Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente.***

CYBERLAW by CIJIC

EDIÇÃO N.º IX – MARÇO DE 2020

REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

EDITOR: NUNO TEIXEIRA CASTRO

SUPORTE EDITORIAL: EUGÉNIO ALVES DA SILVA e AFONSO FREITAS DANTAS

PRESIDENTE DO CIJIC: EDUARDO VERA-CRUZ PINTO

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

NOTAS DO EDITOR:

Globalização. Tecnologia e Inteligência artificial. Mobilidade organizacional e individual. Manipulação. A pandemia de Coronavírus. Hoje. O futuro.

Vivemos tempos "*estranhos*". Acutilantes. Irresolutos. Contingentes. Exigentes. O "tema" que nos capta, quase em exclusivo, a atenção, desde o início do ano de 2020, é a pandemia de coronavírus. Aquela dinâmica, rotineira, até agora tida como "garantida" atravessa momentos de grande indeterminação. Hora a hora somos como que bombardeados com números esmagadores: de taxas mundiais galopantes de infectados, doentes em cuidados intensivos, de mortos. No passar deste tempo, diariamente, deambulámos entre um imoderado e célere na disseminação da infecção *versus* um vagaroso e fleumático passo na demonstração de resultados animadores no seu combate. O racional económico de «custo-benefício» geralmente revelaria a perigosidade associada à extrema cautela. Porém na questão, truncada, do coronavírus é diferente[1]. "*Achatar as curvas*", "*Proteger os mais idosos e os mais vulneráveis*", "*Suster a vaga de procura do SNS por forma a dar-lhe tempo para acudir às solicitações*", mesmo que o custo seja o parar da Economia. Global. Entretanto o tempo continua o seu passo. Assim como a epidemia há-de passar.

1 Cass Sunstein @ https://www.bloomberg.com/opinion/articles/2020-03-26/coronavirus-lockdowns-look-smart-under-cost-benefit-scrutiny

E, quando aí chegados, a questão resolutiva a colocar não deverá andar muito longe de um: "*Que mundo esperar do pós-covid19*"?

O avanço da tecnologia, combinando melhores recursos de *hardware* com inteligência artificial, aos quais o Homem socorre, permitiram sequenciar o genoma do COVID-19 em menos de um mês. A inteligência artificial, por exemplo, num contexto, global, de recursos exíguos tem sido testada para suprir lacunas críticas nos recursos de saúde, ajudando à racionalidade da decisão política, alavancando centros de inovação em inteligência artificial, robótica e automação em saúde. Na Ásia[2]. Por agora.

O mesmo avanço tecnológico, por sua vez, no actual cenário de "*guerra*" ao vírus, colocou a ponderação das liberdades fundamentais num estádio de confronto titânico. Recuperando o "*achatar a curva*", um pouco por todo o mundo, os governos, democráticos, colocaram os respectivos países em *lockdown*. Sem cautelas. Entre confinamentos e quarentenas obrigatórias, um recurso parece permitir - em face da falta de meios humanos para controlo efectivo de milhões de cidadãos - fiscalizar o cumprimento das directrizes estatais. A tentação executiva por esse controlo, universal, dos cidadãos preclude a fruição de múltiplas liberdades constitucionalmente consagradas. O racional da discussão que vinha sendo tido até agora[3], deslocou-se, por via do perigo abstracto que a pandemia comporta, da questão securitária *versus* liberdades fundamentais para "*saúde pública*" *versus* liberdades fundamentais.

Um pouco por todo o ocidente democrático, a tónica recursiva tem passado pelo uso da "*vigilância digital* estadual[4]". Tal como um pouco por todo o mundo, direitos humanos fundamentais[5] são colocados em teste face à imposição destas regras "excepcionais". O Estado de emergência tende a permitir, justificando múltiplas

---

2 Eficiência, especialidade, racionalidade, sistemas capacitativos e colaborativos público-privados. O trabalho dos dados ao serviço dos povos. https://www.technologyreview.com/s/614555/ai-in-health-care-capacity-capability-and-a-future-of-active-health-in-asia/

3 « Tribunal Constitucional chumba acesso das secretas a registos de comunicações», @ https://rr.sapo.pt/2019/09/19/politica/tribunal-constitucional-chumba-acesso-das-secretas-a-registos-de-comunicacoes/noticia/165164/

4 Por exemplo: https://www.wsj.com/articles/europe-tracks-residents-phones-for-coronavirus-research-11585301401

5 Por exemplo, no contexto da América do Sul, «Sociedade civil pede que tecnologias usadas devido à pandemia respeitem os Direitos Humanos», @ https://idec.org.br/noticia/sociedade-civil-pede-governos-da-america-latina-e-caribe-que-tecnologias-digitais-aplicadas

intrusões como *adequadas*[6], *necessárias e proporcionais*[7]. A questão, sendo excepcional e de carácter limitada no tempo, deveria ser pacificamente tolerada pelos cidadãos. Afinal, sob o manto de um fundamento como o "*interesse público*" [8] e salvaguarda da "*saúde pública*" até a limitação do escopo de protecção, desde logo, da privacidade de dados pessoais sensíveis claudica[9].

---

6 No parecer 32/2020, a CNPD, delimitando geograficamente a aplicação de videovigilância por drones ao concelho de Ovar, dada a excepcionalidade da cerca sanitária entretanto imposta, reitera que "(…)as restrições aos direitos fundamentais devem limitar-se ao estritamente necessário às finalidades visadas com este sistema de videovigilância ", recomendando, adicionalmente, "que se garanta que a captação de imagens assim realizada salvaguarde a privacidade daqueles que se encontrem nas respectivas habitações", e, "que se garanta o direito de acesso às imagens gravadas , nos termos legalmente previstos", bem como que se adoptem "medidas adequadas a garantir a integridade das imagens gravadas no processo de transferência dos registos(…) para o "contentor de informação encriptado"" . @ https://www.cnpd.pt/home/decisoes/Par/PAR_2020_32.pdf

7 Por exemplo, em Espanha, a AEPD: «(…)*Los fundamentos que legitiman/hacen posible dichos tratamientos son la necesidad de atender las misiones realizadas en interés público, así como la de garantizar los intereses vitales de los propios afectados o de terceras personas.* ***Las finalidades para las que pueden tratarse los datos son, únicamente, las relacionadas con el control de la epidemia****, entre ellas, las de ofrecer información sobre el uso de las aplicaciones de autoevaluación realizadas por las administraciones públicas o la obtención de estadísticas con datos de geolocalización agregados para ofrecer mapas que informen sobre áreas de mayor o menor riesgo.* ***Los datos que pueden obtenerse y utilizarse han de ser los que las autoridades públicas competentes consideren proporcionados/necesarios para cumplir con dichas finalidades.*** *Estos datos sólo podrán ser facilitados por quienes sean mayores de 16 años. En el caso de tratar datos de menores de 16 años, se requeriría de la autorización de sus padres o representantes legales.* ***Únicamente podrán tratar dichos datos las autoridades públicas competentes para actuar conforme a la declaración del estado de alarma****, es decir, el Ministerio de Sanidad y las Consejerías de Sanidad de las Comunidades Autónomas, que podrán cederse datos entre ellas, y a los profesionales sanitarios que traten a los pacientes o que intervengan en el control de la epidemia.****Las entidades privadas que colaboren con dichas autoridades sólo podrán utilizar los datos conforme a las instrucciones de estas y, en ningún caso, para fines distintos de los autorizados.»*** @ https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-apps-webs-autoevaluacion-coronavirus-privacidad

8 A limitação ao tratamento de dados sensíveis, por exemplo, de saúde sucumbe ante "*razões de interesse público nos domínios da saúde pública*", desde que «(…)***Tais atividades de tratamento de dados sobre a saúde autorizadas por motivos de interesse público não deverão ter por resultado que os dados sejam tratados para outros fins por terceiros, como os empregadores ou as companhias de seguros e entidades bancárias»*** (Considerando 54 in fine) .

Considerando *(54) « O tratamento de categorias especiais de dados pessoais pode ser necessário por razões de interesse público nos domínios da saúde pública, sem o consentimento do titular dos dados. Esse tratamento deverá ser objeto de medidas adequadas e específicas, a fim de defender os direitos e liberdades das pessoas singulares. Neste contexto, a noção de «saúde pública» deverá ser interpretada segundo a definição constante do Regulamento (CE) n.o 1338/2008 do Parlamento Europeu e do Conselho (11), ou seja, todos os elementos relacionados com a saúde, a saber, o estado de saúde, incluindo a morbilidade e a incapacidade, as determinantes desse estado de saúde, as necessidades de cuidados de saúde, os recursos atribuídos aos cuidados de saúde, a prestação de cuidados de saúde e o acesso universal aos mesmos, assim como as despesas e o financiamento dos cuidados de saúde, e as causas de mortalidade(…)****».***

9 Confirmando o Considerando (54), ainda, da leitura conjunta **das alíneas g) e i) do Art.o 9, n.º2, RGPD**: «**G)** *Se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados*;», e**, i)** « *Se o tratamento for* ***necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde*** *ou para assegurar um elevado nível de qualidade e de*

Mas há um "*senão*". O receio de que a excepcionalidade vire regra é real[10]. Com efeito, é inegável que, neste momento, os receios de Yuval Harari [11], criador de *Homo Deus*, sejam partilhados por muitos de nós. Tal como as considerações de Joel P. Trachtman, quanto aos benefícios de um mundo global[12]: benéfico se mais cooperativo, com capacidades regulatórias internacionais reforçadas ao nível da saúde, cibersegurança, proteção ambiental e crises financeiras.

Ambos convergem na necessidade de compromisso, de partilha, cooperação e solidariedade global. O que se conclui espontaneamente dos apontamentos citados, através de um silogismo categórico: ameaça sobre todos os países, ameaça global, logo, resposta de todos os países, global. Não obstante, será que hoje temos líderes políticos mundiais à altura dos desafios[13] pungentes que se nos colocam nestes termos?

E no futuro?

---

segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional;». @ https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

10 Yuval Harari:«(…) *Many short-term emergency measures will become a fixture of life. That is the nature of emergencies. They fast-forward historical processes. Decisions that in normal times could take years of deliberation are passed in a matter of hours. Immature and even dangerous technologies are pressed into service, because the risks of doing nothing are bigger.", @* https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

11 Harari: «(…) *In this moment of crisis, the crucial struggle takes place within humanity itself. If this epidemic results in greater disunity and mistrust among humans, it will be the virus's greatest victory. When humans squabble – viruses double. In contrast, if the epidemic results in closer global cooperation, it will be a victory not only against the coronavirus, but against all future pathogens*.», @ https://time.com/5803225/yuval-noah-harari-coronavirus-humanity-leadership/

12 Joel P. Trachtman, «(…) *Not all global problems result from globalization. For those that do, globalization itself can ameliorate them to some extent. Furthermore, we can establish international laws and institutions to minimize those problems that do arise from globalization: globalized governance to respond to globalization-induced problems. This is smart globalization, and once we do it this way, it is likely that globalization should be retained because, on net, it will make us better off*.", @ https://www.bostonglobe.com/2020/03/30/opinion/not-all-global-problems-result-globalization/

13 Ainda Harari: «(…)*Today humanity faces an acute crisis not only due to the coronavirus, but also due to the lack of trust between humans. To defeat an epidemic, people need to trust scientific experts, citizens need to trust public authorities, and countries need to trust each other. Over the last few years, irresponsible politicians have deliberately undermined trust in science, in public authorities and in international cooperation. As a result, we are now facing this crisis bereft of global leaders that can inspire, organize and finance a coordinated global response*.», *idem*.

Gerd Leonhard, num exercício curioso reproduzido no Diário de Notícias, destaca dois aspectos cruciais. Circunscrevendo-nos à tecnologia, esta *"tornou-se a nova religião"*. "*Estamos a entrar num novo Renascimento*". *O próximo passo será regulamentá-la de forma mais apertada com o objetivo de que humanos e o próprio planeta beneficiem do progresso tecnológico.* Não obstante, esta relação acabará seduzir-se ante uma *vigilância estatal por meios tecnológicos* (que) *irá tornar-se o novo normal após as medidas extraordinárias que foram tomadas para controlar esta pandemia*[14].

E como já vai longo, para concluir, convocamos, novamente, a questão fundamental: "*Que mundo esperar do pós-covid19*"?

A provocação desconcertante e acutilante que se impõe, inclusive politicamente, não poderia ser outra: «*Of course, even if we disappear, it will not be the end of the world. Something will survive us. Perhaps the rats will eventually take over and rebuild civilization. Perhaps, then, the rats will learn from our mistakes. But I very much hope we can rely on the leaders assembled here, and not on the rats.*» [15]

Nesta nova edição da «Cyberlaw by CIJIC», procuramos sustentar o crescimento paralelo que o Mestrado de Segurança da Informação e Direito do Ciberespaço[16] vai granjeando. É pois, com orgulho, que passaremos a destacar produção deste, com maior regularidade. Afinal, este é um desígnio da própria criação da revista. Provavelmente, num futuro não muito distante, estará na calha a edição em papel de futuras edições. Se há questão que se nos colocou com o teletrabalho foi: qual a redundância digital? *Ie*, sem acesso à internet, ou sem eletricidade/bateria, como é que seria possível aceder

14 «Não haverá normal: futuristas preveem mudanças permanentes pós-coronavírus», @ https://www.dn.pt/dinheiro/nao-havera-normal-futuristas-preveem-mudancas-permanentes-pos-coronavirus-11987179.html
15 Yuval Harari: «Yuval Harari's blistering warning to Davos», @ https://www.weforum.org/agenda/2020/01/yuval-hararis-warning-davos-speech-future-predications/
16 Mais informações @ : https://fenix.tecnico.ulisboa.pt/cursos/msidc

a conteúdos para efeitos de estudo? Como ler(aceder) nestas circunstâncias? Como mitigar a "info-exclusão" quando o sistema não é propriamente redundante na acessibilidade[17]?

Reavendo, nesta edição, incorporando conteúdo em inglês escrito, por força de deveres de participação, cooperação e colaboração internacional[18] que muito nos orgulha, procuramos revisitar temas como cibersegurança em contexto marítimo, dados pessoais e dados não pessoais, monitorização de trabalhadores em contexto laboral, a regulação jurídica do ciberespaço - mutação do paradigma à luz do acórdão James Elliot, *Phishing*, redes sociais e manipulação da opinião pública, o problema da mobilidade em contexto organizacional, e, os desafios da cibersegurança forense de *smartphones* no continente africano. Os temas são oportunos. São, igualmente, desafiantes. São, finalmente, abertos a colaboração múltipla, participada.

Resta-me agradecer a todos quantos contribuíram para mais uma edição da Revista, pelo esforço, pela disponibilidade, pela obra, endereçando a todos, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um justíssimo: - Muito Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

Boas leituras.

Lisboa, FDUL, 29 de Março de 2020

Nuno Teixeira Castro

17 Por exemplo, «Ministro Siza Vieira admite aulas por canais "estilo youtube" ou TV por cabo.», @ https://observador.pt/2020/03/29/ministro-siza-vieira-admite-aulas-por-canais-estilo-youtube-ou-tv-por-cabo/
Mas, sem acesso internet, ou sem cabo – até porque a cobertura não é de 100%, há, pelo menos, cerca de 20% de famílias sem acesso ao Cabo – como é que as crianças e adolescentes que se encontrem nesta situação se integram? Como é que se combate esta exclusão digital?
18 Um trabalho colaborativo ímpar. @ https://networkofcenters.net/center/cyberlaw-research-centre-university-lisbon-school-law-cijic

CYBERLAW

by CIJIC

DOUTRINA

PODEM AS EMPRESAS REALIZAR A MONITORIZAÇÃO DE SEUS TRABALHADORES ATRAVÉS DE FERRAMENTAS DE SEGURANÇA DA INFORMAÇÃO, SEM VIOLAR O RGPD?

MÁRCIO COTS [1]

e

ANDRESA CRUZ [2]

1 Advogado português, especializado em Cyberlaw e Direito dos Negócios Digitais, sendo também membro do escritório norte-americano CyberlawStudio PLLC.Professor universitário.Mestre em Direito pela FADISP, especialista em Cyberlaw pela Harvard Law School – EUA, com extensão universitária em Direito da Tecnologia da Informação, pela FGV/EPGE.Membro do Harvard Faculty Club.Advogados.

2 Formada em Direito, atuando como advogada no Brasil e em Portugal em parceria com a COTS Advogados. Éspecialista em Direito Informático, presta consultoria em Proteção de Dados, privacidade e adequação jurídica para as novas tecnologias, além da área contenciosa.Co-autora de obra "O Legítimo Interesse e a LGPDP"

Participante de diversos congressos e eventos com foco em Privacidade, Proteção de Dados, Inteligência Artificial e o Direito 4.0.

RESUMO

Uma das preocupações das empresas na era da informação é a possibilidade do vazamento dos dados, portanto, o investimento em segurança da informação torna-se necessário.

Neste contexto, há como realizar a monitorização de seus trabalhadores a fim de evitar tais vazamentos sem que o direito à reserva da intimidade da vida privada, direito consagrado na Constituição da República Portuguesa, em seu artigo 26º, seja violado? E, ainda, manter os dados pessoais de seus trabalhadores protegidos?

Palavras-chave: Proteção de dados pessoais; Regulamento Geral Proteção Dados; empregador e trabalhador; tecnologia; monitorização.

"Interpretar as normas constitucionais significa (como toda a interpretação de normas jurídicas) compreender, investigar e mediatizar o conteúdo semântico dos enunciados linguísticos que formam o texto constitucional. A interpretação jurídica constitucional reconduz-se, pois, à atribuição de um significado a um ou vários símbolos linguísticos escritos na constituição".

(CANOTILHO, J. J. Gomes)

Uma das preocupações das empresas na era da informação é a possibilidade do vazamento dos dados, portanto, o investimento em segurança da informação torna-se necessário.

Neste contexto, há como realizar a monitorização de seus trabalhadores a fim de evitar tais vazamentos sem que o direito à reserva da intimidade da vida privada, direito consagrado na Constituição da República Portuguesa, em seu artigo 26º, seja violado? E, ainda, manter os dados pessoais de seus trabalhadores protegidos?

O artigo 20º, nº1 do Código do trabalho, prescreve que:

"*O empregador não pode utilizar meios de vigilância a distância no local de trabalho, mediante o emprego de equipamento tecnológico, com a finalidade de controlar o desempenho profissional do trabalhador*".

Já no nº2 do mesmo artigo:

"*A utilização de equipamento referido no número anterior é lícita sempre que tenha por finalidade a protecção*

e segurança de pessoas e bens ou quando particulares exigências inerentes à natureza da actividade o justifiquem".

Ou seja, há sim formas válidas de monitorização dos funcionários, a questão em si é, quais serão as finalidades e limites para o fazê-lo.

> *"Apesar de o artº 20º, nº 1 do Código do Trabalho proibir a utilização de meios de vigilância distância para controlar de forma dedicada e permanente o desempenho profissional do trabalhador,* ***esta utilização é lícita se cumprir os requisitos de fim e publicidade previstos*** *nos nºs 2 e 3 do mesmo artº 20º e* conforme manifestado pela *Comissão Nacional de Protecção de Dados.* ***Neste último caso, os dados obtidos podem servir de meio de prova em procedimento disciplinar e no controlo jurisdicional da licitude da decisão disciplinar****."*[1]

Publicado pelo grupo de trabalho do artigo 29 para Proteção de Dados, em seu parecer 2/2017[2] sobre o tratamento de dados no local de trabalho, e que reafirma também a posição e as conclusões do Parecer 8/2001[3], bem como do documento de trabalho GT55[4], aquando do tratamento dos dados pessoais dos empregados:

- os empregadores devem ter sempre em conta os princípios fundamentais da proteção de dados, independentemente da tecnologia utilizada;

- o conteúdo das comunicações eletrónicas feitas a partir de um estabelecimento comercial goza da mesma proteção dos direitos fundamentais que a das comunicações análogas;

1 *Ac. TRC, de 02.06.2016*
2 Parecer 2/2017 sobre o tratamento de dados no local de trabalho
3 GT 29, Parecer 8/2001 sobre o tratamento de dados pessoais no contexto laboral, GT 48, 13 de setembro de 2001, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf
4 GT 29, documento de trabalho sobre a vigilância das comunicações eletrónicas no local de trabalho, GT 55, 29 de maio de 2002, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_pt.pdf

- é muito improvável que o consentimento possa constituir uma base jurídica para o tratamento de dados no local de trabalho, a menos que os empregados possam recusar, sem consequências adversas;

- a execução de um contrato e o interesse legítimo podem, por vezes, ser invocados, desde que o tratamento seja estritamente necessário para uma finalidade legítima e respeite os princípios da proporcionalidade e da subsidiariedade;

- **os empregados devem receber informações eficazes sobre a realização da monitorização**; e

- qualquer transferência internacional de dados dos empregados apenas deve ser realizada nos casos em que seja garantido um nível de proteção adequado.

Pela própria natureza das atividades relacionadas a monitorização de dados pessoais, ressalta-se a obrigatoriedade de uma Avaliação de Impacto sobre a Proteção de Dados - AIPD, sendo este um dos requisitos obrigatórios ao responsável pelo tratamento de dados, e com previsão no RGPD em seu artigo 35º, devendo ser sempre executado quando um certo tipo de tecnologia, principalmente as "novas tecnologias", impliquem num elevado risco para os direitos e liberdades das pessoas singulares, como por exemplo a temática deste artigo, a monitorização de emails, mensagens eletrónicas, e controlos pertinentes do universo corporativo.

Para tal, e em conformidade com o RGPD artigo 88º, nº 2, para que a monitorização seja resguardada e adequada ao regulamento, o exercício de monitorização, deve ser sustentada com medidas adequadas e específicas de segurança, de forma a salvaguardar a dignidade, os interesses legítimos e os direitos fundamentais do titular dos dados, avaliando se:

- a transferência de dados pessoais é realizada num grupo empresarial ou num grupo de empresas envolvidas numa atividade económica conjunta?;

- a atividade de tratamento e monitorização é necessária?

- a proposta do tratamento de dados pessoais e monitorização é equitativa para os empregados?;

- a atividade de monitorização é proporcional às preocupações suscitadas?; e

- existe transparência do tratamento de dados e sistemas de controlo no local de trabalho, para com os empregados?

Alguns exemplos onde a monitorização e tratamento de dados pode ser considerado legítima por parte do empregador:

- Deteção e prevenção de perda ou vazamento de dados pessoais;

- Deteção e prevenção de perda ou roubo de propriedade intelectual ou física de negócios;

- Finalidades estatísticas;

- Controlos de qualidade.

É importante reconhecer que, embora a melhoria da produtividade e desempenho dos funcionários seja um interesse legítimo do empregador, este não pode colocar em causa os direitos fundamentais e a privacidade dos funcionários.

Para além dos direitos dos trabalhadores, deve-se levar em conta os direitos das entidades patronais, a quem se reservam o "**direito de propriedade privada**"[5], bem como o "**poder de direção**"[6], onde compete ao empregador estipular os termos do contrato de trabalho, nos limites das normas que os regem, e, a partir da elaboração do "**regulamento interno**"[7] estipular as regras de comunicação da empresa, as formas de controlo a serem realizadas e as condições dos tratamentos dos dados. "*Mas a escolha dos meios de controlo por parte do empregador tem de obedecer aos princípios da necessidade, da proporcionalidade e da boa-fé, devendo este demonstrar que escolheu as formas de controlo com menor impacto sobre os direitos fundamentais dos trabalhadores*[8]."

5 Constituição da República Portuguesa, artigo 62º.
6 Código do Trabalho, artigo 97º.
7 Código do Trabalho, artigo 99º.
8 Deliberação n.º 1638/2013 CNPD.

Também parte obrigatória do Regulamento Interno, a monitorização através de ferramentas e aplicativos conhecidos popularmente pelo termo "Redes Sociais", só é permitido quando:

- O perfil na rede social está diretamente relacionada a fins profissionais;

- Em processo de recrutamento e seleção, o perfil do candidato possuir informações sobre habilidades ou características altamente relevantes para o trabalho oferecido.

A título exemplificativo de uma monitorização em "redes sociais, o Tribunal de Matosinhos, declara justa causa em despedimento por ofensas dirigidas ao empregador no Facebook.

Aquando do controlo do correio eletronico, as empresas podem realizar a monitorização dos mesmos, desde que tenham regras bem delineadas e publicitadas (artigo 99º, nº3, Código do Trabalho).

Em alusão ao tema supra mencionado há uma referência histórica onde o "Tribunal dos Direitos do Homem, dá razão a juiz português[9] sobre a privacidade no trabalho em ação que remonta a 10 anos, onde este teve seu voto vencido. Afinal, e ao contrário do que tinha sido decidido anteriormente, as empresas só podem aceder aos e-mails dos seus trabalhadores depois de os avisarem. Trata-se de um marco importante na evolução do direito sobre privacidade no trabalho. O caso diz respeito à Bogdan Barbulescu[10], um engenheiro informático romeno que foi despedido em 2007 por ter usado para comunicações privadas o seu Yahoo!Messenger da empresa. Esta aplicava uma política estrita na matéria, proibindo formalmente os empregados de se servirem do Messenger para quaisquer fins que não fossem profissionais. Barbulescu infringiu a política ao trocar mensagens com o seu irmão e a sua noiva."[11]

9 Juiz Paulo Pinto de Albuquerque
10 O Tribunal Europeu dos Direitos do Homem (TEDH) - http://hudoc.echr.coe.int/eng-press?i=003-5825428-7419362
11 Luís M Faria

Segundo o magistrado português, «uma abordagem ao uso da Internet no local de trabalho centrada nos direitos humanos», com regras claras e transparentes e notificação pessoal da prática da entidade patronal com consentimento explícito dos seus profissionais.

Em Portugal, **os trabalhadores gozam de direito à personalidade, isto é, proteção "contra qualquer ofensa ilícita à sua pessoa física ou moral**", prescrito no Artigo 70.º do Código Civil. Isto posto, a autoridade recorre ao Código do Trabalho e a uma deliberação da Comissão Nacional de Proteção de Dados de forma a estabelecer um enquadramento legal que cubra este direito em contexto de monitorização das comunicações.

Em acordo com o Código do Trabalho no artigo 22.º, **o trabalhador tem direito à reserva e à confidencialidade no que toca a mensagens de cariz pessoal e ao acesso a informação de caráter não profissional via email**. Adverte a ACT, "**tal não prejudica o poder de o empregador estabelecer regras e políticas de utilização dos meios de comunicação na empresa**".

A **Comissão Nacional de Proteção de Dados** emitiu, a 16 de julho de 2013, uma deliberação[12] que **estabelece os limites** dentro dos quais as entidades empregadoras podem proceder a tal vigilância.

> "*Sejam quais forem as regras definidas pela empresa para a utilização do correio eletrónico para fins privados, o empregador não tem o direito de abrir, automaticamente, o correio eletrónico dirigido ao trabalhador*."

12 DELIBERAÇÃO n.º 16 D38/2013 - https://www.cnpd.pt/bin/orientacoes/Delib_controlo_comunic.pdf

As mensagens não perdem o cunho pessoal ou confidencial por ficarem gravadas num servidor detido pela entidade patronal. A deliberação, contudo, **adverte que devem ser criadas pastas próprias dos trabalhadores, devidamente identificadas.**

De fora da monitorização patronal ficam as mensagens relacionadas com segredo e sigilo profissionais:

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

Em caso de **preservação de segredo comercial, a empresa pode proceder a eventuais ações de controlo**. No entanto, estas só podem incidir sobre as pessoas que têm acesso a tais informações sigilosas e quando existe fundamento de possíveis fugas de informações. Neste contexto específico, o acesso ao e-mail deve ser "o último recurso a utilizar pela entidade empregadora", e deve ser feito na presença do trabalhador em questão e, preferencialmente, de um representante da comissão de trabalhadores ou alguém indicado pelo mesmo empregado.

> "*O referido acesso deve limitar-se à visualização dos endereços dos destinatários, o assunto, a data e hora do envio, podendo o trabalhador – se for o caso – especificar a existência de algumas mensagens de natureza privada e que não pretende que sejam lidas pela entidade empregadora."*

Assim, como diz o antigo provérbio "mais vale prevenir, que remediar", cabe a entidade empregadora definir e, muito bem as regras a serem seguidas na empresa, da forma como os ditames legais especificam, publicitá-las e a partir disto monitorizar seus trabalhadores de forma coerente, a fim de resguardar os dados da empresa e os dados pessoais de seus trabalhadores.

O fato é que a privacidade não é o único direito envolvido na questão da relação entre empresas e colaboradores na monitorização dos computadores. Vale ressaltar que, as empresas têm a propriedade da estação de trabalho, do acesso à Internet e do domínio corporativo.

Quem fornece os meios para se trabalhar, também tem seus direitos. Desta feita, é assegurado às empresas o direito à propriedade, pelo artigo 62.º - Direito de propriedade privada - ***1. A todos é garantido o direito à propriedade privada e à sua transmissão em vida ou por morte, nos termos da Constituição***.

No mundo corporativo, a Internet e outros meios eletrónicos de comunicação tornaram-se mais uma ferramenta de trabalho, fornecidas, em certos casos, pela empresa aos seus empregados, que possibilitam agilidade na comunicação.

Sendo esta ferramenta mal utilizada, compromete-se a imagem e segurança da empresa.

No meio jurídico, quando existem questões desta natureza, em que há um conflito de premissas constitucionais a serem aplicadas em um mesmo caso, tenta-se utilizar a proporcionalidade e a razoabilidade, para evitar que um direito constitucional se sobreponha a outro.

Outro ponto polémico é a questão da ***Culpa in eligendo*** (Direito Civil), onde *"há* culpa *in eligendo se dá quando alguém escolhe, para realizar um qualquer acto ou*

actividade, uma pessoa que não tem as necessárias qualidades ou qualificações, quando podia e deveria ter escolhido pessoas diferente. Quando o devedor de uma obrigação faz intervir no cumprimento desta um terceiro que, por falta de aptidões ou de preparação, desencadeia um não cumprimento, é o devedor responsável pelos danos resultantes, fundando-se tal responsabilidade no acto próprio da culposa escolha do substituto ou auxiliar. (...)".[13]

Desta feita, se a empresa tem responsabilidade quanto aos actos praticados por seus funcionários, certamente esta pode, dentro dos parâmetros legais, monitorizar seus actos.

Além do mais, as empresas têm o direito de cuidarem de sua imagem ou marca na internet.

Portanto, caso a empresa, face aos seus direitos constitucionais de propriedade, de imagem e diante de sua responsabilidade ao eleger determinados funcionários para actos de suas responsabilidade, queira monitorizá-los, com ferramentas de segurança da informação, deverá previamente informá-lo de tal monitorização, afim de retirá-lhe a expectativa de privacidade no meio virtual laboral.

13 PRATA, Ana, com colab. CARVALHO, Jorge (2014), Dicionário Jurídico, Vol. I, reimp. da 5ª ed. de jan 2008, Coimbra, Almedina, p. 413.