXECUÇÃO DO CONTROLO ELECTRÓNICO

O controlo electrónico do trabalhador por parte do empregador deverá, então, ter em atenção alguns limites, os quais estão relacionados com a aplicação dos princípios de protecção de dados pessoais, vertente do direito à privacidade.

Teresa Coelho Moreira defende que “o facto do desenvolvimento tecnológico permitir certo tipo de controlo não significa que o seu uso seja lícito tendo em atenção os princípios fundamentais do sistema jurídico” ⁽³⁵⁾. Defende a Autora a aplicação de três grandes princípios, os quais são por nós secundados, os quais terão implícitos a observância de outros com eles interligados. Referimo-nos ao princípio da finalidade, ao princípio da transparência e ao princípio da proporcionalidade.

Estes princípios estão directamente relacionados com os direitos de personalidade legalmente previstos. Atente-se que a matéria dos direitos de personalidade constituiu uma inovação do CT, na sua versão de 2003, nomeadamente com a consagração da confidencialidade de mensagens e de acesso a informação (anterior artigo 21.º, actual artigo 22.º), embora alguns desses direitos tivessem já aflorações em normas dispersas da anterior legislação laboral. Este carácter inovatório é, no entanto, relativo, pois já decorria da CRP e do Código Civil. Na verdade, na CRP já se previa, no artigo 18.º, n.º 1, que “os preceitos constitucionais respeitantes aos direitos, liberdades e garantias são directamente aplicáveis e vinculam as entidades públicas e privadas”; por sua vez, no Código Civil (artigos 70.º a 81.º) já era patente a tutela geral dos direitos de personalidade, nomeadamente no artigo 80.º (“Direito à reserva sobre a intimidade da vida privada”).

Não obstante, os direitos de personalidade encontram-se directamente ligados à dignidade da pessoa humana, sendo, por isso, justificável a sua consagração ao nível do Direito do Trabalho, por ser um direito, não tanto de empresas, mas de pessoas, de prestação de trabalho realizada por pessoas para pessoas, de gestão de pessoas, em que estamos perante uma relação de trabalho que é, pela sua natureza, *intuitu personae*.

Ora, se, por um lado, existe o direito à privacidade, por outro, existe o poder de controlo electrónico do empregador, sendo que este conflito de direitos terá, por conseguinte, de ser resolvido, pelos princípios da finalidade, princípio da transparência e princípio da proporcionalidade, devendo a avaliação dos direitos em causa ser efectuada em cada caso concreto.

⁽³⁵⁾ Teresa Coelho Moreira, in “Estudos de Direito do Trabalho”, Almedina, 2011, p. 40.

I. O PRINCÍPIO DA FINALIDADE

Segundo este princípio, previsto no artigo 6.º, n.º 1, alínea b) da Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995 (relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados) e no artigo 5.º, n.º 1, alínea b) da Lei de Protecção de Dados Pessoais (Lei n.º 67/98, de 26 de Outubro, que transpõe aquela Directiva), os dados de carácter pessoal apenas podem ser recolhidos quando existam motivos determinados, explícitos e legítimos, sendo essencial a definição precisa destas finalidades, não podendo aqueles ser posteriormente tratados de forma incompatível com essas finalidades. Desta forma, exigências, designadamente, de segurança e de não congestionamento da rede podem ser consideradas finalidades lícitas, permitindo um controlo electrónico da navegação dos trabalhadores através da análise de dados externos, tal como a frequência e as horas de navegação na Internet.

Segundo este princípio, o controlo efectuado pelo empregador deverá cingir-se unicamente à comprovação do correcto funcionamento da organização produtiva e do adequado cumprimento contratual pelo trabalhador, devendo o tratamento de dados ter uma finalidade legítima e não violar os direitos fundamentais dos trabalhadores.

II. O PRINCÍPIO DA TRANSPARÊNCIA

Este princípio, decorrente da obrigação prevista no artigo 106.º do CT, como princípio integrante do direito à autodeterminação informativa, expressando a proibição do controlo oculto, e consagrado no artigo 5.º, n.º 1, alínea a) da Lei n.º 67/98, supõe a obrigação de informar o trabalhador acerca da vigilância e do controlo exercidos pelo empregador, nomeadamente dando conhecimento de como e de quando tal controlo é realizado.

Segundo este princípio, o empregador tem de advertir com clareza os trabalhadores sobre os limites ao uso destas novas tecnologias, facultando-lhes indicações sobre a utilização do correio electrónico e da Internet dentro da empresa. Para tanto, os trabalhadores terão de ser informados previamente, e de forma expressa e inequívoca, em que medida os meios de comunicação da empresa poderão ser usados para comunicações pessoais, bem como da limitação da duração do seu uso, da existência do controlo e dos dados recolhidos, do objecto e da finalidade destes, assim como qual irá ser a posterior utilização da informação recolhida e, ainda, da identidade e direcção do responsável pelo tratamento.

O direito à privacidade e à dignidade da pessoa humana devem, pois, sempre ser tidos em conta pelo empregador. O controlo a efectuar deverá ser o mais claro e transparente possível, sendo o trabalhador informado que a sua actividade está a ser controlada e registada.

Refira-se que o princípio da transparência está relacionado também com o princípio da boa fé e com o princípio do conhecimento prévio dos trabalhadores, assim como dos seus representantes. Note-se que o princípio da boa fé adquire no Direito do Trabalho uma feição particular por se tratar de uma relação contratual de duração continuada e por nela ocorrer uma implicação da pessoa do trabalhador. Efectivamente, consistindo a relação laboral numa relação *intuitu personae*, com uma implicação pessoal do trabalhador, a boa fé assume, na mesma, uma especial relevância ⁽³⁶⁾, não apenas na altura da celebração do contrato de trabalho mas também durante a própria execução deste.

Este princípio, juntamente com o princípio da boa fé, consagra, ainda, ao trabalhador, o direito de acesso aos dados pessoais que lhe dizem respeito, tratados pelo empregador e, se for adequado, a possibilidade de solicitar a rectificação, eliminação ou bloqueio se os dados estiverem incompletos ou não forem exactos.

III. O PRINCÍPIO DA PROPORCIONALIDADE / PROIBIÇÃO DO EXCESSO / PRINCÍPIO DA INTERVENÇÃO MÍNIMA

Este princípio, que também pode ser denominado por princípio da proibição do excesso ou princípio da intervenção mínima, tende a realizar a procura do equilíbrio entre as obrigações do trabalhador, que emanam do seu contrato de trabalho, e o âmbito de liberdade constitucional da sua privacidade.

A medida de controlo pressupõe um juízo prévio sobre a sua necessidade ou indispensabilidade e um outro sobre a proporcionalidade dos sacrifícios que comporta para os direitos fundamentais dos trabalhadores.

Este princípio encontra consagração no artigo 6.º, n.º 1, alínea c) da Directiva 95/46/CE e no artigo 5.º, n.º 1, alínea c) da Lei n.º 67/98.

O controlo deverá ser adequado, pertinente e não excessivo em relação à finalidade pretendida; e os dados recolhidos só devem ser conservados pelo tempo que a finalidade exige.

⁽³⁶⁾ O princípio da boa fé no cumprimento das obrigações em geral encontra-se consagrado no artigo 762.º, n.º 2 do Código Civil. No CT, encontra-se expressamente consagrado no artigo 102.º (“Culpa na formação do contrato”), ao nível dos preliminares da formação contratual; no artigo 126.º (“Deveres gerais das partes”), ao nível da execução do contrato de trabalho; no artigo 489.º (“Boa fé na negociação”), em sede de negociação colectiva; e no artigo 522.º (“Boa fé”), em sede de resolução de conflitos colectivos.

A medida de controlo sobre a navegação na Internet deve ter uma repercussão mínima nos direitos do trabalhador, só podendo o empregador efectuar um controlo individualizado quando tiver detectado alguma irregularidade no uso da Internet por parte do trabalhador e não for possível satisfazer o seu interesse através de outros meios de controlo. Apenas em situações excepcionais, portanto, poderá haver um controlo individual do trabalhador, tendo, no entanto, sempre em consideração, o princípio da proporcionalidade. Este controlo deve, pois, ser o menos intrusivo possível, no sentido de se limitar a visualizar apenas a informação relativa ao trabalhador e o tempo gasto estritamente necessários à finalidade subjacente. Assim, se a finalidade era, por exemplo, a de verificar a utilização abusiva dos tempos de conexão à Internet, bastará registar o tempo de conexão do trabalhador e compará-lo com outros trabalhadores que desempenhem idênticas funções.

Este princípio impõe que o empregador, no exercício desse controlo, recorra às técnicas menos invasivas. Acresce que o interesse legítimo do empregador deverá ser apreciado casuisticamente, dependendo das funções exercidas pelos trabalhadores e da própria actividade da empresa.

“Defende-se, ainda, que atendendo ao princípio da finalidade e da proporcionalidade, o acesso a todos os arquivos e pastas que, através do título que detêm, quer pela sua inserção em determinadas pastas ou directórios quer pelo nome suponham ser pessoais e alheias à actividade laboral, fica interdita ao empregador. (...) Contudo, este não fica sem possibilidade de efectuar um certo tipo de controlo e de, eventualmente, sancionar o trabalhador. Poderá, sem analisar o conteúdo, efectuar uma discriminação do tipo de ficheiros contidos em determinadas pastas, e, atendendo ao tipo em causa, eventualmente aplicar alguma sanção disciplinar aos trabalhadores, até como uma forma de evitar possíveis responsabilidades. Imagine-se o caso da instalação de ficheiros “piratas”, de tipo MP3, ou MP4, de MPEGS e de ficheiros executáveis. Nestes casos, parece possível este tipo de controlo sem analisar o conteúdo, mas, atendendo ao seu carácter pessoal, só analisando o tipo de ficheiros introduzido na medida em que está em causa a privacidade dos trabalhadores”⁽³⁷⁾.

Este princípio é, assim, o princípio dos princípios, actuando como ordenador do direito, proporcionando uma solução de compromisso pela qual se dá prioridade a um dos princípios em conflito, mais ajustado ao caso em concreto, sem, porém, anular o outro princípio que será afectado o mínimo possível, respeitando sempre o núcleo essencial do direito em causa

⁽³⁷⁾ Teresa Coelho Moreira, *op. cit.* pp. 654-655.

porque esse é o limite que terá de ser observado já que se acolhe aí o princípio da dignidade da pessoa humana. Ou seja, ao abrigo deste princípio, directamente relacionado com o princípio da necessidade, o empregador tem de verificar se a visualização das comunicações electrónicas, e se o método que pretende utilizar, são absolutamente necessários para um determinado fim: por exemplo, para obter uma confirmação ou prova de certas acções da parte de um trabalhador, ou para manter o acesso à correspondência caso aquele esteja ausente (nomeadamente, por motivo de baixa ou de férias - embora o empregador continue a não poder aceder ao conteúdo dos *emails* pessoais) e a mesma não possa ser garantida de outra forma (nomeadamente, por resposta automática ou reenvio automático).

Da mesma forma, o empregador só deve manter os dados durante o tempo que for necessário para o fim especificado para a visualização.

Ainda nas palavras de Teresa Coelho Moreira, o contrato de trabalho configura-se como um limite ao poder de controlo do empregador, não podendo este ir além dos aspectos que têm uma relação directa com o trabalho e qualquer extra-limitação deste poder torna-se ilícita, legitimando a desobediência. Assim, o poder de controlo do empregador não pode exercer-se sobre a conduta extra-laboral do trabalhador a não ser quando essa conduta possa repercutir-se negativamente sobre o correcto cumprimento da prestação laboral ou quando possa prejudicar os legítimos interesses da empresa e, mesmo nessa hipótese, só pode incidir sobre a repercussão e não sobre o comportamento em si mesmo. Pelo que “os comportamentos do trabalhador na sua vida privada, realizados extra-profissionalmente, não têm relevância para constituírem justa causa de despedimento, nem serem passíveis de controlo (...)”⁽³⁸⁾.

⁽³⁸⁾ *Op. cit.*, p. 410.

CAPÍTULO VIII

A UTILIZAÇÃO DO *E-MAIL*

As principais questões que se colocam relativamente à utilização do *e-mail*, no âmbito de uma relação jurídico-laboral, prendem-se, essencialmente com o seguinte:

- Relativamente aos *e-mails* de carácter profissional, poderá o empregador controlar o seu conteúdo a qualquer momento e constantemente?
- Não existindo uma referência ao carácter pessoal do *e-mail*, poderá o empregador controlar o seu conteúdo?

A resposta a estas questões prende-se, primeiramente, por fazermos uma distinção entre *e-mails* profissionais e *e-mails* pessoais, mas nem sempre tal distinção é fácil.

***E-MAILS* PESSOAIS E *E-MAILS* PROFISSIONAIS**

É importante termos em consideração que existem *e-mails* com naturezas distintas, consoante as finalidades de utilização dos meios de comunicação e das tecnologias de informação. Assente-se que a natureza pública ou privada de um *e-mail* dependerá da informação nele contida, e não tanto do âmbito em que se desenrola.

No caso dos *e-mails* profissionais, contendo estes meras execuções da prestação de trabalho, é assente que o trabalhador envia e recebe mensagens de acordo com as ordens que recebe do empregador, considerando-se que as mesmas não constituem património exclusivo do trabalhador, mas também da empresa. Assim sendo, entende-se que não existe a necessidade de um consentimento prévio do trabalhador para que o empregador legalmente controle o conteúdo destas mensagens. Não nos parece, neste sentido, que o empregador seja um terceiro para efeitos de obtenção de uma prévia autorização judicial, tal como é exigível para o acesso ao conteúdo das mensagens pessoais, como veremos mais adiante. Neste caso, entendemos que existe uma relação comitente-comissário, podendo o empregador controlar o conteúdo dos *e-mails* profissionais. Não obstante, o empregador terá sempre de respeitar todos os requisitos para o exercício correcto do seu poder de controlo, principalmente o requisito da proporcionalidade.

É aconselhável que exista uma política clara acerca da utilização destes meios, com o estabelecimento de limites proporcionais e de acordo com os princípios da boa fé, da informação, da publicidade e da transparência. Atendendo ao princípio da proporcionalidade, não deverá este tipo de controlo ser permanente e a abertura desses *e-mails* profissionais deve

ser excepcional, devendo ocorrer na presença do trabalhador, a não ser que este se encontre ausente por algum motivo e seja exactamente esta a causa da sua visualização.

É assim necessária a presença de uma razão objectiva para o exercício do poder de controlo do empregador, não podendo realizar-se controlos arbitrários, indiscriminados ou exaustivos dos *e-mails* dos trabalhadores.

Por outro lado, o empregador tem de respeitar o princípio da adequação, não tomando conhecimento superior ao necessário e recorrendo às técnicas menos intrusivas.

O controlo efectuado terá, pois, de observar a Lei de Protecção de Dados Pessoais, nomeadamente o princípio da finalidade e da compatibilidade com a finalidade declarada e proporcionalidade.

Não obstante, o trabalhador poderá sempre qualificar certos *e-mails* como pessoais, ficando, desde logo, o empregador inibido de os ler.

Questão diversa é a de saber se, não existindo uma referência ao carácter pessoal do *e-mail*, poderá o empregador, mesmo assim, controlar o seu conteúdo.

No caso de se tratar de mensagens marcadas como pessoais ou de mensagens que não estão qualificadas como tais mas que pelo teor dos dados externos se deduz que o sejam ⁽³⁹⁾, a situação é totalmente diferente da que vimos *supra*. Nestes casos, as mensagens estão protegidas pelo direito ao sigilo das comunicações nos termos constitucionais e também pelo artigo 22.º do CT, sendo assim invioláveis.

O empregador não pode controlar o conteúdo destas mensagens nem mesmo em situações excepcionais em que há suspeitas de abusos ou de incumprimentos contratuais por parte do trabalhador. Mesmo que tais mensagens pareçam profissionais, se o empregador as visualizar e se aperceber da sua natureza pessoal, deverá parar imediatamente a sua leitura e não

⁽³⁹⁾ Em Acórdão do Tribunal da Relação de Lisboa, de 30-06-2011, processo número 439/10.3TTTCSC-A.L1-4, em que foi relatora a Juíza Desembargadora Isabel Tapadinhas e publicado em www.dgsi.pt, refere-se que do artigo 22.º do CT se retira “que o empregador ou quem o represente não pode aceder a mensagens de natureza pessoal que constem da caixa de correio electrónico do trabalhador. No caso em apreço, da visualização das mensagens de correio electrónico ainda que limitada à visualização do endereço do destinatário, do remetente da mensagem, do assunto, data e hora do envio, facilmente se retira que não estamos perante mensagens de natureza pessoal mas antes de mensagens que tratavam de assuntos profissionais respeitantes ao relacionamento comercial do recorrente, administrador da recorrida e da CPC África com outras empresas. Efectivamente, as mensagens em questão: continham no “Assunto” indicações de matérias profissionais, mais concretamente, nomes de negócios futuros da empresa ou nomes de empresas com as quais a recorrida e a C África mantinham relações comerciais (...).”

proceder à sua divulgação a terceiros ⁽⁴⁰⁾.

Qualquer acto de interceptação da comunicação contida nesta parte da caixa postal constituirá uma violação dos preceitos referidos anteriormente, sendo que a prova obtida será considerada nula nos termos do artigo 32.º, n.º 8 da CRP, não podendo o conteúdo de tal mensagem constituir o objecto de um processo disciplinar. E isto independentemente do conteúdo revestir carácter privado ou não, já que a tutela constitucional é realizada em termos objectivos, independentemente do conteúdo.

O artigo 34.º da CRP contém uma proibição geral (nomeadamente no seu n.º 4) que se refere à ingerência das autoridades públicas nos meios de comunicação, salvo os casos previstos na lei em matéria de processo penal e através de decisão judicial, e atendendo aos direitos, liberdades e garantias nos termos do artigo 18.º da Lei Constitucional, ou seja, com respeito dos princípios da necessidade, adequação, proporcionalidade e determinabilidade. Não obstante, entendemos que esta proibição é aplicável, nos mesmos termos, às entidades privadas, nomeadamente às entidades empregadoras. De facto, e como afirmam Gomes Canotilho e Vital Moreira, em anotação a este preceito ⁽⁴¹⁾, “a inviolabilidade da correspondência impõe-se, naturalmente, também foram das relações Estado-cidadão, vinculando toda e qualquer pessoa a não devassar a correspondência ou comunicações de outrem (art. 18.º-1)”. Ainda segundo estes Autores, “a Constituição não garante apenas o sigilo da correspondência e outros meios de comunicação privados (n.º 1), mas também proíbe toda a ingerência (n.º 4), o que é mais vasto, envolvendo nomeadamente a liberdade de

⁽⁴⁰⁾ Note-se que, tal como se refere em Acórdão do Supremo Tribunal de Justiça, de 05-07-2007, processo número 07S043, em que foi relator o Juiz Conselheiro Mário Pereira e publicado em www.dgsi.pt (é de sublinhar que este Acórdão é o único proferido por este douto Tribunal sobre a matéria em causa), “não são apenas as comunicações relativas à vida familiar, afectiva, sexual, saúde, convicções políticas e religiosas do trabalhador, e mencionadas no art.º 16.º, n.º 2 do CT que revestem a natureza de comunicações de natureza pessoal, nos termos e para os efeitos do art. 21.º. Como aí se referiu, a definição de natureza particular da mensagem obtém-se por contraposição à natureza profissional da comunicação, relevando, para tal, antes de mais, a vontade dos intervenientes da comunicação, ao postularem, de forma expressa ou implícita, a natureza profissional ou privada das mensagens que trocam. O art.º 21.º do CT situa-se no âmbito da tutela da confidencialidade do conteúdo das mensagens de natureza pessoal, enquanto que o art.º 16.º visou uma finalidade distinta, a de estabelecer os limites que se impõem a ambas as partes quanto à possibilidade de recolha e divulgação de informações, no âmbito da relação laboral, v.g., aquando do início dessa relação. E não é pela circunstância dos intervenientes se referirem a aspectos da empresa que, por essa simples razão, a comunicação assume desde logo um carácter profissional, legitimando a sua interceptação pelo empregador.” No mesmo sentido, v. Acórdão do Tribunal da Relação de Lisboa, de 07-03-2012, processo número 24163/09.0T2SNT.L1-4, em que foi relator o Juiz Desembargador José Eduardo Sapateiro e publicado em www.dgsi.pt.

⁽⁴¹⁾ J.J. Gomes Canotilho e Vital Moreira, em comentário ao artigo 34.º da “Constituição da República Portuguesa Anotada”, Volume I, 4.ª Edição Revista, Artigos 1.º a 107.º, Coimbra Editora, 2007, p. 544-545.

envio e de recepção da correspondência, a proibição de retenção ou de apreensão, bem como de interferência (telefónica, etc.), etc. O preceito em análise refere-se apenas às «autoridades públicas», mas a proibição de ingerência vale, por maioria de razão, para as entidades privadas”. Ora, o artigo 18.º, n.º 1, ao prever que “os preceitos constitucionais respeitantes aos direitos, liberdades e garantias são directamente aplicáveis e vinculam as entidades públicas e privadas”, faz aplicar directamente nas relações entre particulares os preceitos relativos aos “direitos, liberdades e garantias” (constantes da Parte I, Título II, artigos 24.º a 57.º da Lei Constitucional), conferindo-lhes, pois, uma eficácia geral, *erga omnes*, e não uma eficácia externa, ou em relação a terceiros, pois tais designações ainda pressupõem o paradigma liberal assente nas relações indivíduo-Estado, considerando os “direitos, liberdades e garantias” como direitos subjectivos de defesa perante o Estado e, conseqüentemente, relevantes apenas nas relações entre os particulares e o Estado. “À face da CRP, porém, os particulares não são «terceiros», nem constituem uma componente «externa» da eficácia directa dos «direitos, liberdades e garantias»”⁽⁴²⁾.

Não obstante, o direito ao sigilo das comunicações não é absoluto pois admitem-se excepções (como consta deste n.º 4) previstas em processo criminal sob reserva de lei, só podendo ser decididas por um juiz.

Este artigo tem uma fórmula abrangente, abrangendo toda a espécie de correspondência, incluindo o *e-mail*, nos mesmos termos que preceitua o artigo 194.º, n.º 2 do Código Penal.

Nos termos do artigo 34.º (n.º 4) da CRP, o empregador não poderá controlar o conteúdo sem uma prévia autorização judicial, mesmo que aquele tenha violado as regras estabelecidas pelo empregador, na medida em que a propriedade dos meios não retira a titularidade do direito e a infracção cometida pelo trabalhador é, quando muito, uma infracção disciplinar⁽⁴³⁾.

⁽⁴²⁾ Neste sentido, J.J. Gomes Canotilho e Vital Moreira, em comentário ao artigo 18.º da “Constituição da República Portuguesa Anotada”, Volume I, 4.ª Edição Revista, Artigos 1.º a 107.º, Coimbra Editora, 2007, p. 384-385.

⁽⁴³⁾ No já mencionado Acórdão do Tribunal da Relação do Porto (TRP), de 08/02/2010, processo número 452/08.0TTVFR.P1, em que foi relatora a Juíza Desembargadora Paula Leal de Carvalho e publicado em www.dgsi.pt, Joana Vasconcelos, relativamente à possibilidade de o empregador ler os *e-mails* pessoais do trabalhador, é peremptória ao recusar essa mesma possibilidade, defendendo que a nossa lei “garante, sem mais, o direito à reserva e à confidencialidade de quaisquer mensagens de natureza pessoal – cartas, faxes, correio electrónico, sms, telefonemas, etc. – que o trabalhador envie ou receba no local de trabalho, ainda que utilizando meios de comunicação pertencentes ao empregador. As mesmas reservas e confidencialidade são asseguradas relativamente a informação não profissional que o trabalhador receba ou consulte – por ex., via Internet – no local de trabalho. Esta garantia não cede nem nas situações em que a recepção ou envio de mensagens, ou o acesso a informação não profissional contrarie regras definidas pelo empregador quanto à utilização de meios de comunicação e de tecnologias de informação, e constitua infracção disciplinar. Quando tal suceda, o empregador pode controlar, por ex., o remetente ou o destinatário de mensagens de correio electrónico e o seu assunto, de modo a aferir o seu

Aquela autorização judicial terá lugar nas situações passíveis de integrarem determinados crimes, em que se aplicará o disposto no Código do Processo Penal (artigos 179.º, 187.º e 188.º, aplicáveis *ex vi* do artigo 189.º do mesmo complexo normativo).

Mesmo no âmbito de um processo disciplinar em curso (v.g. por desconfiança de revelação de segredos comerciais), o empregador encontra-se vinculado à proibição de inviolabilidade do direito à reserva e à confidencialidade de quaisquer mensagens de natureza pessoal do trabalhador, não lhe sendo permitido visualizar o respectivo conteúdo. Por isso, a única via para o acesso ao conteúdo passa pelo consentimento do trabalhador, consentimento este que deverá ser prestado de forma livre e individual (o que, no nosso entendimento, poderá ser difícil de avaliar, pois o trabalhador poderá dar tal consentimento perante o receio das consequências de não o fazer).

Em suma, excepto quando exista uma prévia autorização judicial ou o consentimento expresso do trabalhador, o princípio é o da inviolabilidade do conteúdo das mensagens pessoais.

Relativamente ao acesso a informação de carácter não profissional que o trabalhador envie, receba ou consulte, também o artigo 22.º, n.º 1 do CT, ao atribuir àquele o direito de reserva e confidencialidade, “nomeadamente através de correio electrónico”, é nosso entendimento que essa previsão pode, de algum modo, ter querido englobar, embora de forma muito imprecisa, a realidade do acesso à Internet. De facto, a consulta de *sites* visitados poderá permitir, nalguns casos, a constituição de perfis do trabalhador, bem como o conhecimento de gostos, *hobbies*, consulta sistemática de documentação relativa a determinada doença, a compra de determinados produtos, a preparação de uma viagem ou o gozo de férias, a procura de um novo emprego.

Assim, e tal como referimos em relação ao *e-mail*, a proibição de utilização da Internet para fins privados não legitima a devassa sobre as transacções e a navegação do trabalhador sem o seu conhecimento.

Para além das situações *supra* analisadas, existe ainda outra que deveremos ter em atenção: e se não existir uma política clara sobre a utilização do *e-mail* ou, existindo, se se permitir um uso indiscriminado daquele (quer para fins profissionais quer para fins pessoais)? Nestes casos, a questão é de mais difícil resolução.

(Cont. 43) – carácter pessoal, mas nunca o seu conteúdo, tal como pode verificar quais os *sites* a que trabalhador acedeu, mas não o conteúdo da pesquisa efectuada ou da informação neles obtida.”

Nestes casos, parece-nos que o *e-mail* estará protegido pelo direito ao sigilo das comunicações gozando, em princípio, da inviolabilidade. O empregador não pode aceder ao mesmo, nem aos ficheiros dos trabalhadores de forma indiscriminada nem com fins preventivos para controlar ou assegurar o seu bom uso. Se o fizer estará a violar os artigos 34.º da CRP e 22.º do CT.

O controlo destes *e-mails* reveste particular acuidade e o acesso aos mesmos deve ser a última instância a ser utilizada pelo empregador, sendo que este acesso apenas deve ser realizado na presença do trabalhador e de um seu representante – da Comissão de Trabalhadores (a não ser que aquele o dispense).

Portanto, o empregador, apesar de não poder controlar o conteúdo das mensagens no caso dos *e-mails* pessoais ou no caso de um uso indiscriminado, poderá, contudo, controlar alguns dados externos para tentar visualizar se os trabalhadores estão a utilizar correctamente ou não os seus meios de comunicação.

Que tipo de dados externos e de tráfego é que o empregador poderá, então, conhecer?

Os dados de tráfego são, em parte, informações fornecidas pelo remetente e, em parte, informações geradas automaticamente durante o tratamento do *e-mail* (ex.: data e hora de envio). Estes dados estão colocados, no todo ou em parte, no cabeçalho, que é transmitido a quem recebe o *e-mail*, juntamente com a própria mensagem. O conhecimento dos dados de tráfego deve ficar, portanto, limitado ao remetente, ao assunto, à data e à hora do envio, ao tipo de anexos e ao seu tamanho, ao número de mensagens enviadas ou recebidas na direcção de *e-mail* e ao tempo de permanência na rede.

Deste modo, o empregador pode controlar e sancionar o trabalhador sem violar os seus direitos fundamentais. Assim, o empregador pode controlar o custo da ferramenta de trabalho, o tempo gasto pelos trabalhadores na utilização da mesma, o acesso à rede informática. Este controlo permitirá ao empregador aplicar sanções disciplinares ao trabalhador, com base na utilização indevida ou abusiva destes meios das ferramentas de trabalho da empresa.

Questão diversa, mas inerente a esta distinção entre *e-mails* com uma natureza pessoal ou profissional, prende-se com a impossibilidade de o trabalhador controlar os *e-mails* que recebe na sua caixa de correio electrónico, ainda que a mesma tenha sido adstrita exclusivamente para utilização profissional. Nesse caso, o trabalhador não tem qualquer capacidade de controlo sobre esta recepção, pelo que não seria, em princípio, admissível que o

empregador qualificasse esta situação como uma infracção disciplinar. No entanto, haverá que, no caso em concreto, averiguar se das normas de utilização internas da empresa existe alguma estatuição quanto à divulgação do endereço electrónico que lhe foi atribuído para fins que não sejam estritamente profissionais, tendo-se também em atenção a facilidade existente para um terceiro (remetente) em descobrir este endereço sem que tenha havido divulgação por parte do trabalhador.

CAPÍTULO IX

O PROCEDIMENTO ATINENTE AO EXERCÍCIO DO PODER DE CONTROLO PELO EMPREGADOR

O empregador tem a obrigação de observar o cumprimento de algumas regras estabelecidas legalmente por forma a efectivar o legítimo exercício de controlo electrónico sobre o trabalhador. Vejamos, o mais sinteticamente que nos for possível, como se concretiza, então, a **operacionalização** deste exercício de controlo.

I. ENVOLVIMENTO DO TRABALHADOR

Direito de Informação ⁽⁴⁴⁾

O já abordado PRINCÍPIO DA TRANSPARÊNCIA supõe, como vimos *supra*, a obrigação de informar o trabalhador acerca da vigilância e do controlo exercido pelo empregador, nomeadamente dando conhecimento de como e de quando tal controlo é realizado, informação esta que deverá constar, por exemplo, de um Regulamento Interno de Empresa.

Tal como resulta dos artigos 2.º, 5.º n.º 1 al. a) e b), 10.º n.º 1 da Lei n.º 67/98 e do artigo 99.º do CT, a entidade empregadora deve – *antes de iniciar qualquer tipo de tratamento* – informar o trabalhador sobre as condições de utilização dos meios da empresa para efeitos particulares ou sobre o grau de tolerância admitido, sobre a existência de tratamento, suas finalidades, existência de controlo (formas e metodologias adoptadas), sobre os dados tratados e o tempo de conservação, bem como sobre as consequências da má utilização ou utilização indevida dos meios de comunicação colocados à sua disposição.

⁽⁴⁴⁾ Pedro Pais de Vasconcelos, “Protecção de dados pessoais e direito à privacidade” in “Direito da Sociedade da Informação”, Volume I, Coimbra Editora, 1999, p. 249, considera, com a nossa concordância, que a Directiva 95/46/CE “contém um artigo 9.º, segundo o qual os Estados-membros estabelecerão isenções ou derrogações para o tratamento de dados pessoais com fins exclusivamente jornalísticos ou de expressão artística ou literária, apenas na medida em que sejam necessárias para conciliar o direito à vida privada com as normas que regem a liberdade de expressão. Dentro da orientação de sobrepor o jornalismo aos direitos da personalidade, na transposição da Directriz, no n.º 6 do artigo 10.º da Lei n.º 67/98, o Legislador excluiu do direito de informação o tratamento de dados pessoais «efectuado para fins exclusivamente jornalísticos ou de expressão artística ou literária». Esta excepção não encontra justificação ética ou jurídica, e apenas pode ser compreendida na nova lógica de perversão mediática do sistema na sociedade política portuguesa, em considerações de puro oportunismo mediático e na evolução do sistema democrático representativo na Europa, para um novo sistema de oligarquia mediaticamente assistida, que se está progressivamente a instalar. Não é ética nem juridicamente aceitável – não é compatível com a Constituição nem com o carácter supra legal e de Direito Nacional dos direitos de personalidade – restringir e permitir o atropelo de direitos que não são ontologicamente fundantes da personalidade jurídica e da dignidade humana em homenagem a interesses comerciais e de negócio como são os da imprensa ou das vendas em massa”.

Os métodos de controlo devem, pois, ser do conhecimento dos trabalhadores, que deverão saber claramente o grau de tolerância que o empregador dá à utilização dos meios e o grau de intrusão a que estão sujeitos no que respeita à utilização de *e-mail*, informações estas que deverão constar de um documento (Regulamento), o qual será objecto de validação pela CNPD, assegurando-se assim uma efectiva eficácia das disposições que ali constem, designadamente, perante a necessidade de actuação perante um comportamento inadequado praticado por um colaborador, o qual contrarie as normas que ali se encontrem previstas.

Dispõe o artigo 99.º do CT que, tratando-se de um Regulamento Interno, a entidade empregadora deve publicitar o seu conteúdo, designadamente afixando-o na sua sede e nos restantes locais de trabalho, de modo a que os trabalhadores possam dele tomar conhecimento a todo o momento.

Uma das formas mais eficazes de divulgação deste Regulamento por todos os trabalhadores é, no nosso ponto de vista, designadamente através da Intranet eventualmente existente na empresa, ou através da afixação daquele num espaço próprio da mesma, devendo aquele estar disponível a qualquer trabalhador e ser acessível a todo o tempo.

Sem esta publicitação, o Regulamento Interno não produz efeitos, tal como determina o n.º 3, alínea a) do preceito legal em causa.

Não adoptando o empregador um Regulamento Interno, e sim outro meio que contenha as normas de utilização do *e-mail* e da Internet, deverá o mesmo ser igualmente objecto de publicitação junto dos trabalhadores, tal como decorre do dever de informação contido no artigo 10.º da Lei n.º 67/98 e no artigo 106.º do CT.

Consentimento

O consentimento do trabalhador para o tratamento de dados pessoais decorre de diversas normas legais, como sejam o artigo 35.º, n.º 3 da CRP, os artigos 6.º e 7.º da Lei n.º 67/98, o artigo 194.º do Código Penal ou o artigo 81.º do Código Civil (este versando sobre a limitação voluntária dos direitos de personalidade, ainda que a todo o tempo revogável).

A lei não prevê nenhuma forma específica de o trabalhador prestar o seu consentimento. A Lei n.º 67/98, no seu artigo 3.º (Definições”) diz que esse consentimento corresponde a “qualquer manifestação de vontade, livre, específica e informada, nos termos da qual o titular aceita que os seus dados pessoais sejam objecto de tratamento”.

No nosso entender, por forma a aferirmos da existência do consentimento do trabalhador, bastará que do respectivo Processo Individual conste uma declaração, datada e assinada pelo mesmo, em como tomou conhecimento e aceitou as normas vigentes relativas à utilização da

Internet e meios de comunicação de correio electrónico. Não obstante, e conforme prevê o artigo 7.º, n.º 2 da referida Lei n.º 67/98, será ainda necessária a existência de disposição legal ou de autorização da CNPD que legitime o tratamento (e controlo) dos dados pessoais do trabalhador.

De igual modo, nos “Princípios da CNPD”, consta como obrigação dos responsáveis dos ficheiros “recolher e manter as declarações de consentimento expresso do titular para o tratamento de dados pessoais, quando tal for exigido”.

Este consentimento deriva do denominado direito à autodeterminação informativa, o qual consiste na “faculdade que cada pessoa tem de determinar e controlar a utilização dos seus dados pessoais. Há, assim, uma clara rejeição da concepção do homem como mero «objecto de informações»”. (...) “Devido às suas características especiais, os direitos de personalidade não estão na disponibilidade do seu titular e, por isso, ele não pode renunciar a eles, apenas podendo consentir em limitações quanto ao seu exercício. Assim, a ofensa de um qualquer direito sem o consentimento do seu titular tem como consequência a ilicitude do acto lesivo. Porém, se existir consentimento e este tiver sido validamente prestado, essa violação passa a ser lícita, podendo referir-se aqui a figura do *consentimento do lesado*. (...) O artigo 81.º do Código Civil debruça-se sobre esta matéria, tendo a lei, neste artigo, estabelecido uma cláusula geral, de ordem pública, pois seria praticamente impossível delimitar normativamente os actos que objectivamente violam um direito de personalidade.” “No Direito do trabalho não pode dar-se por adquirida, bem ao contrário, a ideia de que tudo funciona nos termos anteriormente expostos quanto ao consentimento do lesado. É que na génese da separação das águas entre o Direito do trabalho e o Direito civil está exactamente a ideia de que a igualdade formal não contribuía para um real equilíbrio negocial entre trabalhador e empregador”. (...). No Direito do trabalho, “o trabalhador sofre duma *capitis diminutio* e, por isso, o seu consentimento pode ser irrelevante. As normas do Direito do trabalho são mínimos garantidos, potenciadores de tratamento mais favorável através da contratação colectiva, fomentador de tratamento *in melius* e proibitivo de tratamento *in peius*. Daí, também, a irrenunciabilidade de muitos direitos laborais. Assim, no que concerne ao consentimento do lesado, é necessário não só que o trabalhador esteja devidamente esclarecido sobre o consentimento que vai prestar mas, principalmente, que este seja dado livremente, isto é, sem qualquer tipo de pressão”⁽⁴⁵⁾.

⁽⁴⁵⁾ Teresa Coelho Moreira, in “Da Esfera Privada do Trabalhador e o Controlo do Empregador”, *Studia Iuridica*, n.º 78, Coimbra Editora, 2004, pp. 115-126.

Presença do Trabalhador no acesso ao *e-mail*

Dos “Princípios da CNPD”, já abordados *supra*, resulta que o acesso ao *e-mail* por parte do empregador (que deve limitar-se à visualização dos endereços dos destinatários, o assunto, a data e hora do envio), deverá ser o último recurso a utilizar pela entidade empregadora, sendo desejável que esse acesso seja feito na presença do trabalhador visado e, de preferência, na presença de um representante da Comissão de Trabalhadores.

Note-se que a CNPD aconselha a presença do trabalhador, não sendo, porém, legalmente exigida.

Direito de oposição

O trabalhador pode, se for o caso, especificar a existência de alguns *e-mails* de natureza privada, não pretendendo que sejam lidos pela entidade empregadora. Recomenda ainda a CNPD que, em face desta oposição do trabalhador, a entidade empregadora deverá abster-se de consultar o conteúdo daqueles.

Este direito de oposição em relação ao tratamento de dados a seu respeito pressupõe a verificação dos requisitos impostos pelo artigo 12.º, al. a) da Lei n.º 67/98, nos termos do qual “o titular dos dados tem o direito de, salvo disposição legal em contrário, e pelo menos nos casos referidos nas alíneas d) e e) do artigo 6.º, se opor em qualquer altura, por razões ponderosas e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam respeito sejam objecto de tratamento, devendo, em caso de oposição justificada, o tratamento efectuado pelo responsável deixar de poder incidir sobre esses dados”. Apenas em sede jurisdicional, poderá aferir-se da veracidade das razões invocadas pelo trabalhador.

A lei é omissa em relação à forma como esta oposição deverá ser realizada. No entanto, e não obstante o princípio de liberdade de forma consagrado no artigo 219.º do Código Civil, consideramos que a forma escrita será a mais adequada, por forma a melhor assegurar os interesses do trabalhador. Esta forma escrita é, aliás, exigida no artigo 14.º, n.º 4 da Lei n.º 67/98, que refere que “os elementos de prova da declaração negocial, do contrato ou do acto jurídico relativos à protecção dos dados, bem como as exigências relativas às medidas referidas no n.º 1, são consignadas por escrito em documento em suporte com valor probatório legalmente reconhecido”.

O trabalhador pode, então, utilizar o direito de oposição – nos termos do artigo 12.º da Lei 67/98 – para evitar a realização de um tratamento que ofenda a sua dignidade. Para o efeito, e para que possa ser apreciada a existência de “oposição justificada”, deve invocar “as razões

ponderosas e legítimas relacionadas com a sua situação particular” que permitem fundamentar o seu direito e que sejam idóneas para proibir o responsável de tratar dados pessoais a se respeito”. Neste caso, o trabalhador deve explicitar as razões subjectivas que justificam o exercício de um direito que se apresenta com um grau de prevalência superior ao da entidade empregadora. Trata-se, na generalidade dos casos, de aplicar o princípio da proporcionalidade conferindo relevância à situação particular do trabalhador.

II. ENVOLVIMENTO DAS ESTRUTURAS DE REPRESENTAÇÃO COLECTIVA DOS TRABALHADORES (ERCT’S)

Como se referiu anteriormente, a CNPD recomenda, não só a presença do trabalhador visado, mas também a presença de um representante da Comissão de Trabalhadores aquando do acesso ao *e-mail* por parte do empregador.

Mais uma vez, esta é apenas uma recomendação, não sendo legalmente necessária.

Conforme consta igualmente dos “Princípios da CNPD”, também as regras que o empregador defina em relação à utilização do correio electrónico e da Internet “devem ser submetidas à consideração dos trabalhadores e dos seus órgãos representativos, sendo claramente publicitadas por forma a que seja assegurada uma informação clara sobre o grau de tolerância, o tipo de controlo efectuado e, mesmo, sobre as consequências do incumprimento daquelas determinações (cfr. artigo 10.º da Lei n.º 67/98).”

Com efeito, a CNPD recomenda a submissão de tais regras aos órgãos representativos dos trabalhadores, apesar de legalmente esta obrigação só ser efectivamente exigível perante a existência de um Regulamento Interno, nos termos do artigo 99.º do CT - segundo este preceito, na elaboração do Regulamento Interno, “é ouvida a Comissão de Trabalhadores ou, na sua falta, as comissões intersindicais, as comissões sindicais ou os delegados sindicais”, sendo, pois, exigível a existência de um parecer emitido por um destes órgãos representativos dos trabalhadores, o qual deverá ser enviado conjuntamente com o pedido de autorização efectuado pelo empregador à Comissão Nacional de Protecção de Dados.

Por analogia com o disposto no artigo 21.º, n.º 4 do CT (relativo à utilização de meios de vigilância à distância), entendemos que, não estando este parecer disponível em 10 dias após a referida consulta, deverá o empregador juntar apenas o comprovativo do pedido de parecer.

III. INTERVENÇÃO DE ENTIDADES TERCEIRAS

III.1. Autoridade para as Condições do Trabalho (ACT)?

Recomenda a CNPD que “o grau de utilização dos meios da empresa para fins privados, a delimitação das condições de tratamento e a especificação das formas de controlo adoptadas devem constar de *Regulamento Interno* o qual, nos termos legais, deverá ser submetido a parecer da Comissão de Trabalhadores e aprovado pelo IDICT.” (note-se que este Instituto foi extinto, sendo actualmente a Autoridade para as Condições do Trabalho a entidade que detém esta competência). Da mesma forma, o artigo 99.º do CT, na sua versão original, dispunha que o Regulamento Interno só produzia efeitos após o seu envio àquela entidade. É de salientar, no entanto, que, com as mais recentes alterações a nível laboral, o regulamento interno não tem já de ser enviado à Autoridade para as Condições do Trabalho (ACT) para produzir os seus efeitos. Com efeito, a Lei n.º 23/2012, de 25 de Junho alterou o n.º 3 do artigo 99.º do CT, aprovado pela Lei n.º 7/2009, de 12 de Fevereiro, sendo que, actualmente, para produzir os seus efeitos o regulamento interno necessita apenas de ser publicitado, *“designadamente através de afixação na sede da empresa e nos locais de trabalho, de modo a possibilitar o seu pleno conhecimento, a todo o tempo, pelos trabalhadores.”*

III.2. Comissão Nacional de Protecção de Dados (CNPD) ⁽⁴⁶⁾

Nos termos do artigo 2.º da Lei n.º 43/2004, de 18 de Agosto (Lei de organização e funcionamento da Comissão Nacional de Protecção de Dados), “a CNPD é uma entidade administrativa independente, com poderes de autoridade (artigo 21.º Lei n.º 67/98), que funciona junto da Assembleia da República, com as atribuições e competências definidas na lei”.

“A Constituição impõe ao legislador a definição do regime jurídico da protecção dos particulares relativamente ao tratamento automatizado, conexão e transmissão e utilização de dados pessoais (n.º 2, 2.ª parte). A protecção incumbirá, desde logo, aos órgãos públicos com competência geral para a defesa dos direitos, liberdades e garantias. Perante a insuficiência da exclusiva protecção jurisdicional, a Revisão de 1997 faz expressa alusão à protecção através da entidade administrativa independente, tornando incontornável a obrigatoriedade da criação desta entidade pelo legislador (cfr. artigo 267.º, n.º 3 da CRP). Neste contexto, a lei instituiu a

⁽⁴⁶⁾ Nos termos do artigo 25.º da Lei n.º 67/98, a CNPD é composta por 7 membros: o presidente e dois vogais são eleitos pela Assembleia da República; dois vogais são magistrados (um judicial e um do Ministério Público) com mais de 10 anos de carreira e designados, respectivamente, pelo Conselho Superior da Magistratura e pelo Conselho Superior do Ministério Público; dois vogais são designados pelo Governo.

Comissão Nacional de Protecção de Dados, cuja atribuição principal é a de “controlar e fiscalizar o incumprimento das disposições legais e regulamentares em matéria de dados pessoais, em rigoroso respeito pelos direitos da pessoa e pelas liberdades e garantias consagradas na Constituição e na lei” (cfr. Lei n.º 67/98, art. 22.º, n.º 1, e Lei n.º 43/2004, de 18/08)”⁽⁴⁷⁾.

A CNPD é uma entidade administrativa independente, cujas funções consistem em “controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de protecção de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei” (artigo 22.º, n.º 1 da Lei 67/98).

Nos termos do artigo 27.º da Lei n.º 67/98, os responsáveis pelo tratamento de dados pessoais devem fazer a respectiva notificação junto da CNPD, antes da realização do tratamento ou conjunto de tratamentos.

Esta notificação deverá ser feita por via electrónica, através do preenchimento de um formulário próprio – “Formulário Geral de Notificação” (disponível em www.cnpd.pt), e tem o objectivo de se proceder a um controlo prévio por parte da CNPD, nos termos do artigo 28.º da Lei n.º 67/98. De facto, tratando-se de dados sensíveis (relativos à vida privada do trabalhador), prevê o n.º 2 do artigo 7.º que, não existindo uma disposição legal nesse sentido (como sucede nas situações de acesso a determinadas profissões em que a lei exige a existência de um registo criminal, ou mesmo para efeitos de segurança e saúde no trabalho), torna-se necessária, para além da notificação descrita, a autorização prévia da CNPD, sendo também exigível a existência de motivos de interesse público ou o consentimento expresso do trabalhador para esse tratamento. É entendimento da CNPD que este interesse público poderá corresponder a um interesse sério da empresa, nomeadamente quando esta pretende disciplinar o uso de ferramentas de trabalho por forma a garantir a segurança, eficácia e operacionalidade das mesmas.

Ainda que o empregador não consulte os dados pessoais do trabalhador (e exceptuando as situações de dispensa de notificação que veremos de seguida) esta notificação à CNPD será sempre necessária, pois a possibilidade dessa consulta estará sempre presente. Sem esta notificação, o Regulamento (ou documento realizado sob outra forma) não produzirá efeitos e o empregador incorrerá numa contra-ordenação, como melhor veremos mais adiante.

⁽⁴⁷⁾ J.J. Gomes Canotilho e Vital Moreira, em comentário ao artigo 35.º da “Constituição da República Portuguesa Anotada”, Volume I, 4.ª Edição Revista, Artigos 1.º a 107.º, Coimbra Editora, 2007, p. 553-554.

Esta notificação está sujeita ao pagamento de uma taxa, fixada pela CNPD, na Deliberação 50/2011, publicada no Diário da República n.º 5, II Série, de 7 de Janeiro de 2011, a qual deverá ser paga por via electrónica no prazo de 3 dias úteis após a submissão (também electrónica) do formulário (cfr. artigo 6.º da Deliberação).

O pagamento da taxa de notificação electrónica pode ser efectuado por transferência bancária, através do sistema de banco electrónico ou directamente no balcão de agência bancária, por cheque emitido à ordem da CNPD ou por numerário entregue nas suas instalações, sendo obrigatoriamente indicado o código de pagamento fornecido pela CNPD no momento da submissão do formulário (cfr. artigo 7.º da Deliberação).

Na impossibilidade de submissão electrónica, serão aceites notificações em suporte de papel, apresentadas directamente nos serviços da CNPD ou remetidas por correio postal, desde que acompanhadas do respectivo pagamento, que, para este efeito, só poderá ser efectuado por cheque emitido à ordem da CNPD ou em numerário entregue nas suas instalações (cfr. artigo 8.º da Deliberação).

Os tratamentos de dados não se consideram notificados se a taxa não for paga no prazo e nas condições previstas. Com efeito, dispõe o artigo 9.º da Deliberação que “se não forem cumpridos os procedimentos previstos nos artigos 6.º, 7.º e 8.º, a notificação não se considera efectuada”.

De acordo com o artigo 2.º da Deliberação atrás referida, a taxa em causa tem o valor de € 150,00.

Com a notificação à CNPD as entidades responsáveis devem juntar o Regulamento Interno e especificar as formas como publicitaram as condições de tratamento de dados junto dos trabalhadores. O Regulamento deverá ser enviado em anexo ao formulário electrónico, só sendo possível carregar-se um único ficheiro em formato Word, PDF ou Excel. Caso a informação esteja em vários ficheiros, o empregador terá de a reunir num ficheiro ZIP ou RAR para envio de um único ficheiro. Note-se, ainda, que o ficheiro anexado não pode ter um tamanho superior a 10 MB.

Após o pagamento da exigida taxa, o empregador recebe, por *e-mail*, um recibo com o número do processo, tendo de aguardar que a autorização da CNPD seja emitida. Durante este período de espera, poderá a CNPD solicitar mais informações ao requerente, devendo este, atento o dever de colaboração expresso no artigo 24.º da Lei n.º 67/98, facultar as informações solicitadas e disponibilizar o exame do sistema informático e dos ficheiros de dados pessoais.

A CNPD pronunciar-se-á sobre a legitimidade do requerente para o tratamento dos dados que pretende efectuar, nomeadamente averiguando a existência de interesses legítimos daquele, os quais se prenderão com a pretensão de disciplinar o uso de ferramentas de trabalho por forma a garantir a segurança, eficácia e operacionalidade das mesmas.

O artigo 29.º da Lei n.º 67/98 enumera as informações que o pedido de autorização do responsável pelo tratamento de dados deve conter, entre as quais constam as finalidades do tratamento, a descrição da categoria dos dados a tratar (nomeadamente: nome, profissão, local de trabalho, endereço electrónico do remetente, assunto da mensagem, endereço electrónico dos destinatários, data e hora de envio da mensagem), o cumprimento do direito de informação dos trabalhadores (nomeadamente quanto às finalidades da recolha e condições de utilização e controlo), a forma como os trabalhadores podem ter conhecimento e corrigir os dados pessoais que lhes respeitem, o tempo de conservação dos dados pessoais, entre outros.

Dispensa de notificação à CNPD

A entidade empregadora que permite a utilização do *e-mail* para fins privados e que não põe limitações à utilização da Internet, que não pretende estabelecer limites à utilização e, em consequência, se recusa a efectuar qualquer tipo de controlo dos trabalhadores está dispensada de notificar aqueles “registos de comunicações” (tratamentos) à CNPD.

Isenção de notificação à CNPD

A CNPD pode autorizar simplificações ou isenções de notificação em situações em que tal se revele desnecessário. Estas autorizações são publicadas em Diário da República.

Até à presente data, a CNPD proferiu 6 autorizações de isenção, tendo sido publicadas no Diário da República n.º 22, 2.ª Série, de 22 de Janeiro de 2000, e estabelecidas ao abrigo do n.º 2 do art.º 27.º:

- a) Autorização de Isenção n.º 1/99 – Processamento de Retribuições, Prestações, Abonos de Funcionários ou Empregados;
- b) Autorização de Isenção n.º 2/99 – Gestão de utentes de bibliotecas e arquivos;
- c) Autorização de Isenção n.º 3/99 – Facturação e Gestão de Contactos com Clientes, Fornecedores e Prestadores de Serviços;
- d) Autorização de Isenção n.º 4/99 – Gestão Administrativa de Funcionários, Empregados e Prestadores de Serviços;
- e) Autorização de Isenção n.º 5/99 – Registo de Entradas e Saídas de Pessoas em Edifícios;

f) Autorização de Isenção n.º 6/99 – Cobrança de Quotizações em Associações e Contactos com os respectivos Associados.

CAPÍTULO X

RESPONSABILIDADE CONTRA-ORDENACIONAL E PENAL

I. VÍCIOS

Contra-ordenações

A Lei n.º 67/98, nos seus artigos 37.º e 38.º, qualifica como contra-ordenações, puníveis com coimas (as quais, tratando-se de pessoas colectivas, e tratando-se de dados sujeitos a controlo prévio, corresponderão a um mínimo de €3.000,00 a um máximo de €30.000,00), alguns incumprimentos praticados pelo empregador, nomeadamente a omissão ou defeituoso cumprimento da obrigação de notificação à CNPD, ainda que por negligência.

A tentativa de violação das obrigações resultantes dos artigos 27.º e 29.º é sempre punida (cfr. artigo 40.º).

Também puníveis com coimas são a desobediência ao princípio da finalidade (artigo 5.º), o incumprimento do dever de informação (artigo 10.º), a violação do direito de oposição do trabalhador (artigo 12.º) – casos estes em que quer a tentativa quer a negligência são sempre puníveis.

O artigo 39.º prevê que, caso o mesmo facto constitua, simultaneamente crime e contra-ordenação (concurso de infracções), o agente seja punido a título de crime. E ainda que as sanções aplicadas às contra-ordenações em concurso são sempre cumuladas materialmente.

Crimes

Os artigos 43.º e seguintes da Lei n.º 67/98 definem como crimes (puníveis com pena de prisão ou multa) o não cumprimento de algumas obrigações relativas à protecção de dados, como sejam nomeadamente a omissão intencional de notificação ou do pedido de autorização já referido, o acesso a dados pessoais vedados sem a devida autorização, sendo que a tentativa é sempre punível (artigo 48.º).

A Lei prevê ainda, no seu artigo 49.º, a possibilidade de aplicação de uma pena acessória de proibição temporária ou definitiva do tratamento, bloqueio, apagamento ou destruição total ou parcial dos dados; publicidade da sentença condenatória; advertência ou censura públicas do responsável do tratamento.

Há ainda que atender ao disposto no artigo 194.º do Código Penal, o qual, sob a epígrafe “Violação de correspondência ou de telecomunicações”, dispõe:

“1 - Quem, sem consentimento, abrir encomenda, carta ou qualquer outro escrito que se encontre fechado e lhe não seja dirigido, ou tomar conhecimento, por processos técnicos, do seu conteúdo, ou impedir, por qualquer modo, que seja recebido pelo destinatário, é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias.

2 - Na mesma pena incorre quem, sem consentimento, se intrometer no conteúdo de telecomunicação ou dele tomar conhecimento.

3 - Quem, sem consentimento, divulgar o conteúdo de cartas, encomendas, escritos fechados, ou telecomunicações a que se referem os números anteriores, é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias.”

O procedimento criminal por este tipo de crime depende, segundo o artigo 198.º daquele Código, de queixa ou de participação, sendo o trabalhador competente para a apresentação de queixa, uma vez que é o portador concreto do bem jurídico.

Esta infracção só é punível a título de dolo, sendo bastante o dolo eventual.

II. NULIDADE DA PROVA

Como já vimos anteriormente, o controlo pelo empregador do conteúdo de mensagens marcadas como pessoais ou de mensagens que não estão qualificadas como tais mas que pelo teor dos dados externos se deduz que o sejam, ainda que em situações excepcionais em que há suspeitas de abusos ou de incumprimentos contratuais por parte do trabalhador, estando as mesmas protegidas pelo direito ao sigilo das comunicações nos termos constitucionais e também pelo artigo 22.º do CT, constituirá uma violação dos preceitos referidos anteriormente, sendo que a prova obtida será considerada nula nos termos do artigo 32.º, n.º 8 da CRP ⁽⁴⁸⁾.

Como se retira do Acórdão do Supremo Tribunal de Justiça, de 05-07-2007, processo número 07S043, em que foi relator o Juiz Conselheiro Mário Pereira e publicado em www.dgsi.pt, tais provas são, pois, inatendíveis, por violação da tutela da confidencialidade, não havendo, obviamente, “que entrar na análise do conteúdo do *e-mail* nem que apurar se esse conteúdo é violador de normas de deveres laborais e se traduz, por isso, um incumprimento contratual ou

⁽⁴⁸⁾ No mesmo sentido, o Acórdão do Tribunal da Relação de Lisboa, de 05-06-2008, processo número 2970/2008-4, em que foi relator o Juiz Desembargador Leopoldo Soares e publicado em www.dgsi.pt, “se a entidade patronal incumprir as supra citadas regras não serão de atender os decorrentes meios de prova juntos ao processo disciplinar”.

um cumprimento defeituoso”.

E isto, como já vimos, independentemente do conteúdo revestir carácter privado ou não já que a tutela constitucional é realizada em termos objectivos, independentemente do conteúdo.

Conforme *supra* exposto [Ponto VI, b)] nos termos do artigo 34.º da CRP, o empregador não poderá controlar o conteúdo sem uma prévia autorização judicial, mesmo que aquele tenha violado as regras estabelecidas pelo empregador, na medida em que a propriedade dos meios não retira a titularidade do direito e a infracção cometida pelo trabalhador é, quando muito, uma infracção disciplinar.”

III. CONTROLO FORMAL

Nos termos do artigo 23.º, n.º 1 da Lei n.º 67/98, “competem em especial à CNPD apreciar as reclamações, queixas ou petições dos particulares” [alínea k)] e “deliberar sobre a aplicação de coimas” [alínea n)].

III.1. Indeferimento do pedido de autorização para o tratamento de dados pessoais

Refere o n.º 3 do mesmo preceito que “no exercício das suas funções, a CNPD profere decisões com força obrigatória, passíveis de reclamação e recurso para o Tribunal Central Administrativo”. Deste modo, caso a CNPD indefira o pedido de autorização para o tratamento de dados pessoais, tem o empregador a possibilidade de apresentar reclamação para a CNPD e recurso para o Tribunal Central Administrativo (artigo 23.º, n.º 3 da Lei n.º 67/98) ⁽⁴⁹⁾.

Esta reclamação deverá ser efectuada no prazo de 15 dias úteis a contar da sua notificação, para o autor do acto (CNPD), nos termos dos artigos 72.º, 158.º e 162.º do Código do Procedimento Administrativo, aprovado pelo Decreto-Lei N.º 442/91, de 15 de Novembro e alterado pelo Decreto-Lei N.º 6/96, de 31 de Janeiro.

O recurso para o Tribunal Central Administrativo será interposto no prazo de 30 dias contados a partir da notificação da decisão da CNPD, nos termos do artigo 144.º do Código de Processo nos Tribunais Administrativos, aprovado pela Lei n.º 15/2002, de 22/02.

⁽⁴⁹⁾ No mesmo sentido, v. Acórdão do Tribunal Central Administrativo Sul, de 29/06/2009, processo número 05203/09, Magistrada Maria Antónia Soares e publicado em www.dgsi.pt.

III.2. Aplicação de coimas

Por outro lado, e agora relativamente à aplicação de coimas resultantes da verificação da prática de uma contra-ordenação por parte do empregador, dispõe o artigo 41.º daquela Lei que “a aplicação das coimas previstas na presente lei compete ao presidente da CNPD, sob prévia deliberação da Comissão” e que “a deliberação da CNPD, depois de homologada pelo presidente, constitui título executivo, no caso de não ser impugnada no prazo legal”.

Esta impugnação deverá ser feita no prazo 20 dias úteis após o seu conhecimento, pelo arguido, da aplicação da coima, nos termos dos artigos 59.º e 60.º do DL n.º 433/82, de 27 de Outubro (Regime geral das contra-ordenações), aplicáveis subsidiariamente *ex vi* artigo 35.º da Lei n.º 67/98.

IV. CONTROLO SUBSTANTIVO

Por outro lado, nos termos do artigo 33.º da Lei n.º 67/98, “sem prejuízo do direito de apresentação de queixa à CNPD, qualquer pessoa pode, nos termos da lei, recorrer a meios administrativos ou jurisdicionais para garantir o cumprimento das disposições legais em matéria de protecção de dados pessoais.”

Isto significa que, perante a constatação de uma violação dos seus direitos relativos ao tratamento de dados pessoais, pode o trabalhador apresentar queixa junto da CNPD, a qual será por esta apreciada [(cfr. citado artigo 23.º, n.º 1, alínea k)] ou recorrer aos Tribunais para a reposição daqueles, sem prejuízo do direito de obter do responsável a reparação pelo prejuízo sofrido, a título de responsabilidade civil (artigo 34.º da Lei n.º 67/98).

Segundo também entendimento da CNPD, “no caso de processos de contra-ordenação (aplicáveis ao empregador), as decisões da CNPD são recorríveis para os tribunais de pequena instância criminal ou para os tribunais judiciais competentes, isto é, os Tribunais de Trabalho. Não obstante, o trabalhador tem ainda a possibilidade de apresentar queixa junto da ACT, a qual remeterá a mesma para a CNPD caso considere estar em causa o tratamento de dados pessoais.

Atenta a proibição de aceder ao conteúdo dos *e-mails* pessoais do trabalhador e dos *sites* consultados pelo mesmo, em situação de litígio, caberá ao empregador provar que actuou nos termos legalmente consignados, atendendo aos requisitos legalmente exigidos. Incumbir-lhe-á, nomeadamente, provar que é detentor de uma autorização judicial prévia que o habilitasse a visualizar o conteúdo das comunicações electrónicas do trabalhador, ou, em alternativa,

apresentar meios de prova quanto ao conhecimento e consentimento do trabalhador. Para tanto, deverá este munir-se de um documento assinado e datado pelo trabalhador, que poderá constar, nomeadamente, do seu Processo Individual, comprovativo da tomada de conhecimento e aceitação das normas existentes na organização relativamente ao controlo das suas comunicações electrónicas e acessos à Internet. Deverá ainda o empregador comprovar que escolheu as formas de controlo que têm menor impacto sobre os direitos fundamentais dos trabalhadores.

O carácter ou natureza pessoal ou não das mensagens em causa dependem de apreciação e prova pelo Tribunal, cabendo ao trabalhador o ónus da prova sobre tal carácter pessoal. Esta análise não será, certamente, fácil. De facto, e conforme decorre do Ac. TRP, 08/02/2010, não é pela circunstância dos intervenientes se referirem a aspectos da empresa que, por essa simples razão, a comunicação assume desde logo um carácter profissional, legitimando a sua interceptação pelo empregador. E de igual modo, não é o facto de os meios informáticos pertencerem ao empregador que afasta a natureza privada da mensagem e o legitima a aceder ao seu conteúdo.

A falta de marca prévia, expressa e formal, da “pessoalidade” da mensagem, não afasta a tutela aí prevista. Tendo o empregador, mesmo que de boa fé, acedido ao *e-mail* do trabalhador, a natureza pessoal deste e a sua inerente confidencialidade, impunham-lhe que desistisse da leitura do seu conteúdo logo que se apercebesse dessa natureza ⁽⁵⁰⁾.

Essa obrigação legal resulta, tanto quanto entendemos, da própria natureza e finalidade da tutela constitucional e ordinária.

V. ACÇÃO DE TUTELA DA PERSONALIDADE DO TRABALHADOR

O Código de Processo do Trabalho (CPT), desde a sua revisão de 2009, inclui, para além do procedimento cautelar laboral comum, ainda um processo especial destinado à tutela da personalidade do trabalhador. Este processo destina-se a evitar a consumação de qualquer

⁽⁵⁰⁾ Neste sentido, v. Acórdão do Supremo Tribunal de Justiça, de 05-07-2007, processo número 07S043, em que foi relator o Juiz Conselheiro Mário Pereira e publicado em www.dgsi.pt (é de sublinhar, como já o fizemos *supra*, que este Acórdão é o único proferido por este douto Tribunal sobre a matéria em causa).

violação dos direitos de personalidade do trabalhador ou atenuar os efeitos da ofensa já praticada. Será, pois, este o processo a utilizar em caso de situações de ilegalidade cometidas pelo empregador em matéria de tratamento de dados pessoais.

Assim, nos termos do artigo 186.º-D daquele Código, “o pedido de providências destinadas a evitar a consumação de qualquer violação dos direitos de personalidade do trabalhador ou atenuar os efeitos da ofensa já praticada é formulado contra o autor da ameaça ou ofensa e, igualmente, contra o empregador”, sendo os requeridos citados para contestar no prazo de 10 dias. Independentemente de haver ou não contestação, o tribunal decide após a apreciação das provas produzidas (artigo 186.º-E do CPT).

“Assim, o trabalhador que veja ameaçado ou violado alguns dos direitos reconhecidos nos artigos 14.º e 22.º do CT pode lançar mão deste processo especial para pôr termo a essa ameaça ou violação, tendo o pedido de ser formulado não só contra o respectivo autor (v.g. o superior hierárquico ou companheiro de trabalho que praticou a ofensa ou dirigiu a ameaça) como ainda contra o empregador, em regime de litisconsórcio”⁽⁵¹⁾.

A acção de tutela da personalidade do trabalhador tem natureza urgente (cfr. artigo 26.º, n.º 1, alínea g) e artigo 186.º-F do CPT). No entanto, é uma natureza urgente mitigada, porquanto, sem prejuízo do disposto no n.º 2 do artigo 143.º do Código de Processo Civil, os actos a praticar em tais acções apenas têm lugar em férias judiciais quando, em despacho fundamentado, tal for determinado pelo juiz (artigo 26.º, n.º 2 do CPT), pelo que, no silêncio do juiz, não correm em férias.

⁽⁵¹⁾ Abílio Neto, em anotação ao artigo 186.º-D, in “Código de Processo do Trabalho Anotado”, Ediforum, Edições Jurídicas, Lda, Lisboa, 2011, p. 424.

CONCLUSÃO

A Internet alterou a nossa forma de viver, de trabalhar e, até, de pensar. De facto, hoje, perante qualquer dúvida que possa surgir ou qualquer necessidade de contactar um serviço ou de fazer uma pesquisa quase que involuntariamente o homem tende a recorrer à Internet para a satisfação dessas necessidades, na medida em que as possibilidades que esta oferece são ilimitadas. Nas relações entre empresas e clientes, na poupança de tempo e custos, na rapidez, qualidade e quantidade de informação a que temos acesso, nos serviços que nos oferece, na interactividade que proporciona, a Internet representa o maior e melhor instrumento de gestão existente. Atrevemo-nos a afirmar que, hoje em dia, seria quase inimaginável vivermos e trabalharmos sem esta “máquina”. A sua eliminação implicaria um inimaginável retrocesso social, económico, político e legal da sociedade.

Mas a grande questão dos tempos modernos prende-se em decidir qual o valor a atribuir às vantagens conseguidas pelo uso das novas tecnologias de informação e comunicação face ao desvalor que implica perante os direitos fundamentais constitucionalmente previstos. Poderemos entender que vivemos hoje o tempo do primado do homem tecnológico em detrimento do homem dotado de individualidade própria e de valores fundamentais. Até agora, todo o ordenamento jurídico português assenta na tutela e no primado dos direitos do homem, e isso é visível não só no Código Civil como na CRP, como mesmo na lei penal (v.g. artigo 70.º e segs. do Código Civil, artigo 24.º e segs. da CRP, artigo 131.º e segs. do Código Penal). Ou seja, o núcleo do bem jurídico a proteger encontra-se caracterizado por todos estes direitos fundamentais, nos quais encontramos o direito à reserva da vida privada. Conciliar este postulado com as vantagens oferecidas pelas NTIC tem sido de facto o grande desafio que várias controvérsias tem levantado e que tem suscitado a constante necessidade de intervenção de autoridades reguladoras à medida que situações novas se vão desenrolando na sociedade em termos de impactos das novas tecnologias. Referimo-nos, em concreto, à CNPD que, recorrentemente, emite orientações neste sentido como sucedeu mais recentemente na Deliberação n.º 1638/2013, de 16 de Julho.

Se ainda se poderá dizer que o homem é livre nas suas escolhas no que respeita à exposição ou não da sua vida privada, o mesmo não poderá dizer-se no que respeita aos seus dados pessoais, na medida em que, para qualquer acto da sua vida, hoje é exigida a recolha e o tratamento informático desses mesmos dados. Tais factos são constatados se pensarmos que

para um simples pagamento da água, da luz, ou para o fornecimento de informações fiscais, é necessário o tratamento destes dados.

É tempo de reflectirmos se hoje atribuímos o mesmo valor que atribuíamos há décadas atrás relativamente a toda a tipologia de dados pessoais. É assim tão importante hoje que seja inacessível a terceiros o nosso nome, estado civil, morada? Ou é tão vulgar a inserção destes dados em ficheiros automáticos de entidades públicas e privadas que passou a ser desvalorizada esta informação? Naturalmente que o acesso à Internet não passará apenas pela simples partilha ou exposição de dados pessoais – esse acesso poderá reflectir muito mais de nós: as nossas preferências, as nossas escolhas. Poderá ainda reflectir aquilo que não queremos que seja conhecido de toda a gente. Mas o acesso à internet é feito de forma consciente e voluntária, pelo que o agente, ao aceder à mesma, representa para si os impactos que tal implica.

Quando se fala em contexto da relação jurídica laboral, parece-me que a esfera de liberdade nesta matéria é mais diminuta ainda, ou seja, se hoje, ao acedermos às novas tecnologias, enquanto indivíduos, sabemos do grau de lesão que a protecção dos nossos direitos pode sofrer em virtude de ser possível a terceiros conhecerem os nossos dados, gostos, etc., por maioria de razão se deverá compreender que a utilização das novas tecnologias enquanto ferramentas de trabalho, propriedade do empregador, nos expõe ainda mais e limita a protecção que pretendemos ter relativamente ao uso dessas ferramentas. De facto, sendo dado conhecimento de que o empregador pode aceder e controlar todos os acessos à Internet bem como *e-mails*, não pode ser desconhecido de um colaborador o grau de intrusão a que está sujeito. Naturalmente que se poderá dizer que o colaborador pode controlar o que faz e o que emite em sede de *e-mails* mas já não se poderá dizer o mesmo quanto aos *e-mails* que recebe. Efectivamente, o acesso do empregador aos *e-mails* do colaborador, ainda que este se encontre devidamente informado dessa prerrogativa, nunca poderá deixar de ser efectuado ou na sua presença e após aviso para o efeito, por forma a que este possa identificar os *e-mails* que tenham informação de índole pessoal, precisamente porque não é possível controlar os conteúdos das mensagens recebidas.

Ter conhecimento é ter poder. E o empregador, sendo desde logo detentor de uma posição de supremacia relativamente ao trabalhador, através da informação que a Internet lhe possibilita obter acerca dos seus trabalhadores, adquire cada vez mais um quase infinito poder sobre aquele, cuja esfera da vida pessoal se torna cada vez mais transparente aos olhos do mesmo.

Este crescente poder de controlo sobre o trabalhador poderá ser nocivo para a sua saúde, quer física quer psicologicamente, podendo, em casos extremos, originar stress, depressões, fadiga, ansiedade e situações de assédio moral.

É hoje mais do que evidente que o avanço tecnológico encontra-se presente nas empresas, sendo incontornável as vantagens que apresenta enquanto ferramenta de trabalho.

É no entanto discutível se o empregador, perante os direitos da personalidade do trabalhador (nomeadamente, o respeito pela sua vida privada), pode controlar ou ter acesso ao correio electrónico do seu trabalhador.

Os argumentos favoráveis a esse acesso resumem-se à titularidade/propriedade de tais meios de comunicação pelo empregador; ao poder directivo do mesmo, o qual lhe permite dirigir, controlar e punir a prestação de trabalho dos seus trabalhadores; à responsabilização da empresa pelos actos dos seus trabalhadores, tornando-se razoável que faça a fiscalização e leitura das mensagens recebidas e emitidas nos computadores da empresa.

Em sentido contrário, os argumentos centram-se no facto de que o direito de propriedade não é absoluto e deve ceder perante a garantia da privacidade das comunicações, que só pode ser suprimida por ordem judicial; no poder de direcção do empregador, que é relativo e que não se pode sobrepor à intimidade e à privacidade do trabalhador; na possibilidade da empresa poder prevenir a responsabilidade pelos actos praticados pelos seus trabalhadores, designadamente adoptando programas impeditivos do envio de mensagens para endereços não pré-determinados ou proibindo a remessa de imagens não relacionadas com o desempenho das tarefas contratuais, por meio de códigos de conduta, ou mesmo, não atribuindo um endereço electrónico a cada trabalhador, por forma a que estes utilizem apenas o endereço institucional da empresa, inibindo-se assim o uso do mesmo para fins pessoais.

Já no que respeita à utilização da Internet, ponto assente é que se torna essencial valorizar-se o trabalhador que tem uma atitude pró-activa, que procura informação para além daquela que consta em *sites* normais de pesquisa, tentando ampliar e aprofundar a sua prestação de trabalho, contribuindo para as possibilidades de negócios da empresa com eventuais reduções de custos. Por outro lado, é de desvalorizar o trabalhador que utiliza a Internet e o correio electrónico, que estão à sua disposição, para finalidades estritamente pessoais, tais como jogos ou pesquisas de lazer. Em face dessa utilização inadequada defendemos que o empregador tome as medidas necessárias para impedir essa utilização. No entanto, mesmo em situações de abuso, o empregador terá de se cingir à visualização de apenas determinados

dados externos, como por exemplo, a frequência no número de comunicações de carácter pessoal. Para tanto, será aconselhável o conhecimento prévio por parte do trabalhador e a presença de um representante da Comissão de Trabalhadores, que tutele os direitos daquele, controlando as garantias de transparência, sendo exigível ainda que, em caso de procedimento disciplinar, o empregador não descure o princípio da proporcionalidade e o nexo causal entre a prática abusiva e a sanção a aplicar.

O empregador deverá, para tanto, estabelecer, de início, as regras do “jogo”, as quais serão transpostas, nomeadamente, em Regulamento Interno de Empresa, salientando que nem o *e-mail* nem a consulta da Internet são os meios idóneos para finalidades pessoais, embora possíveis desde que utilizados prudentemente e sem que acarretem prejuízos para a empresa.

De facto, o trabalhador passa a maior parte do seu tempo num computador e o esbatimento das fronteiras espaço-temporais da relação de trabalho justifica que o empregador consinta na utilização (prudente) destes meios.

Por conseguinte, o empregador deverá indicar claramente, aos trabalhadores, as condições em que o uso privado da Internet é permitido, bem como especificar o material que não pode ser visualizado ou copiado, e assegurar que aqueles conhecem as formas de controlo utilizadas na empresa – ou seja, é de toda a conveniência a existência e a divulgação adequadas da política de monitorização do correio electrónico e da Internet.

“Se se pretende implementar uma política de utilização do *e-mail*, e defendemos que essa mesma política seja anexada ao contrato de trabalho, a administração deve tomar algumas medidas:

- Informar os seus empregados dos riscos inerentes a um uso abusivo e impróprio do *e-mail* e fazê-los compreender que o *e-mail* é atribuído para facilitar a sua actividade profissional;
- O uso inadequado do *e-mail* pode colocar em perigo o sistema de segurança da empresa, a privacidade dos funcionários e de todos os outros e acarretar responsabilidade legal para a organização;
- A política adoptada deve ser revista e actualizada, acompanhando o desenvolvimento acelerado da Internet e das Tecnologias de Informação;
- O funcionário deve compreender que uma utilização pautada por razoáveis níveis de bom senso vai acabar por levar o empregador a flexibilizar a política inicial, adaptando-a às suas necessidades e tornando-a menos restritiva;
- Deve evitar-se o envio/recepção de mensagens através do *e-mail* da empresa que visem perturbar, hostilizar, difamar, injuriar ou transmitir pornografia;

- O empregado vai certamente aceitar mais facilmente a actividade de monitorização se tiver conhecimento do tipo de informação que vai ser monitorizada, da forma como se pretende tratar e de quem vai tratar essa mesma informação.

Parece-nos bastante mais sensato que se o empregado deseja que a sua mensagem assuma um carácter verdadeiramente privado, é preferível não usar o *e-mail* da empresa e limitar a sua utilização aos assuntos estritamente profissionais! ⁽⁵²⁾”

O tratamento destes dados pessoais sensíveis, referentes à vida privada do trabalhador, depende de notificação e autorização da CNPD, excepto quando o empregador permitir a utilização do *e-mail* para fins privados e não colocar limitações à utilização da Internet, não pretender estabelecer limites à utilização e, em consequência, se recusar a efectuar qualquer tipo de controlo dos trabalhadores.

É assente, pois, como princípio fundamental, a necessidade de as entidades empregadoras procederem à notificação destes tratamentos à CNPD, já que o controlo e a verificação dos *e-mails* e, bem assim, do grau de utilização da Internet constituem verdadeiros tratamentos de dados pessoais dos trabalhadores e, conseqüentemente, há que adoptar medidas que salvaguardem a sua privacidade.

A jurisprudência é muito restritiva quanto às possibilidades de controlo do correio electrónico na empresa.

Defendemos que a monitorização do *e-mail* e da Internet pelo empregador deverá ser feita de forma aleatória e não persecutória e ter como finalidade primordial a promoção do sistema informático e da sua *performance*. “O *e-mail* pode estar ao serviço da empresa mas tem de se respeitar o facto de que um acesso indiscriminado e excessivo pela entidade empregadora ao conteúdo do mesmo, reduz ao mínimo uma das vertentes principais do direito ao trabalho. Isto porque este direito não exige apenas que o seu exercício seja acompanhado de condições adequadas de salubridade e higiene mas também que requisitos básicos relativos à liberdade de autodeterminação e dignidade profissional sejam respeitados ⁽⁵³⁾”.

Este controlo deve, pois, ser limitado, mas não tanto que se torne impraticável ao empregador, em função da aplicação do princípio da boa fé, ou melhor, da sua não transgressão, controlar

⁽⁵²⁾ Paula Rainha e Sónia Queiroz Vaz, *op. cit.* pp. 57-58.

⁽⁵³⁾ Paula Rainha e Sónia Queiroz Vaz, *op. cit.* p. 67.

questões adjacentes a estes tipos de comunicação, nomeadamente o custo das ferramentas de trabalho da empresa, o tempo gasto pelos trabalhadores na utilização das mesmas e o acesso à rede informática, fazendo cessar ou não a relação de trabalho com base numa utilização inadequada ou abusiva daquelas.

Acresce, ainda, que determinado tipo de acções de “fiscalização” pode assumir claramente os contornos de controlo de correspondência e/ou interceptação de conversações ou comunicações, sujeitas ao regime fixado nos artigos 179.º e 187.º e seguintes do Código de Processo Penal, aplicáveis *ex vi* artigo 190.º do mesmo complexo normativo.

Recordemos as palavras de José de Faria Costa: “E se alguém aceder ao conteúdo de uma informação veiculada por *e-mail*? Poderemos nós aplicar o art. 194.º do Código Penal? A matéria é, como se vê, de extraordinária actualidade, porquanto as situações de violação daquele conteúdo informacional privado irão, mais tarde ou mais cedo, suscitar uma questão jurídico-penal. Sem se querer avançar com qualquer posição minimamente definitiva – o que seria sinal de insensatez e de comezinha petulância intelectual –, julgamos ser pertinente lembrar um ou dois princípios fundamentais nesta matéria. O primeiro é o de que a interpretação analógica, relativamente à norma incriminadora, é absolutamente proibida⁽⁵⁴⁾. O segundo prende-se com este, mas ganha autonomia, porquanto se pode, pois, defender que, sendo proibida a interpretação analógica, não o é a interpretação extensiva.

Ora, assim sendo, tanto mais que a lei fala em conteúdo de telecomunicação, parece, por conseguinte, defensável dizer-se que quem perscrutar e aceder ao conteúdo informacional veiculado por *e-mail* comete o crime previsto no n.º 2 do art. 194.º. Repare-se que o tipo legal de crime não se refere a escrito, como acontece no n.º 1, caso em que seria muito mais difícil ou até impossível aplicar esta norma incriminadora, já que, nessas circunstâncias, se não está perante palavra escrita mas, como se viu, perante palavra virtual. Todavia, a palavra virtual dá-nos conteúdos de significações, quer como a palavra escrita, quer como a palavra falada. Foi esse conteúdo que o legislador quis continuar a preservar. E a preservar tendo em consideração os novos meios de telecomunicação. E o chamado correio electrónico é, sem sombra de dúvida, um eficaz e potentíssimo meio de comunicação à distância. Um, hoje, indispensável meio de telecomunicação.⁽⁵⁵⁾”

⁽⁵⁴⁾ Cfr. artigo 1.º, n.º 3 do Código Penal.

⁽⁵⁵⁾ José de Faria Costa, “As telecomunicações e a privacidade: o olhar in(discreto) de um penalista” in “As Telecomunicações e o Direito na Sociedade da Informação”, Coimbra, 1999, p. 71.

Por outro lado, não podemos perder de vista que, tal como resulta do disposto nos artigos 194.º e 198.º do Código Penal e do artigo 44.º da Lei n.º 67/87, o procedimento criminal depende de queixa. Daí que qualquer iniciativa incriminatória passe, necessariamente, por um impulso processual da pessoa que vê devassada a mensagem.

O controlo da actuação da entidade empregadora pode, pois, ser efectuado pelos trabalhadores (v.g. através do direito de acesso, correcção e exercício do direito de oposição) e pela CNPD, nos termos do artigo 27.º, n.º 1 e 2 da Lei n.º 67/98. Este controlo não poderá, actualmente, passar pela Autoridade para as Condições do Trabalho, atento o facto de ter desaparecido legalmente a obrigação de envio do regulamento interno àquela entidade.

Note-se que, nos termos do n.º 3 deste artigo 194.º, não só é ilícito o conhecimento não autorizado do conteúdo de mensagens pessoais, como também a sua divulgação, tal como sucede com o destinatário de cartas-missivas confidenciais, nos termos dos artigos 75.º, 76.º e 78.º do Código Civil. De igual modo, o artigo 22.º do CT estabelece o direito à confidencialidade das mensagens de natureza pessoal dos trabalhadores através de vários meios de comunicação, nomeadamente o *e-mail*. A protecção conferida abrange, pois, não apenas o acesso a tais mensagens como também a sua divulgação.

Ora, se existir consentimento das partes, o terceiro pode conhecer o conteúdo. No entanto, no âmbito da relação laboral, este consentimento poderá ser relativo e não totalmente livre, atenta a posição de subordinação em que o trabalhador se encontra. Pelo que, terá, pois, de haver uma autorização prévia e voluntária do trabalhador, e, mesmo nesta situação, tal autorização será revogável a todo o tempo, nos termos do artigo 81.º, n.º 2 do Código Civil.

O consentimento do titular dos dados pessoais, livre e individualmente prestado, é um dos elementos fundamentais do direito à autodeterminação informativa. Mas, numa relação de trabalho, o consentimento prestado pelo trabalhador será, efectivamente, um consentimento livre? No nosso entender, o legislador deveria ter tido em atenção as especificidades da relação laboral e ter adoptado uma legislação própria.

Pelo que, a legitimidade da entidade empregadora para tratar determinado tipo de dados, especialmente quando afectam alguns direitos dos trabalhadores (v.g. a sua intimidade ou privacidade, deve passar, cada vez menos, pelo consentimento ou, mesmo, por disposições de natureza contratual, devendo, preferencialmente, assentar em disposições legais. Por isso, o nosso legislador tem, ainda, um longo caminho a percorrer. É neste sentido que o Direito do Trabalho deve equilibrar os interesses em causa: a livre iniciativa e a autonomia privadas do

empregador e a integridade física e a reserva da intimidade da vida privada do trabalhador, sempre numa óptica de acompanhar o ritmo da sociedade.

BIBLIOGRAFIA

Ascensão, José de Oliveira – “A Sociedade da Informação” *in* “Direito da Sociedade da Informação”, Volume I, Coimbra Editora, 1999, pág. 163-184.

Canotilho, J.J. Gomes e Moreira, Vital – “Constituição da República Portuguesa Anotada”, Volume I, 4.^a Edição Revista, Artigos 1.º a 107.º, Coimbra Editora, 2007.

Castro, Catarina Sarmiento e – “Direito da Informática, Privacidade e Dados Pessoais”, Almedina, 2005.

Cordeiro, António Menezes – “O respeito pela esfera privada do trabalhador” *in* I Congresso Nacional de Direito do Trabalho – Memórias (Coordenação António Moreira), Almedina, 1998, pág. 17-37.

Costa, José de Faria – “As telecomunicações e a privacidade: o olhar in(discreto) de um penalista” *in* “As Telecomunicações e o Direito na Sociedade da Informação”, Coimbra, 1999, pág. 49-78.

Dias, Jorge de Figueiredo, com a direcção de “Comentário Conimbricense do Código Penal, Parte Especial”, Coimbra Editora, 1999.

Fernandes, António Monteiro – “Direito do Trabalho”, 13.^a Edição, Almedina, 2006.

Gomes, Manuel Januário – “O problema da salvaguarda da privacidade antes e depois do computador” *in* BMJ n.º 319, pág. 31, 1982.

Guerra, Amadeu – “A privacidade no Local de Trabalho – As Novas Tecnologias e o Controlo dos Trabalhadores através de Sistemas Automatizados – Uma abordagem ao Código do Trabalho”, Almedina, 2004.

Guerra, Amadeu – “Telecomunicações e Protecção de Dados” *in* “As Telecomunicações e o Direito na Sociedade da Informação”, Coimbra, 1999, pág. 107-121.

Guerra, Amadeu – “A lei de protecção de dados pessoais” *in* “Direito da Sociedade da Informação”, Volume II, Coimbra Editora, 2001, pág. 145.

Guerra, Amadeu – “Informática e Tratamento de Dados Pessoais – Os direitos dos cidadãos e as obrigações dos responsáveis pelos tratamentos automatizados”, Vislis Editores, 1997.

Marecos, Diogo Vaz – “Código do Trabalho Anotado”, Coimbra Editora, 2010.

Martinez, Pedro Romano – “Relações entre empregador e empregado” *in* “Direito da Sociedade da Informação”, Volume I, Coimbra Editora, 1999, pág. 185-200.

Martinez, Pedro Romano, Monteiro, Luís Miguel, Vasconcelos, Joana, Brito, Pedro Madeira de, Dray, Guilherme e Silva, Luís Gonçalves da – “Código do Trabalho Anotado”, Almedina, 2013.

Martins, Pedro Furtado – “A crise do contrato de trabalho”, *in* RDES n.º 4, 1997, pág. 335-368.

Moniz, Helena – “Internet e Globalização – Problemas Jurídico-Penais” *in* “As Telecomunicações e o Direito na Sociedade da Informação”, Coimbra, 1999, pág. 367-385.

Moreira, Teresa Alexandra Coelho – “Estudos de Direito do Trabalho”, Almedina, 2011.

Moreira, Teresa Alexandra Coelho – “A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: contributo para um estudo dos limites do poder de controlo electrónico do empregador”, Almedina, 2010.

Moreira, Teresa Alexandra Coelho – “Da Esfera Privada do Trabalhador e o Controlo do Empregador”, *Studia Iuridica*, n.º 78, Coimbra Editora, 2004.

Neto, Abílio – “Novo Código do Trabalho e Legislação Complementar Anotados”, Ediforum, Edições Jurídicas, Lda, Lisboa, 2010.

Neto, Abílio – “Código de Processo do Trabalho Anotado”, Ediforum, Edições Jurídicas, Lda, Lisboa, 2011.

Neto, Abílio – “Código Civil Anotado”, Ediforum, Edições Jurídicas, Lda, Lisboa, 2010.

Rainha, Paula e Vaz, Sónia Queiroz – “Guia Jurídico da Internet em Portugal”, 2001.

Ramalho, Maria do Rosário Palma – “Direito do Trabalho – Parte II – Situações Laborais Individuais”, Almedina, Coimbra, 2006.

Vasconcelos, Joana – “O Contrato de Trabalho: 100 Questões”, Universidade Católica Editora, 3.^a Edição, 2010.

Vasconcelos, Pedro Pais de – “Protecção de dados pessoais e direito à privacidade” *in* “Direito da Sociedade da Informação”, Volume I, Coimbra Editora, 1999, pág. 241-253.

Xavier, Bernardo da Gama Lobo, com a colaboração de Martins, Pedro Furtado, Carvalho, António Nunes de, Vasconcelos, Joana e Almeida, Tatiana Guerra de – “Manual de Direito do Trabalho”, Verbo, 2011.

Xavier, Bernardo da Gama Lobo – “Procedimentos Laborais na Empresa – Ensinar e Investigar”, Universidade Católica Editora, 2009.

Páginas da Internet:

www.google.pt

www.sapo.pt

<http://pt.wikipedia.org>

www.ucp.pt

www.dre.pt

www.datajuris.pt

<http://www.pgdlisboa.pt>

www.dgsi.pt

<http://eur-lex.europa.eu>

www.stj.pt

www.cnpd.pt

<http://www.acessibilidade.gov.pt/docs/lverde.htm>

ANEXO I

ASSENTO LEGAL

AS PRINCIPAIS DISPOSIÇÕES INTERNACIONAIS, EUROPEIAS E NACIONAIS

I. A PROTECÇÃO DA PRIVACIDADE NO DIREITO INTERNACIONAL

➤ **Declaração Universal dos Direitos do Homem** ⁽⁵⁶⁾

Artigo 12.º

“Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a protecção da lei”.

➤ **Pacto Internacional relativo aos Direitos Civis e Políticos** ⁽⁵⁷⁾

Artigo 17.º

“1. Ninguém será objecto de ingerências arbitrárias ou ilegais na sua vida privada, na sua família, o seu domicílio ou na sua correspondência, nem de ataques ilegais à sua honra e reputação.

2. Toda a pessoa tem direito a protecção da lei contra essas ingerências ou esses ataques.”

⁽⁵⁶⁾ Aprovada pela Assembleia Geral das Nações Unidas a 10 de Dezembro de 1948.

⁽⁵⁷⁾ Assinado em Nova Iorque a 7 de Outubro de 1976. Ratificado por Portugal através da Lei n.º 29/78, de 12 de Junho.

II. A PROTECÇÃO DA PRIVACIDADE NO DIREITO EUROPEU

- **Convenção Europeia dos Direitos do Homem (Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais) ⁽⁵⁸⁾**

Artigo 8º

Direito ao respeito pela vida privada e familiar

“1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.”

- **Convenção para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal (Convenção 108 do Conselho da Europa) ⁽⁵⁹⁾**

Artigo 1.º

Objectivos e finalidade

“A presente Convenção destina-se a garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito («protecção dos dados»).”

- **Directiva 95/46/CE, do Parlamento e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados ⁽⁶⁰⁾**

Artigo 1.º

“1. Os Estados-Membros assegurarão, em conformidade com a presente directiva, a protecção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais.”

⁽⁵⁸⁾ Assinada em Roma a 4 de Novembro de 1950, entrou em vigor na ordem internacional a 3 de Setembro de 1953, e foi aprovada, para ratificação, pela Lei n.º 65/78, de 13 de Outubro.

⁽⁵⁹⁾ Adoptada e aberta à assinatura em Estrasburgo, a 28 de Janeiro de 1981. Aprovada para ratificação pela Resolução da Assembleia da República n.º 23/93, de 9 de Julho. Ratificada pelo Decreto do Presidente da República, n.º 21/93, de 9 de Julho.

⁽⁶⁰⁾ Adoptada a 24 de Outubro de 1995 e publicada no Jornal Oficial das Comunidades Europeias a 23 de Novembro de 1995.

➤ **Carta dos Direitos Fundamentais da União Europeia ⁽⁶¹⁾**

Artigo 7.º

Respeito pela vida privada e familiar

“Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.”

Artigo 8.º

Protecção de dados pessoais

“1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.

2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.

3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.”

⁽⁶¹⁾ Proclamada solenemente em Nice, a 7 de Dezembro de 2000, pelo Parlamento Europeu, pelo Conselho Europeu e pela Comissão Europeia, e publicada no Jornal Oficial das Comunidades Europeias de 18 de Dezembro de 2000.

III. A PROTECÇÃO DA PRIVACIDADE NO ORDENAMENTO JURÍDICO PORTUGUÊS

➤ **Constituição da República Portuguesa ⁽⁶²⁾**

Artigo 26.º

Outros dados pessoais

“1. A todos são reconhecidos os direitos à identidade pessoal (...), à reserva da intimidade da vida privada e familiar (...).”

Artigo 32.º

Garantias de processo criminal

“8. São nulas todas as provas obtidas mediante (...), abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações.”

Artigo 34.º

Inviolabilidade do domicílio e da correspondência

“1. O domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis.

2. A entrada no domicílio dos cidadãos contra a sua vontade só pode ser ordenada pela autoridade judicial competente, nos casos e segundo as formas previstos na lei.

3. Ninguém pode entrar durante a noite no domicílio de qualquer pessoa sem o seu consentimento, salvo em situação de flagrante delito ou mediante autorização judicial em casos de criminalidade especialmente violenta ou altamente organizada, incluindo o terrorismo e o tráfico de pessoas, de armas e de estupefacientes, nos termos previstos na lei.

4. É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvo os casos previstos na lei em matéria de processo criminal.”

⁽⁶²⁾ Aprovada em 2 de Abril de 1976, na redacção que lhe foi dada pelas Leis Constitucionais n.ºs 1/82, de 30 de Setembro; 1/89, de 8 de Julho; 1/92, de 25 de Novembro; 1/97, de 20 de Setembro; 1/2001, de 12 de Dezembro; 1/2004, de 24 de Julho; e 1/2005, de 12 de Agosto.

Artigo 35.º

Utilização da informática

“2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente.

3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.

4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei.”



Código do Trabalho, aprovado pela Lei n.º 7/2009, de 12 de Fevereiro ⁽⁶³⁾

Artigo 22.º

Confidencialidade de mensagens e de acesso a informação

“1. O trabalhador goza do direito de reserva e confidencialidade relativamente ao conteúdo das mensagens de natureza pessoal e acesso a informação de carácter não profissional que envie, receba ou consulte, nomeadamente através do correio electrónico.

2. O disposto no número anterior não prejudica o poder de o empregador estabelecer regras de utilização dos meios de comunicação na empresa, nomeadamente do correio electrónico.”

Artigo 106.º

Dever de informação

“1. O empregador tem o dever de informar o trabalhador sobre aspectos relevantes do contrato de trabalho.”

⁽⁶³⁾ Aprovado pela Lei n.º 7/2009, de 12 de Fevereiro; rectificado pela Declaração de Rectificação n.º 21/2009, de 18 de Março; e alterado pelas Leis n.ºs 105/2009, de 14 de Setembro), 53/2011, de 14 de Outubro, 23/2012, de 25 de Junho e 47/2012, de 29 de Agosto).

➤ **Código Civil ⁽⁶⁴⁾**

Artigo 80.º

Direito à reserva sobre a intimidade da vida privada

“1. Todos devem guardar reserva quanto à intimidade da vida privada de outrem.

2. A extensão da reserva é definida conforme a natureza do caso e a condição das pessoas.”

➤ **Lei n.º 67/98, de 26 de Outubro (Lei da Protecção de Dados Pessoais)**

Artigo 3.º

Definições

“a) «Dados pessoais»: qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável a pessoa que possa ser identificada directa ou indirectamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social.”

b) «Tratamento de dados pessoais» («tratamento»): qualquer operação ou conjunto de operações sobre dados pessoais, efectuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição”

Artigo 5.º

Qualidade dos dados

“1 — Os dados pessoais devem ser:

a) Tratados de forma lícita e com respeito pelo princípio da boa fé;

b) Recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser posteriormente tratados de forma incompatível com essas finalidades;

⁽⁶⁴⁾ Aprovado pelo Decreto-Lei n.º 47 344, de 25 de Novembro de 1966.

c) Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e posteriormente tratados;

d) Exactos e, se necessário, actualizados, devendo ser tomadas as medidas adequadas para assegurar que sejam apagados ou rectificad os dados inexactos ou incompletos, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente;

e) Conservados de forma a permitir a identificação dos seus titulares apenas durante o período necessário para a prossecução das finalidades da recolha ou do tratamento posterior.

2 — Mediante requerimento do responsável pelo tratamento, e caso haja interesse legítimo, a CNPD pode autorizar a conservação de dados para fins históricos, estatísticos ou científicos por período superior ao referido na alínea e) do número anterior.

3 — Cabe ao responsável pelo tratamento assegurar a observância do disposto nos números anteriores.”

Artigo 6.º

Condições de legitimidade do tratamento de dados

“O tratamento de dados pessoais só pode ser efectuado se o seu titular tiver dado de forma inequívoca o seu consentimento ou se o tratamento for necessário para:

a) Execução de contrato ou contratos em que o titular dos dados seja parte ou de diligências prévias à formação do contrato ou declaração da vontade negocial efectuadas a seu pedido;

b) Cumprimento de obrigação legal a que o responsável pelo tratamento esteja sujeito;

c) Protecção de interesses vitais do titular dos dados, se este estiver física ou legalmente incapaz de dar o seu consentimento;

d) Execução de uma missão de interesse público ou no exercício de autoridade pública em que esteja investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados;

e) Prossecução de interesses legítimos do responsável pelo tratamento ou de terceiro a quem os dados sejam comunicados, desde que não devam prevalecer os interesses ou os direitos, liberdades e garantias do titular dos dados.”

Artigo 7.º

Tratamento de dados sensíveis

“1 — É proibido o tratamento de dados pessoais referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica,

bem como o tratamento de dados relativos à saúde e à vida sexual, incluindo os dados genéticos.

2 — Mediante disposição legal ou autorização da CNPD, pode ser permitido o tratamento dos dados referidos no número anterior quando por motivos de interesse público importante esse tratamento for indispensável ao exercício das atribuições legais ou estatutárias do seu responsável, ou quando o titular dos dados tiver dado o seu consentimento expresso para esse tratamento, em ambos os casos com garantias de não discriminação e com as medidas de segurança previstas no artigo 15.º.

3 — O tratamento dos dados referidos no n.º 1 é ainda permitido quando se verificar uma das seguintes condições:

a) Ser necessário para proteger interesses vitais do titular dos dados ou de uma outra pessoa e o titular dos dados estiver física ou legalmente incapaz de dar o seu consentimento;

b) Ser efectuado, com o consentimento do titular, por fundação, associação ou organismo sem fins lucrativos de carácter político, filosófico, religioso ou sindical, no âmbito das suas actividades legítimas, sob condição de o tratamento respeitar apenas aos membros desse organismo ou às pessoas que com ele mantenham contactos periódicos ligados às suas finalidades, e de os dados não serem comunicados a terceiros sem consentimento dos seus titulares;

c) Dizer respeito a dados manifestamente tornados públicos pelo seu titular, desde que se possa legitimamente deduzir das suas declarações o consentimento para o tratamento dos mesmos;

d) Ser necessário à declaração, exercício ou defesa de um direito em processo judicial e for efectuado exclusivamente com essa finalidade.

4 — O tratamento dos dados referentes à saúde e à vida sexual, incluindo os dados genéticos, é permitido quando for necessário para efeitos de medicina preventiva de diagnóstico médico, de prestação de cuidados ou tratamentos médicos ou de gestão de serviços de saúde, desde que o tratamento desses dados seja efectuado por um profissional de saúde obrigado a sigilo ou por outra pessoa sujeita igualmente a segredo profissional, seja notificado à CNPD, nos termos do artigo 27.º, e sejam garantidas medidas adequadas de segurança da informação.”

➤ **Código Penal** ⁽⁶⁵⁾

Artigo 194.º

Violação de correspondência ou de telecomunicações

“1 - Quem, sem consentimento, abrir encomenda, carta ou qualquer outro escrito que se encontre fechado e lhe não seja dirigido, ou tomar conhecimento, por processos técnicos, do seu conteúdo, ou impedir, por qualquer modo, que seja recebido pelo destinatário, é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias.

2 - Na mesma pena incorre quem, sem consentimento, se intrometer no conteúdo de telecomunicação ou dele tomar conhecimento.

3 - Quem, sem consentimento, divulgar o conteúdo de cartas, encomendas, escritos fechados, ou telecomunicações a que se referem os números anteriores, é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias.”

➤ **Código de Processo Penal** ⁽⁶⁶⁾

O artigo 189.º deste Código remete para o disposto nos artigos 187.º e 188.º do mesmo diploma, os quais se referem à admissibilidade de interceptação e a gravação de conversações ou comunicações telefónicas. Vejamos:

Artigo 189.º

Extensão

“1 - O disposto nos artigos 187.º e 188.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à interceptação das comunicações entre presentes.

⁽⁶⁵⁾ Aprovado pelo Decreto-Lei nº 400/82, de 23 de Setembro.

⁽⁶⁶⁾ Aprovado pelo Decreto-Lei nº 78/87, de 17 de Fevereiro.

2 - A obtenção e junção aos autos de dados sobre a localização celular ou de registos da realização de conversações ou comunicações só podem ser ordenadas ou autorizadas, em qualquer fase do processo, por despacho do juiz, quanto a crimes previstos no n.º 1 do artigo 187.º e em relação às pessoas referidas no n.º 4 do mesmo artigo.”

Artigo 126.º

Métodos proibidos de prova

“3 - Ressalvados os casos previstos na lei, são igualmente nulas, não podendo ser utilizadas, as provas obtidas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações sem o consentimento do respectivo titular.”

ANEXO II

“PRINCÍPIOS SOBRE A PRIVACIDADE NO LOCAL DE TRABALHO” – Comissão Nacional de Protecção de Dados (CNPd)

- “A entidade empregadora que permite a utilização do *e-mail* para fins privados e que não põe limitações à utilização da Internet, que não pretende estabelecer limites à utilização e, em consequência, se recusa a efectuar qualquer tipo de controlo dos trabalhadores está dispensada de notificar aqueles «registos de comunicações» (tratamentos) à CNPD”.

Na utilização do *e-mail*:

- “O facto de a entidade empregadora proibir a utilização do *e-mail* para fins privados não lhe dá o direito de abrir, automaticamente, o *e-mail* dirigido ao trabalhador.”

- “Os poderes de controlo da entidade empregadora – que não podem ser postos em causa – devem ser compatibilizados com os direitos dos trabalhadores, assegurando-se que devem ser evitadas intrusões. A entidade empregadora deve, por isso, escolher metodologias de controlo não intrusivas, que estejam de acordo com os princípios previamente definidos e que sejam do conhecimento dos trabalhadores”.

- “A entidade empregadora não deve fazer um controlo permanente e sistemático do *e-mail* dos trabalhadores. O controlo deve ser pontual e direccionado para as áreas e actividades que apresentem um maior “risco” para a empresa”.

- “O acesso ao *e-mail* deverá ser o último recurso a utilizar pela entidade empregadora, sendo desejável que esse acesso seja feito na presença do trabalhador visado e, de preferência, na presença de um representante da Comissão de Trabalhadores. O 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 alguns *e-mails* de natureza privada e que não pretende que sejam lidos pela entidade empregadora”.

- “Perante tal situação a entidade empregadora deve abster-se de consultar o conteúdo do *e-mail*, em face da oposição do trabalhador”.

Na utilização da Internet:

- “A entidade empregadora deve assegurar-se que os trabalhadores estão claramente informados e que estão conscientes dos limites estabelecidos em relação à utilização de Internet para fins privados e que conhecem as formas de controlo que podem ser adoptadas.”

- “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 forma não individualizada, e global, em relação a todos os acessos na empresa, com referência ao tempo de conexão na empresa”.
- “A realização de estudos estatísticos pode ser suficiente para a entidade empregadora se poder 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 que seja feito um tratamento dos sítios mais consultados na empresa, sem identificação dos postos de trabalho”.
- “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.”

ADENDA

DELIBERAÇÃO N.º 1638/2013, de 16 de Julho – Comissão Nacional de Protecção de Dados (CNPD)

A CNPD aprovou, na sua sessão plenária de 16 de Julho de 2013, esta Deliberação, cujo texto foi divulgado no dia 14 de Novembro, e que veio rever a Deliberação que aquela Comissão havia emitido em 29 de Outubro de 2002 sobre a mesma matéria.

Não obstante esta Deliberação não ser vinculativa para os responsáveis pelo tratamento de dados pessoais, a CNPD seguirá as suas próprias orientações nas suas decisões de aprovação de um determinado tratamento, pelo que é de atentar aos aspectos mais relevantes da mesma.

A CNPD esclarece que o n.º 2 do artigo 22.º do Código do Trabalho não atribui às entidades empregadoras o poder de controlo sobre as comunicações que o trabalhador efectue através das contas (de correio electrónico, redes sociais ou qualquer outro tipo) que aderiu a título pessoal, ainda que acedidas através do computador da empresa.

ACNPD afirma que o controlo da utilização para fins privados das tecnologias de informação e comunicação no contexto laboral resulta num verdadeiro tratamento de dados. Pelo que, deverá visar finalidades determinadas, explícitas e legítimas que, no contexto laboral, podem consistir na gestão dos meios da empresa e da produtividade dos trabalhadores.

Refere a CNPD que não devem ocorrer controlos individualizados dos dados de tráfego associados às comunicações dos trabalhadores, sendo suficiente a tratamento de alguns dados, tais como a hora e a duração da comunicação. A entidade empregadora deve, pois, privilegiar metodologias genéricas de controlo, aplicadas ao universo global dos trabalhadores (v.g. número de mensagens enviadas e tipo de ficheiros em anexo, tempo gasto em consultas na Internet).

Consta novidade desta deliberação a especificação de um prazo de conservação dos dados obtidos no contexto deste tipo de tratamento, o qual não deverá ultrapassar 6 meses, sem prejuízo da sua possível manutenção no decurso de processo disciplinar ou judicial.

A CNPD entende que o fundamento para o tratamento dos dados pessoais dos trabalhadores resultantes da sua utilização dos sistemas de informação do empregador para fins pessoais é a lei, concretamente os artigos 22.º, n.º 2 e 97.º do Código do Trabalho.

A CNPD entende que os objectivos das entidades empregadoras poderão ser alcançados sem necessidade de recurso a interconexões, consideradas desproporcionais. Assim, o tratamento de dados não deve ser sujeito a interconexões com outros tratamentos de dados da responsabilidade da entidade empregadora (como, por exemplo, as bases de dados de recursos humanos) ou de terceiros.

Como novidade, a CNPD estabelece a necessidade de a entidade empregadora avaliar previamente o impacto das medidas de controlo que pretende implementar (ou “Privacy Impact Assessment”, como a própria CNPD refere) na privacidade dos trabalhadores e, em função disso, encontrar aquelas que sejam menos intrusivas para esta, e que simultaneamente satisfaçam os legítimos objectivos da organização.

Ainda como novidade, e quanto a medidas de segurança, a CNPD assinala que os responsáveis pelo tratamento estão obrigados a implementar uma política de análise de *logs*, com a realização de relatórios periódicos, que devem ser mantidos para efeitos de fiscalização pela CNPD. As medidas adoptadas pela entidade empregadora devem impedir o acesso à informação por pessoas não autorizadas, estabelecendo-se um perfil de acesso específico para as finalidades aqui em análise. 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. 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, respectiva data e hora (*timestamp*), operações efectuadas atribuindo um número sequencial a cada ocorrência e um campo de *hash* aplicado sobre os elementos anteriores (id, utilizador, data, hora e operação). Os *logs* terão de ser assinados digitalmente e apenas poderão ser conservados durante um ano. O responsável deve identificar um conjunto de situações consideradas anómalas de forma a poder desenvolver um sistema de alarmes que permita identificar utilizações indevidas do sistema.

No que respeita ao controlo de correio electrónico e de dados de tráfego, determina, também, a CNPD que a entidade empregadora deve exigir aos trabalhadores a criação de pastas próprias onde devem arquivar os correios electrónicos de conteúdo pessoal que constam da caixa de correio profissional.

Também o segredo profissional que impenda sobre o empregado deve ser preservado (v.g. sigilo médico, sigilo profissional de advogado, segredo das fontes de jornalistas), não devendo o conteúdo das suas mensagens ser acedido em circunstância alguma nem os dados de tráfego reveladores dos remetentes ou destinatários exteriores ser objecto de tratamento para fins de controlo.

Os eventuais controlos fundamentados na prevenção ou detecção da divulgação de segredos comerciais devem ser direccionados, exclusivamente, para as pessoas que têm acesso a esses segredos e apenas quando existam fundadas suspeitas daquele facto. A preservação de segredo comercial, industrial ou de propriedade intelectual deve ser realizada no âmbito de uma filosofia preventiva, adoptando as entidades empregadoras mecanismos estritos de controlo de acesso à informação sigilosa, minimizando deste modo eventuais riscos de divulgação indevida.

É de ter em consideração que a entrada de correspondência na caixa de correio electrónico do trabalhador é independente da sua vontade, pelo que devem ser dadas instruções ao mesmo para que apague as mensagens eventualmente recebidas que contrariem o Regulamento Interno.

A CNPD reforça o entendimento de que o acesso à conta de correio electrónico do trabalhador deve ser limitado à visualização dos endereços dos destinatários, assunto, data e hora de envio, sendo que o mero registo de envio cumpre o objectivo do tratamento, devendo, pois, a entidade empregadora abster-se de consultar o conteúdo das mensagens.

São determinadas regras para casos de ausência prolongada ou cessação do contrato de trabalho. Assim, no caso de ausência do trabalhador, deve ser adoptado um mecanismo de resposta automática (*out of office reply*), com indicação do endereço alternativo. As razões para aceder à caixa postal do trabalhador ausente devem ser claramente explicitadas e comunicadas ao mesmo no Regulamento Interno, bem como deve o mesmo acesso ser

realizado na presença de um representante da comissão de trabalhadores ou de outra pessoa indicada pelo trabalhador visado.

No caso de cessação de contrato de trabalho, deve ser concedido ao trabalhador um prazo para retirar o conteúdo de cariz pessoal arquivado no correio electrónico, devendo posteriormente eliminar a respectiva conta. O empregador deve assegurar que o mesmo endereço electrónico não será posteriormente atribuído a outro trabalhador.

Quanto ao controlo da navegação na Internet, o empregador deve garantir que, através do Regulamento Interno, os trabalhadores estão devidamente informados relativamente aos limites de utilização da Internet para fins privados. E afirma a CNPD que se deve admitir um certo grau de tolerância em relação ao acesso à Internet, nomeadamente se tal ocorrer fora do horário de trabalho.

Recomenda a CNPD, no âmbito de uma filosofia preventiva, a utilização de filtros que impossibilitem a visita de certos *sites* não autorizados pelo empregador, ou a delimitação de períodos em que é autorizada a utilização da Internet em detrimento de métodos de controlo dos *sites* visualizados pelos trabalhadores.

Sublinha a CNPD que o controlo em relação ao tempo de acesso diário e aos sítios consultados por cada trabalhador só deverá ser realizado em circunstâncias excepcionais, designadamente por iniciativa do trabalhador (quando puser em causa as indicações do empregador e quiser conferir a realização de tais acessos, por exemplo para verificar as horas de conexão – início e fim – para comprovar que o acesso para fins privados ocorreu fora do horário de trabalho).

A CPD considera que, mesmo que o trabalhador utilize a Internet no local de trabalho, em condições não permitidas pelo Regulamento Interno da Empresa, o acesso pelo empregador ao perfil pessoal daquele em redes sociais é proibido.

Relativamente ao acesso remoto ao computador do trabalhador, estabelece a CNPD a proibição de utilização, pelo empregador, de sistemas que permitam visualizar, seguir ou monitorizar as acções efectuadas no computador, sem o seu conhecimento, assim como procurar ou extrair a informação armazenada. Pelo que, as ferramentas que permitam a existência de ambientes de trabalho remotos ou a partilha de ambiente gráfico, que permitem acompanhar as acções e operações que o trabalhador leva a cabo no computador, seja em

tempo real, seja em tempo diferido através da gravação daquelas operações, 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.

De igual modo, são proibidos sistemas que permitam, nos computadores da organização, a pesquisa e localização de documentos de forma automática e remota, por exemplo através da utilização de palavras-chave.

Os possíveis procedimentos de realização de cópias de segurança da informação, contida nos computadores individuais, ou de centralização em arquivo geral de documentação profissional dispersa, devem garantir que não é acedida e copiada informação de natureza privada (sendo necessário que tais procedimentos prevejam uma separação inequívoca de pastas pessoais e profissionais, bem como uma orientação prática quanto à forma correcta de arquivar eventuais documentos privados).

Nota: Este trabalho não obedece às regras do novo Acordo Ortográfico, por opção.