O papel fundamental da Cibersegurança na Proteção de Dados Pessoais

Diogo Lopes Alves*

Resumo: Constitui o objeto do presente artigo realçar a importância da integração da Cibersegurança na Proteção de Dados Pessoais, tanto de uma perspetiva legislativa, que estabelece a Cibersegurança como imperativo da condição para a *accountability* do RGPD, como da autorregulação, estando ambas dependentes de um grau de maior exigência do que aquele que têm tido. Almeja-se com este texto promover a consciencialização das organizações e das pessoas para a segurança dos seus dados pessoais, de forma a criar uma maior sensibilidade por parte de cada um em relação à segurança dos dados pessoais de que são responsáveis ou de que são titulares. Há, por isso, um longo caminho a percorrer para além das políticas de privacidade e dos acordos de subcontratação das organizações.

Palavras-Chave: *Proteção de Dados Pessoais; Cibersegurança; Ciberataques; Medidas de Segurança; Reporte de Incidente.*

Abstract: The purpose of this article is to highlight the importance of integrating Cybersecurity in Personal Data Protection both from the legal standpoint that establishes Cybersecurity as imperative to the accountability of GDPR, as well as self-regulation, the standards of which are now more demanding than ever before. This article aims to promote greater awareness and sensibility regarding personal data security on the part of organizations and individuals that hold such information. There is a long a road ahead beyond privacy policies and subcontracting agreements.

Keywords: *Personal Data Protection; Cybersecurity; Cyberattacks; Security Measures; Incident Report.*

---

* Advogado, Licenciado em Direito e Mestre em Direito da Empresa e dos Negócios pela Universidade Católica Portuguesa. Exerce funções de Legal & Compliance no Centro de Engenharia e Desenvolvimento (CEIIA). Frequentou a 7ª edição do Curso Breve de Proteção de Dados Pessoais da NOVA School of Law em 2018.

Introdução

A Proteção de Dados Pessoais e a Cibersegurança são dois conceitos indissociáveis na era digital, onde existe um ciberespaço sem demarcações nítidas e com uma débil regulação que traz desafios constantes para os nossos dados pessoais face ao rápido desenvolvimento da tecnologia, às novas ameaças diárias, ao esbatimento das barreiras físicas e à conectividade permanente que amplia a superfície de vulnerabilidade. A frágil, ou inexistente, noção da simbiose entre a Proteção de Dados Pessoais e a Cibersegurança por quem faz o seu tratamento, pode ter origem em vários elementos como, por exemplo: a desconsideração pela privacidade e a falta de formação nessas áreas, combinados com o facto de as pessoas serem o elo mais fraco da cadeia, pelo desconhecimento das tecnologias e dos procedimentos de segurança, pelo excesso de trabalho, pelas funções desajustadas e por atos maliciosos, intrínsecos à natureza humana. Dessa forma, para garantir a proteção dos dados pessoais, é necessário saber quais os perigos que existem no ciberespaço, na maior parte das vezes, desconhecidos de cada um de nós, e reconhecer as fragilidades técnicas e humanas existentes, sendo certo que só através do equilíbrio entre estes dois vetores será possível assegurar a proteção de dados pessoais de uma forma segura e condizente com a realidade atual.

Pese embora a ubiquidade do digital *(Internet of Things, Big Data, Cloud Computing, 5G*, etc.) representar uma vantagem para o desenvolvimento da sociedade, constitui, de igual forma, um fator de risco para os titulares dos dados pessoais que têm perdido o controlo sobre os mesmos, potenciando a redução da sua privacidade. Essa falta de controlo sobre os dados provém, não só, de quem os trata, mas também da condescendência com que são disponibilizados, muito graças à insipiência do seu ciclo de vida e do nível de sensibilidade nesta matéria por parte dos titulares dos dados, que contribui gradualmente para o aumento do risco, trazendo consequências inexoravelmente prejudiciais para a proteção dos dados pessoais. Na realidade, a gratuitidade do digital faz com que, frequentemente, cedamos, facilmente, os nossos dados, tendo apenas como contrapartida o acesso a um serviço. Tratar os dados como contraprestação, ajuda esta monetização dos dados, a hipótese do pagamento de um preço em troca de dados pessoais confere-lhes uma natureza de mercadoria, devendo

ser um caminho a evitar, visto poder não ter retorno. Acresce outro fator de risco que ocorre em contexto laboral decorrente do facto de a fronteira entre a vida profissional e privada ser cada vez mais ténue, seja pelo recurso ao teletrabalho, seja pela informação pessoal e profissional se encontrar num só dispositivo seja, finalmente, pelo uso de dispositivos pessoais no local de trabalho, tudo constituindo fatores potenciadores de riscos de Cibersegurança para os dados pessoais e que os tornam vulneráveis.

O Regulamento Geral de Proteção de Dados (RGPD) teve o condão de ter contribuído para a existência de uma ética no tratamento de dados pessoais através da redistribuição de responsabilidade entre as partes que os tratam com o intuito de assegurar que o titular dos dados tenha o controlo total e o poder de decisão sobre os mesmos.

A privacidade e a proteção de dados pessoais deixaram de ser conceitos etéreos e a violação das mesmas começaram a ter implicações financeiras[1] por não serem respeitadas. Porém, não nos podemos ater a essa premissa simplista pois uma organização pode sofrer consequências bem mais gravosas, quando é alvo de um Ciberataque, nomeadamente, ao nível reputacional, e traduzir-se em implicações diretas nos titulares dos dados pessoais. No seio de uma organização que lide com dados pessoais, a forma como a informação é tratada através de medidas de segurança e do reporte de incidentes vai ditar a sua "*accountability*"[2], não devendo, consequentemente, ser descurada a sensibilização de cada colaborador para esta temática, constituindo-se como elemento chave em cada organização que faça o respetivo tratamento, conferindo-lhe valor essencial e diferenciador no mercado. A constante mutação do tipo de ameaças requer, por outro lado, que a segurança tenha de ser cuidada, todos os dias, para evitar que os dados pessoais fiquem em risco, dependendo tal operação da organização interna da Cibersegurança, de boas bases de gestão de risco e da integração do princípio da Segurança e Privacidade desde a conceção e por defeito.

---

[1] Art.83.º do RGPD, Regulamento (UE) 2016/679 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.

[2] N. º2 do art. 5.º, art. 24.º e considerando 89 do RGPD.

As medidas existentes, em termos de segurança e privacidade, apresentam-se, nos dias que correm, como insuficientes e a necessitar de outra abordagem de modo a criar uma sociedade digital consciente dos riscos relativamente à qual não poderá ser colocado de parte nenhum dos intervenientes já que uma sociedade só funciona, na sua plenitude, se existirem garantias de respeito dos direitos e liberdades fundamentais, não sendo a sociedade digital diferente, nem devendo ser tratada como tal, nem estar sujeita ao livre arbítrio de cada um.

Com o aumento dos Ciberataques, a proteção dos dados pessoais está, mais do que nunca, dependente da Cibersegurança, pelo que tentar proteger aqueles sem o recurso a esta última torna-se um desígnio ilusório e que dependerá, não apenas de alterações legislativas, mas sobretudo da melhoria das medidas de segurança que venham a ser implementadas e da forma como são executadas.

1. Proteção de Dados Pessoais

O RGPD constituiu um importante passo no aumento da consciência dos cidadãos da União Europeia sobre privacidade[3], muito graças às coimas[4] elevadas que estão previstas no referido diploma. Porém, o RGPD ultrapassa esse ditame pecuniário dado que a proteção da privacidade e a proteção dos dados pessoais são pilares fundamentais de uma sociedade evoluída e informada do valor dos seus dados, estando a mesma dependente do respeito destes direitos, consagrados universalmente[5] e que representam um valor incomensuravelmente maior que qualquer

---

[3] ENISA, "Good practices in innovation under ncss" – Good practices in innovation on cybersecurity under the national cyber security strategies, novembro 2019, p.8, disponível em: <https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1>, acedido a 23/03/2020.

[4] Desde maio de 2018 até março de 2020 as autoridades de controlo impuseram 231 coimas e sanções. CMS, GDPR, disponível em: <https://www.enforcementtracker.com/?insights>, acedido a 12/02/2020.

[5] N.º 2 do art. 1.º e considerando 4 do RGPD, art. 26.º e 35.º da Constituição da República Portuguesa, art.º 8.º da Convenção Europeia dos Direitos do Homem, art. 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia, art. 16.º do Tratado de Funcionamento da União Europeia, art. 12.º da Declaração Universal dos Direitos Humanos.

coima. O referido diploma procura assegurar a total e efetiva aplicação desses direitos[6], considerando que os dados não podem ser tratados a qualquer custo, devendo ser geridos de forma diferente dos dados corporativos, isto é, com um grau maior de sensibilidade. Caso flagrante da sua diminuta efetividade é o das políticas de privacidade, extremamente técnicas e ininteligíveis para a população em geral, sendo este, aliás, um dos fatores de falta de transparência de quem trata os dados e que vem favorecer o alheamento em relação ao controlo dos dados pessoais, criando uma exposição perigosa a possíveis "agendas escondidas" das organizações.

Se os dados pessoais são o novo petróleo, a sua proteção é o controlo da poluição. Quem os trata deve ter especial cuidado, não só pelo valor comercial que possam ter, mas sobretudo atendendo aos direitos fundamentais envolvidos, jamais podendo ser causa justificativa da violação desses dados, tanto a liberdade existente no ciberespaço, como o facto de a tecnologia avançar a uma velocidade difícil de acompanhar por qualquer ordem normativa. É nessa medida que a Cibersegurança pode ter um papel decisivo na proteção dos dados pessoais.

O RGPD veio revolucionar a cultura de negócio à volta dos dados, apresentando-se como uma oportunidade, não só forçando os intervenientes a respeitar as mesmas regras com os mesmos princípios, como permitindo criar produtos e serviços mais éticos, convertendo a proteção de dados pessoais num caminho que maximiza a criatividade e a inovação, exigindo que as organizações tenham uma abordagem mais abrangente em relação à proteção dos dados pessoais para assegurar o cumprimento do RGPD desde o início de cada processo. Existe, dessa maneira, a necessidade de salvaguardar a privacidade e os dados pessoais, na medida em que uma violação destes direitos, nos termos do considerando n.º 85 do RGPD, "...pode causar danos físicos, materiais ou imateriais às pessoas singulares como a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos...".

---

[6] Training Data Protection Authorities and Data Protection Officers – T4DATA, *The DPO Handbook Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation*, julho de 2019, p. 21-26, disponível em: <https://www.garanteprivacy.it/documents/10160/0/T4DATA-The+DPO+Handbook.pdf.>, acedido a: 16/04/2020.

Depreende-se do acima explicitado que estando os dados pessoais maioritariamente no ciberespaço e representando os Ciberataques uma inevitabilidade para o aumento do risco para os direitos e liberdades, torna-se primordial a realização de avaliações de impacto sobre a proteção de dados[7], cumprindo dessa forma o que vem preceituado no n. º1 do art. 32.º do RGPD. Outro contributo que o RGPD confere para elevar o nível de Cibersegurança no mercado único digital, será a certificação[8] que permitirá que os titulares dos dados avaliem rapidamente o nível de proteção de dados proporcionado pelos produtos, serviços e processos em causa[9], bem como também os códigos de conduta[10] que poderão consubstanciar um papel de garante do tratamento correto pelo responsável pelo tratamento e subcontratante[11]. Tanto os códigos de conduta como os procedimentos de certificação são fatores demonstrativos do cumprimento das obrigações, de acordo com o que dispõe o n.º 3 do art. 32.º do RGPD, ainda que nenhum destes mecanismos exclua, de forma automática, a responsabilidade, em caso de incumprimento.

A própria definição de violação de dados pessoais no RGPD refere que se trata de uma violação da segurança[12], donde se infere que a Cibersegurança é um imperativo normativo que demonstra a proximidade entre a proteção de dados pessoais e a segurança, realçando a importância de uma abordagem coordenada entre as duas para identificar e gerir os riscos, consequentemente, aumentando a eficácia e reduzindo os esforços[13].

É, ainda, de salientar a crescente preocupação dos titulares dos dados com a violação dos seus dados pessoais (55%), mais do que, por exemplo, em perder a carteira (23%) de acordo com um estudo relacionado com

---

[7] Alínea d) do n. º7 do art. 35.º do RGPD.

[8] Art.42.º do RGPD.

[9] Art.42.º e considerando 15 do RGPD, considerando 74 do Regulamento EU 2019/881 do Parlamento Europeu e do Conselho de 17 de abril de 2019.

[10] Art.40.º do RGPD.

[11] N. º3 do art. 24.º do RGPD.

[12] Art.4.º ponto 12) do RGPD.

[13] NIST Special Publication 800-37 Revision 2 *Risk Management Framework for Information Systems and Organizations – A System Life Cycle Approach for Security and Privacy*, dezembro 2018, p.163, disponível em: https://doi.org/10.6028/NIST.SP.800-37r2, acedido a 8/4/2020.

proteção de dados pessoais e Cibersegurança[14]. Por outro lado, 52% das pessoas não se sentem bem informadas sobre Cibersegurança de acordo com o Relatório Cibersegurança em Portugal de 2019[15], o que reflete uma assincronia entre a proteção de dados e a Cibersegurança, que deve ser urgentemente corrigida.

Ainda que seja utópica a ideia de um cumprimento integral do RGPD[16], não existirá uma efetiva proteção de dados pessoais no mundo digital sem Cibersegurança, sendo dois vetores que terão de estar sempre ligados, que vão para além do que esteja preceituado em qualquer diploma legal.

2. Cibersegurança

A Cibersegurança pode ser definida como qualquer medida implementada para proteção e segurança da informação que estiver no ciberespaço, como das infraestruturas onde residem, de possível disrupção e ataque[17]. Estando os nossos dados pessoais maioritariamente em modo digital e no ciberespaço, o RGPD constituiu um passo essencial ao nível da Cibersegurança, ao criar regras para o tratamento dos dados pessoais, do ponto de vista da segurança. Desse modo, a Cibersegurança deverá ser parte integrante da execução do RGPD por parte das organizações[18], a

---

[14] Radware's 2018 C-Suite Perspectives: *Trends in the Cyberattack Landscape, Security Threats and Business Impacts*, disponível em: <https://www.radware.com/LegalNotice/.consumer sentiments: cybersecurity, personal data and the impact on customer loyalty>, acedido a 13/05/2020.

[15] Observatório de Cibersegurança, Centro Nacional de Cibersegurança "*Relatório Cibersegurança em Portugal de 2019*", dezembro de 2019.p.7, disponível em: https://www.cncs.gov.pt/content/files/relatrio_sociedade_2019_-_observatrio_de_cibersegurana_cncs.pdf, acedido a 24/04/2020.

[16] O USBank assume na sua política privacidade que qualquer armazenamento e transmissão de dados não pode ser garantida a 100%, disponível em: https://www.usbank.com/about-us-bank/privacy/security.html, acedido a 2/07/2020.

[17] White Paper, Advisera, *Privacy, Cybersecurity and ISO 27001-How are they related?*, 2016.p.7, disponível em: <https://info.advisera.com/27001academy/free-download/privacy-cyber--security-and-iso-27001>, acedido a 18/04/2020.

[18] Considerandos 6 e 7 do RGPD.

evolução tecnológica assim o exige e só dessa forma se poderá estabelecer um quadro sólido de proteção de dados pessoais. O RGPD ao exigir um determinado patamar de medidas técnicas e organizativas que garantam a segurança de dados e o exercício dos vários direitos ali previstos (portabilidade, apagamento, acesso, etc.), sem os quais não é possível assegurar um grau adequado de privacidade, veio realçar a relevância da Cibersegurança, contribuindo para a maturidade digital de segurança das organizações. Por sua vez, o aumento do número de pessoas a utilizar o ciberespaço e do número de fontes de armazenamento de dados (muitos deles pessoais) resulta no aumento dos desafios da Cibersegurança dos dados pessoais.

Tendo em apreço o referido e de a conectividade ser o nosso oxigénio atualmente[19], sem o qual não podemos viver, potenciam-se, de igual forma, os Ciber riscos que podem afetar direitos fundamentais da forma mais simples, como seja um mero clique num *e-mail* de *phishing*.

A violação de dados pessoais é um risco real e um dos custos imediatos de um Ciberataque, devendo a proteção de dados pessoais ser sempre desenvolvida de forma centrada no respeito dos direitos humanos e das liberdades fundamentais, tendo por base os interesses dos cidadãos e organizações em conformidade com os direitos em matéria de privacidade e de proteção de dados. Ainda que a segurança dos dados pessoais não seja, suficientemente, relevante para as organizações, o risco da continuidade do negócio e a reputação poderão ser fatores determinantes para fomentar uma atitude diferente em relação àqueles[20].

Pelo bem dos dados pessoais, a solução poderá passar por integrar as políticas de Cibersegurança nos processos de negócio de uma organização.

---

[19] O número de aparelhos de IoT instalados espera-se que exceda os 21 biliões em 2025 no mundo inteiro-Statista 2019, disponível em: <https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/>, acedido a 05/05/2020.

[20] De acordo com inquérito sobre a perceção de ciber risco realizada a 1.300 executivos pela Marsh e pela Microsoft no qual se constatou que o cenário com maior potencial de impacto em termos de perdas está associado à "interrupção do negócio" (75%), seguido do risco de "danos reputacionais" (59%) e da "violação da informação dos clientes"(55%), revelador do grau de prioridade de cada um, disponível em:

<https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf>, acedido a 16/05/2020.

Situação evidente da prioridade do negócio em detrimento da segurança é o da migração de dados para a *cloud* realizado pelas organizações, nomeadamente, para *clouds* públicas, aumentando o risco, decisão suportada unicamente no custo e funcionalidade (disponibilidade de acesso) e raramente na segurança. Adstrita a esta opção, as organizações negligenciam o facto de virem a ser responsabilizadas em caso de violação de dados pessoais e não o Encarregado de Proteção de Dados (EPD) ou o departamento de informática, o que deve conduzir à reflexão da questão da Cibersegurança como prioridade na sua estratégia (operacional e financeira, para além da legal).

As falhas na garantia de segurança poderão tornar-se, por essa razão, o melhor incentivo para que se invista na segurança, pois as perdas financeiras e os danos reputacionais poderão ser consideráveis, pense-se num Ciber incidente[21] que faça capa de jornais e no potencial do impacto catastrófico na balança comercial de uma organização, tendo em conta que o dano infligido aos dados pessoais será superior a qualquer coima[22]. Aliás, esta é a principal razão pela qual as organizações evitam comunicar incidentes o que, por sua vez, dificulta que outras tenham noção das potenciais perdas no caso de sofrerem um incidente, constituindo um desequilíbrio de informação entre as organizações, fruto do desconhecimento das consequências reais de um Ciberataque.

Naturalmente, os requisitos de segurança e os respetivos custos são proporcionais à sensibilidade da informação porém, a falta de responsabilização, muitas vezes por não se saber quem foi o autor de um ataque ou sequer se foram atacados, a dificuldade em obter o direito de

---

[21] Um incidente de Cibersegurança traduz-se em qualquer ação não autorizada ou ilegal que envolva computadores (sistemas ou aplicações) ou redes, representando quebras nas medidas de Cibersegurança e as medidas de resposta envolvem o bloqueio do ataque e a reposição do normal funcionamento, bem como a identificação das causas do incidente de forma a prevenir futuros ataques, fraudes e extorsões, disponível em: <https://www.gee.gov.pt/pt/documentos/estudos-e-seminarios/temas-economicos/7237-te54-a-economia-da-ciberseguranca/file>, acedido a 2/6/2020.

[22] O *data breach* da empresa Talk Talk em 2015 causou enormes danos reputacionais, não só expôs dados pessoais de mais de 150 mil clientes, mas viu a sua receita reduzida em mais de 20 milhões de dólares e perder mais de 100 mil clientes. Passado um ano do ataque o valor de mercado desceu e passado quatro anos continua abaixo do valor de 2015, disponível em: <https://www.ft.com/paidpost/aon/cyber-risk-counting-the-cost.html>, acedido a 7/05/2020.

regresso sobre os danos que sejam causados, a sensação de impunidade, o anonimato e ausência de fronteiras, desconsidera os custos dos incidentes de segurança, tornando difícil de justificar possíveis alocações em segurança preventiva. Com a agravante de o custo de um incidente poder não ser mensurado financeiramente quando ocorre, uma vez que o incidente pode demorar anos a ser resolvido – algumas organizações podem nunca recuperar – e o titular dos dados pessoais poder perder, de forma irreversível, a confiança na mesma, com os prejuízos imediatos que isso pode comportar.

Ao contrário do que se possa julgar não é um investimento sem retorno, a poupança será maior que o investimento, pois a Cibersegurança permitirá diminuir os custos relacionados com os incidentes que podem salvaguardar a continuidade do negócio.

Entende-se que a implementação de medidas simples de Cibersegurança (como o uso extensivo de cifragem) será uma solução associada a redução de custos de incidente, além de ser um facilitador de oportunidade de negócio e não um fator impeditivo daquele e conferir um selo de qualidade na forma segura como são tratados os dados pessoais. A preocupação das organizações com a segurança será tanto maior quanto mais tiverem a perder com essas falhas, contudo, a grande questão é saber se existe estímulo suficiente para que invistam em Cibersegurança, isto é, se têm perceção das potenciais perdas financeiras que poderão resultar de Ciberataques.

O facto de grande parte das organizações ainda optar pela internalização desta função, por não a considerarem uma área prioritária, poderá ser explicado pelo facto de o tecido empresarial ser constituído na sua grande maioria por PME´s, com menor capacidade financeira para fazer face às necessidades de uma política de Cibersegurança eficaz. Não obstante isso, o facto de o tecido empresarial português ter essas caraterísticas não pode ser justificação para a escassa consciência da importância da Cibersegurança, visto este tipo de organizações pequenas poderem ser encaradas pelos atacantes como alvos fáceis tornando-as um foco de risco, para além de, em caso de transferência de dados pessoais para um operador de infraestruturas críticas, ser um risco ainda mais acrescido.

Convirá realçar que nenhuma organização é demasiado pequena para ser atacada, logo, a maneira mais fácil de motivar uma organização a adotar

serviços de segurança é depois de ela sofrer um ataque, devendo-se essa mentalidade ao conhecimento – muitas vezes inexistente – que as organizações têm sobre estes temas, por não estarem cientes da necessidade que existe em proteger a sua infraestrutura, as suas operações e o seu próprio negócio.

A realidade é que, e a menos que seja estritamente necessário por questões legais (e aqui, pode ser determinante o RGPD e a sua execução), os ataques não são comunicados. Esta perceção de um aparente conforto leva as organizações a negligenciar a segurança da sua informação.

Acresce a este cenário, ainda, a confiança "cega" na tecnologia que podem possuir que, diga-se, por muito melhor que seja, não transfere um grande valor para a organização se não for implementada, gerida e monitorizada de forma adequada, já que por vezes a falta de recursos não é na tecnologia, a qual já pode existir dentro da organização, mas na inexistência de procedimentos para as utilizar, por exemplo, a existência de uma *firewall* não é suficiente se não tiverem um controlo de acesso à informação.

Em resultado da existência de uma utilização massiva das tecnologias de informação por parte das organizações, estas não podem querer mudar digitalmente e não serem responsáveis pela Cibersegurança. No caso da segurança dos dados pessoais, dificilmente a segurança é demonstrável, mas facilmente se identificam as quebras de segurança, ficando a Cibersegurança dos nossos dados a depender do rigor colocado na *accountability* do RGPD por parte das autoridades de controlo, isto é, na capacidade de se poder comprovar o cumprimento por parte dos responsáveis pelo tratamento, que poderá ser insuficiente face à realidade atual e que não garante, por si só, o que se pretende proteger, dados pessoais. O facto de a Cibersegurança afetar toda a organização deverá ser condição suficiente para o Ciber risco ser integrado nos riscos da mesma, o qual pode ter origem, não só, num determinado ativo, mas numa vulnerabilidade no sistema daquela. É, por consequência, necessário ter uma visão ampla da Cibersegurança, dado que esta se relaciona com vários setores e tem implicações em serviços essenciais, administração pública, empresas, indivíduos, convocando várias áreas: tecnologias de informação, comunicação, segurança, direito, economia, sociologia ou relações internacionais, o que não lhe confere um caráter isolacionista de vertente técnica ou criminal.

A Cibersegurança é um processo contínuo, na linha do cumprimento do RGPD, seja através da atualização das políticas (evidencia-se que não é por ter muita documentação que as pessoas cumprem o que está preceituado) seja da monitorização do sistema de gestão da informação, é, em síntese, um trabalho que nunca acaba; convém é, em alguns casos, iniciá-lo.

Estamos, evidentemente, perante uma grande mudança de práticas estabelecidas que vão sendo alteradas de uma forma suave, em todas as organizações, devendo ser encontrados pontos de entendimento que resultem em que os intervenientes (colaboradores, subcontratados e titulares de dados pessoais) vejam vantagens em a adotar. Compromisso que só resultará se for estabelecida como um integrador em cada departamento da organização e, para isso, tem de fazer parte da estratégia da mesma e não ser um elemento facultativo. Um caso paradigmático é o envio dos dados encriptados por *e-mail* conferir a proteção face a terceiros para que estes não tenham acesso aos dados em apreço, ainda que possa ser um processo moroso a implementar numa fase inicial. Na prática, todos os dias, tomamos decisões de segurança tão simples como trancar a porta de casa, ainda que não saibamos como funciona o mecanismo da fechadura, trata-se de um ato natural e, desse mesmo modo, deverá ser entendida a Cibersegurança, posto que se esta não tiver a adesão das pessoas e continuar a ser um elemento estranho significa que não alcançou a efetividade necessária e os dados pessoais continuam em risco. Entendida a premência da existência de um ambiente seguro para estabelecer e desenvolver qualquer atividade económica ou social, a segurança deve existir para libertar os cidadãos e as organizações de preocupações, de modo a que se possam focar nas suas atividades[23].

Da parte do titular dos dados, também existe pouco estímulo para exigir a Cibersegurança dos seus dados pessoais porque, a maior parte das vezes, não tem perceção do alcance do risco, já que grande parte dos utilizadores do ciberespaço não são capazes de distinguir quais são os dispositivos/sistemas que são seguros ou não, levando a essa falta de exigência. Ao não existir essa perceção por parte dos utilizadores

[23] Centro Nacional de Cibersegurança *Quadro Nacional de Referência para a Cibersegurança*, p.10, 2019.

também não haverá estímulo para que as organizações promovam a Cibersegurança.

A preocupação com a Cibersegurança de cada um, seja em atividades laborais ou na esfera pessoal, pode ter resultados vantajosos, quando tratamos os dados pessoais de terceiros, podendo esta consciencialização ser um ponto de inflexão na questão da mesma.

O RGPD não especifica medidas de Cibersegurança concretas, mas que sejam tomadas as medidas adequadas[24], ainda que não exista um modelo ideal e do ónus de cada organização ter as suas idiossincrasias, o compromisso da direção, a existência de políticas, definição dos responsáveis, evolução da performance, monitorização e auditoria interna tornam-se fatores diferenciadores de um programa de Cibersegurança robusto que vai para além do cumprimento de qualquer diploma. Necessitando, para alcançar o sucesso, não apenas da componente técnica mas também da identificação do contexto onde é utilizado, da proteção dos sistemas e dos ativos, da deteção de desvios, das respostas prévias aos incidentes e do estabelecimento de operações de continuidade de negócio[25], mas sobretudo depende de uma boa relação das pessoas com a Cibersegurança, do reconhecimento que as pessoas representam a parte mais frágil nas cadeias de Cibersegurança e de criar condições para torná-las *firewalls* humanas robustas contra os Ciberataques[26]. A criação de uma cultura de Cibersegurança constitui-se, dessa forma, como essencial para solucionar os problemas que possam surgir, de uma forma adequada[27] e que não se cinja a uma *accountability* não representativa da realidade, em face duma exigência diminuta por parte da autoridade de controlo, com os efeitos

---

[24] National Cyber Security Center "Cyber Security Toolkit for Boards", p. 18, abril 2019, disponível em: https://www.ncsc.gov.uk/collection/board-toolkit, acedido a 27/05/2020.

[25] NIST, "Cybersecurity approach to cybersecurity Framework (CSF)", white paper series, issue 5, p.8 2019.

[26] ENISA, "Cyber Security Culture in organisations", *European Union Agency For Network and Information Security*, novembro 2017, p.29, disponível em: <https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations>, acedido a 1/7/2020.

[27] Centro de Ciberseguridad Industrial "CCI, roadmap de la ciberseguridad industrial en españa, 2019-2020", 2019, p.10, disponível em: <https://www.cci-es.org/detalle-actividad/-/journal_content/56/10694/974082>, acedido a 16/03/2020.

irreversíveis para a organização e para os titulares dos dados pessoais que daí podem resultar[28-29-30].

Abreviadamente, as organizações devem assumir que nunca estão seguras e não podem confiar que o cumprimento da lei as exime de qualquer responsabilidade, tendo de ter, também, em linha de conta que os processos legislativos tendem a ser mais lentos que a evolução tecnológica (desenvolvimento de *malware* que está constantemente a criar novas ameaças, p.ex.).

A dúvida sobre os Ciberataques não é em saber se vão existir, mas em saber, quando vão acontecer.

3. Ciberataques

Muitas são as organizações que têm fragilidades na segurança e se deparam com Ciberataques aos dados pessoais que possuem, cada vez com mais frequência[31]. Esta é uma situação que normalmente não é bem

---

[28] Como prova de que a Cibersegurança e a Proteção de Dados Pessoais andam de mãos dadas, temos o caso do ciberataque à EasyJet, onde foram revelados dados de *e-mail* e dados de viagens de aproximadamente 9 milhões de clientes, assim como mais de 2000 clientes viram os dados dos seus cartões de crédito expostos, tendo sido acedidos por uma parte não autorizada. A autoridade de controlo do Reino Unido lançou uma investigação e o Centro Nacional de Cibersegurança está a trabalhar com a Easyjet para perceber como o ataque afetou os cidadãos do Reino Unido, disponível em: <https://www.theguardian.com/business/2020/may/19/easyjet-cyber-attack-customers-details-credit-card>, acedido a 8/8/2020.

[29] Em 16 de outubro a British Airways foi multada pela autoridade de controlo (ICO) pela falta de proteção de dados dos seus clientes, o ciberataque permitiu aceder a dados pessoais de mais de 400.000 clientes da companhia, o que revelou não existirem medidas de segurança adequadas, disponível em: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers>, acedido a 19/10/2020.

[30] A autoridade de controlo do Reino Unido impôs uma sanção de 20.7 milhões de euros à Marriott por não assegurar medidas de segurança apropriadas no processamento de dados pessoais dos seus clientes, violação que teve origem num ciberataque que comprometeu o sistema de IT, disponível em: <https://gdprhub.eu/index.php?title=ICO_-_Monetary_Penalty_on_Marriott_International_Inc.&mtc=today>, acedido a 17/11/2020.

[31] A Uber referiu que duas pessoas que não trabalhavam para a empresa acederam a dados através de um serviço de *cloud* que a empresa utiliza, disponível em: https://us.norton.com/internetsecurity-emerging-threats-uber-breach-57-million.html, acedido a 23/08/2020.

acolhida externamente, quer por colocar em evidência as insuficiências, quer por revelar uma segurança deficitária que resulta num impacto negativo na sua credibilidade. Convém dar nota que a exposição aos riscos é uma condição intrínseca de estarmos no ciberespaço permanentemente e os Ciberataques abrangerem todo o tipo de organizações, independentemente da dimensão. Estando o ciberespaço ainda a caminho da sua maturidade civilizacional, marcada pela assimetria entre os conhecimentos necessários para cometer um cibercrime e as competências necessárias para se defender dele com as consequentes ausências de regras que daí decorrem, tornam a Cibersegurança uma prioridade para as organizações que têm como foco a proteção dos dados pessoais.

No que concerne aos Ciberataques, propriamente ditos, estes podem ter vários tipos de objetivos como o roubo de dados pessoais, o uso abusivo dos mesmos, roubo de identidade, divulgação indesejada/ não autorizada de informação, destruição de reputação, etc., sendo os meios para aceder a estes variados: engenharia social, *phishing, ransomware, malware*, redes sociais, *cloud computing, DDO's* (ataques de negação de serviços), etc.[32] Ao contrário do que se possa pensar, a maioria dos ataques são baseados em técnicas já conhecidas e não somente em técnicas sofisticadas, começando,

---

Em abril mais de metade de um bilião de ficheiros de usuários do Facebook foram expostos por uma terceira parte não protegida de um serviço de *cloud*. A informação financeira de mais de 80 milhões de americanos foi exposta através de um ataque a um serviço de *cloud*, disponível em: https://research.checkpoint.com/2019/cyber-attack-trends-2019-mid-year-report/Capital One- personal information of more than 100 million individuals, including Social Security numbers and bank accounts, was compromised in a massive data theft <https://eu.usatoday.com/story/money/2019/07/29/capital-one-data-breach-2019-millions-affected-new-breach/1863259001/>, acedido a 3/9/2020.

A Equifax anunciou que dados de mais de 147 milhões de pessoas foram expostos através de uma violação de dados, disponível em: <https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement>, acedido a 9/9/2020.

A companhia área Cathay Pacific Airways Limited foi multada em £500,000 por falhas de segurança aos dados dos seus clientes, entre outubro de 2014 e maio de 2018 não existiam medidas adequadas de segurança que levaram a que os dados ficassem expostos, disponível em: https://ico.org.uk/action-weve-taken/enforcement/cathay-pacific/, acedido a 17/9/2020.

[32] Os *hackers* maliciosos precisam de começar seja através de servidores vulneráveis, *e-mails* de *phishing* ou de credenciais furtadas. Verizon, "2019 Data Breach Investigations Report", p.66-67, disponível em: <https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf>, acedido a 9/7/2020.

por vezes, com técnicas muito simples, sendo o *e-mail* a forma mais comum para um ataque[33].

Não fossem já suficientes os meios existentes, todos os dias há novos tipos de *malware*, o que torna premente uma adequada Cibersegurança que vise proteger a privacidade e os dados pessoais[34]. Em 2021, espera-se que eventos de Ciberataques tenham custos de 6 triliões de dólares[35], ainda que o custo total não seja compreendido no impacto que provoca o incidente. Os Ciberataques tornaram-se um perigo comum para os indivíduos e para os negócios, de acordo com o relatório global de riscos do WEF, que se refere àqueles como um dos maiores riscos para realizar negócios globalmente, nos próximos 10 anos[36].

Se por um lado, os Ciberataques se tornam mais intensos, complexos e sofisticados, por outro, existe uma maior partilha de informação, mais massa crítica e novos processos tecnológicos e organizacionais que ajudam a reduzir o fosso existente entre os intervenientes.

No entanto, nenhuma organização vai estar verdadeiramente preparada para um Ciberataque, o que torna a preparação para o rescaldo de um incidente um fator distintivo nos resultados a longo prazo. Deve-se, de igual forma, estar preocupado não só com a prevenção, mas, em especial, com a "cura" da violação dos dados pessoais.

Por sua vez, a implementação do RGPD, ao ter obrigado as organizações a rever os seus processos, políticas, a averiguar que dados tinham armazenados e as respetivas medidas de segurança, deverá constituir condição suficiente para colocar na ordem do dia o impacto de um Ciberataque e vir a estabelecer a Cibersegurança como prioridade para a proteção dos dados pessoais.

---

[33] *Idem,* p.13 "90% das organizações recebem *malware* através deste canal."

[34] European Data Protection Supervisor "Leading by Example, EDPS 2015-2019", 2019, p.68, disponível em: <https://edps.europa.eu/data-protection/our-work/publications/strategy/leading-example-edps-2015-2019_en>, acedido a 26/04/2020.

[35] Cisco and Cybersecurity Ventures Press Release 2019, Cybersecurity Almanac, junho de 2019, disponível em: <https://cybersecurityventures.com/cybersecurity-almanac-2019/>, acedido a 3/9/2020.

[36] World Economic Forum "The Global Risks Report 2020", 15ª edição, p.12, disponível em: <https://www.weforum.org/reports/the-global-risks-report-2020>, acedido a 6/8/2020.

4. Proteção e segurança de dados desde a conceção e por defeito

A proteção de dados desde a conceção e por defeito, preceituadas no art. 25.º do RGPD, têm um papel fulcral nos dados pessoais, podendo resultar do seu não cumprimento a aplicação de coimas[37], o que implica que a privacidade esteja integrada no conjunto de requisitos não funcionais desde o momento em que se concebe e desenha[38] e devendo, em função disso, ser também arquitetada uma segurança desde a conceção e por defeito, através de medidas técnicas e organizativas. De igual modo, a proteção por defeito (n.º 2 do art. 25.º do RGPD) tem um papel importante, no que à Cibersegurança diz respeito, através da limitação de acesso ou na minimização dos dados[39] que resulta numa postura mais cautelosa em relação àqueles, protegendo a sua segurança.

Por via disso, a proteção de dados pessoais (Cibersegurança) não pode jamais ser encarada como colocando em causa a funcionalidade e viabilidade de uma organização, sob pena de colocar em risco os dados que ela se propõe tratar.

Não ter isso em conta será como construir um automóvel sem cinto de segurança.

Atualmente, já temos departamentos jurídicos, *developers*, marketing e recursos humanos, todos sentados à mesma mesa para assegurar que as medidas de proteção dos dados pessoais e a sua ética estejam integradas ao longo do ciclo de vida de um produto/serviço, que se faz realizando a integração da proteção de dados pessoais e da Cibersegurança de uma forma colaborativa, quase orgânica. Tratando-se de um processo contínuo, pode suceder que uma medida implementada no início já não esteja a proteger nas mesmas condições, o que pode resultar no aumento de risco, daí ser necessário ter em atenção o estado da arte, conforme decorre do próprio artigo, não significando, por isso, que seja necessário um investimento avultado, como também no sentido oposto, a falta de

---

[37] Alínea c) do n.º 1 do art. 38.º da Lei nº 58/2019 e alínea a) do n.º 4 do art. 83.º do RGPD.

[38] Agencia Española Protección Datos, "Guía de Privacidad desde el Diseño", outubro 2019.p.8, disponível em: <https://www.aepd.es/sites/default/files/2019-11/guia-privacidad--desde-diseno.pdf>, acedido a 24/07/2020.

[39] Alínea c) do n. º1 do art. 5.ºdo RGPD.

investimento não pode ser causa justificativa para o não cumprimento da proteção de dados pessoais.

Cumpre, ainda, referir que não existem medidas de segurança mais adequadas do que outras, o que é relevante é a sua eficácia, este é o cerne do conceito de proteção de dados desde a conceção[40] e, por conseguinte, da Cibersegurança.

É, em função do acima descrito, essencial que o responsável pelo tratamento, quando esteja a implementar as medidas, tenha o entendimento necessário dos direitos e princípios que estão em causa e saiba que estão em causa direitos dos titulares dos dados que devem ser invioláveis.

Assegurar a privacidade e a segurança dos dados pessoais não podem ser obstáculos, mas premissas de quem os trata, desde a conceção e por defeito.

5. As Medidas de Segurança

O RGPD[41] refere a obrigação do responsável pelo tratamento e o subcontratante aplicarem medidas técnicas e organizativas de forma a assegurarem um nível de segurança adequado ao risco, sendo necessário, portanto, analisar qual o nível de adequação exigido para essas medidas garantirem a segurança dos dados.

Os sinais dados não são promissores, por exemplo, quando na alínea g) do n.º 1 do art. 30.º do RGPD se faz referência ao registo das atividades de tratamento e de que neste deve constar a descrição geral das medidas técnicas e organizativas no domínio da segurança, "se possível", o que lhe retira relevância e lhe confere um caráter opcional, negligenciando o facto de os dados pessoais estarem no ciberespaço implicar inevitavelmente um risco[42] para os direitos dos titulares, devendo, por essa ordem de razão, constituir, desde logo, um caráter obrigatório de implementação

---

[40] European Data Protection Board "Guidelines 4/2019 on Article 25, Data Protection by Design and by Default" novembro 2019, p.7, disponível em: <https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en>, acedido a 10/07/2020.

[41] Alínea f) do n.º 1 do art. 5.º, 32.º e considerandos 74 e 78 do RGPD.

[42] N. º 5 do art. 30.º do RGPD.

de medidas de segurança, não apenas para organizações com mais de 250 trabalhadores.

Outra questão que requer algumas cautelas diz respeito às "medidas técnicas e organizativas adequadas" que surge no RGPD como conceito indeterminado e deixa ao livre arbítrio de cada organização definir quais são e vir a descurá-las, resultando em efeitos severos para a proteção dos dados pessoais.[43]

No que às medidas de segurança o RGPD se refere, surge a pseudonimização[44] como uma das medidas técnicas possíveis e recomendadas para a segurança dos dados, segundo a alínea a) do n.º 1 do artigo 32.º, ainda que possa não ser a mais adequada dado poder haver o risco de uma "inversão não autorizada"[45] e dessa forma ser reversível. Por essa razão, vê-se como mais aconselhável[46] a cifragem para dados mais sensíveis, podendo ser uma medida alargada a todo o tipo de dados pessoais, o que diminuiria o risco de violação dos mesmos.

A tecnologia tem aqui um papel fulcral para o cumprimento da proteção de dados pessoais tanto na cifragem de todos os dispositivos que contenham dados pessoais (PC´s, telemóveis, *pens* USB), como na cifragem de todos os *e-mails* que contenham dados pessoais (evitandas situações de envio de *e-mail* para destinatário errado com dados pessoais) e na cifragem da informação em serviços *cloud*. Por conseguinte, perante situações de perda ou violação de dados, se a organização detiver total controlo sobre a cifra, pode resguardar-se do embaraço de ter de notificar a autoridade de controlo, bem como os titulares dos dados, dessas falhas de segurança – isto, porque os dados são incompreensíveis fora do universo interno da organização.

Cifrar os dados, implica torná-los indecifráveis para quem não tenha autorização de acesso aos mesmos, sendo uma medida básica de mitigação

---

[43] Conforme decorre da Deliberação nº 984/2018 da Comissão Nacional de Proteção de Dados "as limitações técnicas não podem justificar a adoção irrestrita de procedimentos de validação de acessos que praticamente tornam irrelevante o núcleo essencial do direito fundamental à proteção de dados pessoais".

[44] Ponto 5 do art.º 4.º e considerandos 26, 28, 29 e 78 do RGPD.

[45] Considerandos 75 e 85 do RGPD.

[46] Grupo de Trabalho do Artigo 29.º, Parecer n.º 5/2014, 2014 p.33, disponível em: <https://www.gpdp.gov.mo/uploadfile/2016/0831/20160831042518381.pdf>, acedido a 9/07/2020.

do risco de perda ou roubo de dados pessoais, tornando-os, por essa via, ininteligíveis em casos de ataques de *ransomware* ou de outro tipo de violação de segurança.

Também a alínea b) do n.º 1 do art. 32.º e o considerando 39 do RGPD podem ser exemplificadores na importância da Cibersegurança no RGPD, atendendo a que a segurança é um estado transitório e que requer, para a atenuação dos riscos, que sejam cumpridos determinados requisitos para cumprir o desiderato a que se propõe desde o início.

As informações devem estar disponíveis para utilizar quando for necessário e os sistemas que a fornecem possam resistir adequadamente a ataques e recuperar ou evitar falhas (disponibilidade)[47], as informações serem observadas ou divulgadas apenas para aqueles que têm o direito de a saber (confidencialidade)[48], as informações devem ser completas, precisas e protegidas contra modificações não autorizadas (integridade)[49], as transações comerciais, bem como as trocas de informações entre empresas ou parceiros, devem ser confiáveis (autenticidade e não repúdio)[50], requisitos que facilmente serão postos em causa, se não existir um programa de Cibersegurança robusto.

O RGPD realça, de igual modo, a necessidade de realizar uma identificação e avaliação de riscos[51] dos ativos e dos processos de negócio, seguida da implementação de controlos de segurança de diferentes classes (tecnológicos, físicos e organizativos) em função das estratégias para a gestão das ameaças. A organização deve classificar os seus ativos (humanos, tecnológicos de *hardware* e *software*, dispositivos, dados, tempo e aplicações), de acordo com a criticidade e valor que estes ativos representem para si, quanto maior o risco para os direitos e liberdades para os titulares dos dados, mais rigorosas deverão ser as medidas a

---

[47] Art. 13.º e 15º do RGPD, que podem ficar em risco devido a ataques de negação de serviço, causas estruturais, causas naturais p.ex.

[48] Alínea f) do n.º 1 do art. 5.º e considerandos 75 e 83 do RGPD, através de acessos não autorizados, exfiltração de dados, espionagem comercial e/ou industrial, engenharia social, por exemplo.

[49] Alínea f) do n.º 1 do art. 5.º do RGPD, que podem ficar fragilizadas devido a fraudes, ataques à cadeia de distribuição, ataques *man-in-middle* p.ex.

[50] Considerando 49 do RGPD.

[51] N. º 2 do art. 32.º do RGPD.

implementar[52]. Esta decisão pode passar por mitigar, transferir ou evitar ou aceitar o risco, devendo apenas aceitar-se este quando não acarrete consequências significativas para a concretização das atividades críticas do negócio (dados pessoais).

De referir que os riscos de Cibersegurança não são muito diferentes dos riscos no espaço físico, a diferença assenta no impacto e na magnitude que têm os primeiros, devendo ser encarados como cruciais para os dados pessoais. Com uma clara visão sobre os riscos[53] será possível escolher as medidas de segurança dos dados pessoais que são necessárias[54]o que só resultará da integração da Cibersegurança e Proteção de Dados Pessoais.

Depois de definido o programa de Cibersegurança a implementar, é necessário realizar auditorias de segurança e mecanismos de supervisão, bem como a consolidação de informação de registo e monitorização num sistema integrado de gestão de eventos (SIEM) como formas de cumprir a alínea d) do n.º 1 do art. 32.º do RGPD e de aferir a eficácia do mesmo. Esta alínea é demonstrativa da sua relevância pelo facto de em grande parte das organizações as medidas apenas serem atingidas formalmente, o que não é suficiente, já que devem envolver a monitorização contínua dos controlos, avaliação e revisão recorrentes, criando uma melhoria eficiente na Cibersegurança da organização.

Posto isto, tanto o responsável pelo tratamento como o subcontratante[55] têm a obrigação de aplicação de medidas técnicas e organizativas

---

[52] ENISA, "Handbook on Security of Personal Data Processing", janeiro 2018, p. 6, disponível em <https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing>, acedido a 18/05/2020.

[53] Considerandos 75, 76, 77 e art.83.º do RGPD.

[54] Information Commissioner's Office "A practical guide to IT security ideal for the small business", p.4, disponível em: <https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf>, acedido a 3/06/2020.

[55] No que diz respeito aos subcontratantes é necessário averiguar que medidas são tomadas efetivamente por estes e evitar ficar refém, de um acordo formal de subcontratação, pouco efetivo. Se o grau de exigência colocado por parte das organizações em relação ao tratamento dos dados pode ser frágil, em relação aos subcontratantes não é diferente, no que concerne à Cibersegurança, veja-se o caso dos provedores de *cloud services* subcontratados, contratos de "pegar ou largar" condicionando a segurança de quem os contrata. Montagnani, Maria Lillà e Cavallo, Mirta Antonella, "*Cybersecurity and Liability in a Big Data World*", *Market and*

adequadas para proteger os dados pessoais[56], cujo incumprimento pode resultar na aplicação de uma coima[57], tornando-se decisivo o grau de responsabilidade de cada um, no incumprimento do estabelecido nos art. 25.º e 32.º do RGPD.

A organização tem de centrar-se, para além do risco da própria organização, no risco do titular dos dados visto poder ainda acrescer à coima, instaurada pela autoridade de controlo, uma ação judicial[58] instaurada pelo titular dos dados pessoais, podendo resultar numa indemnização pelos danos sofridos[59], ficando a cargo de quem trata os dados pessoais[60] provar que não foi responsável, não desprezando, todavia, as consequências reputacionais que daí podem advir.

Ter uma Cibersegurança de dados pessoais deficitária não isentará, certamente, dessa responsabilidade como fica patente pelas ações tomadas por várias autoridades nacionais de controlo de vários países europeus que aplicaram sanções a organizações por incumprimento do art. 32.º do RGPD[61].

Contudo, mais do que avaliar as opções do legislador ou o grau de exigência da autoridade de controlo em relação às medidas de segurança adequadas, cumpre-nos indicar soluções[62] que podem, inclusivamente, ser encontradas no nosso ordenamento jurídico, podendo ter um papel

---

Competition Law Review, Volume II, No. 2, outubo 2018, p. 91-92 Art. 28.º e considerando 81 do RGPD.

[56] Art. 24.º e 28.º do RGPD.

[57] Alínea d) do n.º 2 do art. 83.º do RGPD e alínea i) do n.º 1 do art. 38.ºda Lei nº 58/2019.

[58] Art. 79.º do RGPD.

[59] Art. 82.º do RGPD e art. 33º da Lei nº58/2019.

[60] N. º 3 do art. 82.º do RGPD e n.º 2 do art. 33.º da Lei nº 58/2019.

[61] Disponível em: <https://edpb.europa.eu/news/national-news/2019/bfdi-imposes-fines-telecommunications-service-providers_pt>; <https://edpb.europa.eu/news/national-news/2019/romanian-national-supervisory-authority-issues-fine-against-fan-courier_pt>; <https://edpb.europa.eu/news/national-news/2019/norwegian-data-protection-authority-imposes-fine-city oslo_en>; <https://gdprhub.eu/index.php?title=ANSPDCP__Fine_against_Enel_Energie_Muntenia>; <https://www.datatilsynet.no/contentassets/9d5792264c884f3a903d3981c38812ac/~-20_02191-1-vedtak-om-overtredelsesgebyr---ralingen-kommune-202444_10_1.pdf>, acedido a 17/11/2020.

[62] O recurso a normas de certificação e boas práticas de gestão de Segurança da Informação (ISO/IEC 27001 e NIST 800-53 poderão ser uma solução eficaz na segurança dos dados pessoais.

importante o recurso à Resolução do Conselho de Ministros 41/2018, de 28 de março de 2018, destinada a definir orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais e aplicá-las nas organizações excluídas da obrigação de possuírem medidas de segurança específicas, podendo ser uma ferramenta útil para as organizações, atendendo ao facto de ser neutra quanto ao tipo de tecnologia a utilizar e definir padrões mínimos.

Não tendo pretensões de se exibirem competências técnicas que não se possuem, elencam-se algumas medidas técnicas e organizativas, recomendadas pelo Centro Nacional de Cibersegurança, que podem representar o nível de adequação que pode estar implícito naquele conceito indeterminado anteriormente referido, de que são exemplo: a implementação de uma política de segurança, procedimento de notificação de incidentes, desenho e implementação de arquitetura e segurança perimétrica (*firewalls*, sistema de deteção e proteção de intrusão IDS/IPS/HIDS), implementação de sistema de recolhas e armazenamento de fluxos de tráfego, inventariação de ativos (CMDB), mapa de rede, recolha centralizada de registos (*logs*),criação de instrumentos de correção ou mitigação de incidente, entre outras.

Para além das medidas técnicas existentes, as medidas organizacionais são essenciais para prevenir e gerir um ataque, que passará por cada colaborador ter consciência do impacto do seu comportamento para evitar a concretização de um Ciberataque, o que requer o conhecimento não só da organização (vulnerabilidades e ameaças a que estão expostos) como também depende do nível da preparação, implicando testar, fazer simulações de ataques para responder de forma rápida quando acontecer, com o fito de melhorar a capacidade de resposta.

Clarificador da importância do acima referido é importante enquadrar em que ponto nos encontramos atualmente, e que de acordo com o *EY Global Information Security Survey 2019*, a informação mais valiosa para os ciberatacantes é a informação de clientes (17%), sendo os maiores Ciber riscos para as organizações, o *phishing* (22%) e, em segundo lugar, o *malware* (20%), o que evidencia a relevância da Cibersegurança para os dados pessoais.

Cumpre, por sua vez, fazer referência ao que está a ser realizado em termos de medidas implementadas, e que de acordo com o Eurostat

6/2020[63] de 13 de janeiro, 93% das empresas da União Europeia utilizam pelo menos um tipo de medida de segurança; 62% consciencializam os colaboradores das obrigações de medidas de segurança; apenas 24% disponibilizam formação; 34% têm documentos com políticas e medidas de segurança e 12% tiveram pelo menos um incidente de Cibersegurança em 2018. Segundo o referido estudo as medidas mais comuns são: atualizações de *software* (87%), autenticação de password forte (77%), *back up* (76%), controlo de acesso (64%), uso de VPN (42%), utilização de técnicas de encriptação para dados, documentos e *e-mails*, (38%) e testes de segurança (36%).

Não obstante tudo o que foi referido anteriormente, convirá ter a perceção de que não existe nenhuma medida técnica e organizacional de segurança que garanta na íntegra a segurança da proteção de dados e de que a única forma de garantir uma segurança impenetrável é não tratar os dados, que não é o que se pretende.

6. Firewall Humana

O elemento central da Cibersegurança são as pessoas, que atuam como a primeira linha de defesa na deteção de uma falha de segurança, devendo, dessa maneira, a segurança da organização ser uma responsabilidade daquelas[64], que será tão ou mais efetiva se lhe retirarmos a conotação tecnológica que ainda possui, de forma a que aquelas sejam sempre entendidas como parte fundamental.

A sensibilização dos colaboradores de uma organização torna-se essencial já que são eles quem efetivamente trata os dados pessoais, estando os responsáveis pelo tratamento e os subcontratantes obrigados a

---

[63] No que diz respeito a Portugal temos, 98% das empresas têm pelo menos uma medida de segurança; 28% têm documentos e medidas de cibersegurança, 54% consciencializam os colaboradores para estas medidas, 8% experienciaram pelo menos um incidente, disponível: <https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f>, acedido a 14/07/2020.

[64] World Economic Forum "The cybersecurity guide for leaders in today´s digital world", outubro 2019, p. 19, disponível em: <http://www3.weforum.org/docs/WEF_Cybersecurity_Guide_for_Leaders.pdf>, acedido a 12/06/2020.

assegurar que aqueles e terceiros estejam consciencializados das medidas de segurança e que as cumprem independentemente da dimensão que possuam[65].

As organizações devem procurar a consciencialização e não a imposição, devendo centrar-se no efeito positivo que vão ter, de forma a que as pessoas fiquem incentivadas a ter comportamentos ciberseguros, sendo algo intrínseco, que se torna um hábito nos processos de trabalho, mais ainda, quando falamos em tratamento de dados pessoais de outrem, não devendo interferir na produtividade, para se vir a estabelecer como um dos fatores potenciadores da Cibersegurança dos dados pessoais.

Ainda que, a Cibersegurança, sem dúvida, dependa da vertente tecnológica, a natureza humana, através da componente comportamental, tem um papel relevante que não deve ser descurado tendo em conta fatores comuns de não cumprimento das medidas de segurança como são o excesso de trabalho e a complexidade do sistema de segurança[66], a que acresce o desconhecimento de tecnologias e dos procedimentos de segurança. Para além disso, comportamentos que se registam a título pessoal, seja através de *apps* ou do *e-mail* pessoal, são mimetizados para a organização onde trabalham, desse modo, o que se faz atualmente na esfera da nossa vida pessoal e profissional não pode já ser considerado como desconexo ou passível sequer de não ser tido em conta, pois cada ação exercida numa das esferas de atuação pode ter um impacto efetivo e sério na outra. De facto, se tivermos em apreço que a grande maioria das pessoas passa uma parte substancial do seu tempo útil de vida, no seu local de trabalho, torna-se inegável que às organizações já não é possível deixar de assumir alguma responsabilidade pelos comportamentos pessoais dos seus colaboradores que terão impactos diretos na organização.

Situação evidente é a presença dos dispositivos móveis pessoais no local de trabalho, que é atualmente prática corrente, que deverá atentar as organizações para os riscos que possa representar para os dados

---

[65] Data Protection Comission "Guidance for Controllers on Data Security", fevereiro 2020, p.3, disponível em: <https://www.dataprotection.ie/sites/default/files/uploads/2020-02/Data%20Security%20Guidance_Feb20.pdf>, acedido a 22/04/2020.

[66] ENISA, "Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity",abril 2019, p.13 disponível em: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity, acedido a 19/06/2020.

pessoais ali tratados e que poderá constituir um incentivo para a criação de uma política de uso aceitável dos recursos de cada um (política *Bring Your Own Device*) como medida de segurança em razão de os dispositivos nem sempre estarem devidamente protegidos, devendo, por essa razão, conduzir a organização a ter como prioridade a formação inicial a todos os colaboradores, optando por treino de Cibersegurança pessoal para depois as pessoas atuarem com o mesmo rigor no local de trabalho, no sentido de garantir a segurança do mesmo. Entende-se que segregar a Cibersegurança a um único departamento é um equívoco, dada a abrangência daquela e do facto de todos os colaboradores serem uma das razões do sucesso e, claro, do insucesso, designadamente através de publicidade encoberta ou ataques de engenharia social, que procuram tirar partido da apetência natural do individuo para ser curioso e social. Aliás, a grande maioria dos ataques com sucesso, não se reveste de grande complexidade, antes resulta da fragilidade do fator humano na sua interação com as tecnologias ao invés das fragilidades das mesmas, sendo os ataques informáticos, na sua grande maioria, facilitados pelos colaboradores que desconhecem os "sinais" de alerta[67].

Como até nos melhores sistemas de segurança existem erros, requer-se uma resposta para esses incidentes como efeito mitigador, antecipando o que deve ser realizado, pois ainda que as medidas técnicas e organizativas estejam a funcionar, a medida mais importante em qualquer organização é assegurar que os colaboradores estejam cientes das suas responsabilidades[68].

Criar a perceção da importância da Cibersegurança dos dados pessoais entre os colaboradores é fulcral para que, quando estiverem a ser alvo de um ataque, saibam como responder, pois muitas vezes, nem sabem que foram alvo de um, nem como devem atuar, o que resulta na sua não comunicação, traduzindo-se em efeitos desastrosos para a organização, mas acima de tudo para os titulares dos dados pessoais.

---

[67] De acordo com o estudo IBM 2018 Cyber Security Intelligence Index, 75% dos incidentes de cibersegurança que envolviam *malware* estavam relacionados com negligência dos colaboradores, e consistem em clicar em links de *phishing*, uso de USB inseguras, uso de passwords fracas, por exemplo, disponível em: <https://www.ibm.com/security/data-breach/threatintelligence>, acedido a 12/07/2020.

[68] Alínea b) do art. 11.º da Lei 58/2019 e art. 24.ºe 37.º a 39.º do RGPD.

7. O Reporte de Incidente

O reporte de incidente de uma violação de dados pessoais está indissociavelmente associado à Cibersegurança em caso de um Ciberataque, e para o qual o RGPD os art. 33.º e 34.º preceituam a necessidade de notificar a autoridade de controlo e, em casos mais graves, o próprio titular dos dados em caso de violação de dados pessoais, podendo resultar o seu não cumprimento numa coima[69].

A obrigação do responsável pelo tratamento em relação aos incidentes de violação da proteção de direitos pessoais surge do princípio de *accountability* (responsabilidade) do n.º 2 do art. 5.º e do n.º 5 do art. 33.º do RGPD.

Tratando-se de um Ciberataque, estes tipos de notificações só serão fidedignas e, principalmente, eficientes, se houver um entendimento claro do que é a Cibersegurança de forma a responder da forma mais exata ao que vem elencado no n.º 3 do art. 33.º do RGPD, nomeadamente em termos de medidas a tomar, das consequências e, acima de tudo, da abrangência da violação. O n.º 4 do art. 33.º do RGPD refere, ainda, situações em que não seja possível fornecer todas as informações ao mesmo tempo, aqui, facilmente, se enquadrando alguns tipos de incidentes de Cibersegurança, que constituem violações mais complexas, em que seja necessária uma investigação forense aprofundada para determinar plenamente a natureza da violação e em que medida os dados pessoais foram afetados[70].

É, igualmente, importante ter em atenção que, em certos casos, a não notificação de uma violação, ou uma notificação incompleta, pode revelar uma ausência de medidas de segurança ou uma inadequação das medidas de segurança existentes. Por isso, uma organização que queira ser *accountable*, que pretenda respeitar as obrigações de segurança de dados, terá precauções com a violação da proteção de dados e, no caso de ocorrer, possuir procedimentos para identificar e comunicar o incidente,

---

[69] Alíneas j) e k) do n. º 1 do art. 38.º da Lei nº 58/2019 e alínea a) do n.º 4 do art. 83.º do RGPD.

[70] Grupo de trabalho do artigo 29 para a proteção de dados, "Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679", fevereiro 2018 p.12, disponível em:

<https://ec.europa.eu/info/law/law-topic/data-protection_en, acedido a 3/7/2020>.

reduzindo o dano infligido aos titulares dos dados pessoais, diminuindo o nível de exposição do responsável pelo tratamento em sofrer sanções e danos reputacionais.

Podemos, então, concluir que apenas notificar e comunicar não é suficiente, transcendendo a questão formal, pois, quando uma organização sofre um Ciberataque que resulte numa violação de dados pessoais, é necessário dar resposta imediata ao incidente e ter a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico[71]. Passará por estabelecer procedimentos e responsabilidades para assegurar uma classificação e resposta eficazes aos incidentes de segurança, através da criação de um procedimento interno para notificação de incidentes que indique como deve proceder um colaborador perante um incidente ou um evento suspeito, da preparação de um plano de monitorização, da posse de equipamento que permita a salvaguarda de informação considerada prioritária para a organização, possibilitando a respetiva reposição em caso de necessidade (*backup/restore*), de ter implementado um mecanismo de prevenção de perda de dados, ou DLP (*Data Loss Prevention*) que se traduz uma abordagem integrada e consolidada da segurança da informação, registo e análise de toda a atividade de acessos de modo a procurar ameaças prováveis[72].

Devem, por conseguinte, fazer parte do Plano de Continuidade de Negócio os elementos essenciais que permitam à organização continuar em operação perante um qualquer desastre ou incidente que cause (ou tenha potencial para causar) uma disrupção, significativa ou até total, na atividade, criando contactos alternativos em caso de reporte de incidente e de os sistemas ficarem comprometidos, impedindo o contacto[73].

Os responsáveis pelo tratamento devem, ainda, documentar todos os incidentes que ocorram, incluindo quando e como aconteceram e as ações de reparação adequadas, que lhes permitam demonstrar estar em

---

[71] Alínea c) do n. º 1 do art. 32.ºdo RGPD, os sistemas de armazenamento devem garantir a redundância e disponibilidade, não devendo existir nenhum "*single point of failure*".

[72] CNCS, "Roteiro para as capacidades mínimas de cibersegurança", outubro 2019, p. 33, disponível em: <https://www.cncs.gov.pt/content/files/cncs_roteiro_capacidades_minimas_ciberseguranca.pdf>, acedido a 4/07/2020.

[73] Idem, p.28.

compliance com a comunicação do incidente à autoridade de controlo. É, por sua vez, fundamental que a documentação contenha indicadores relativos à probabilidade do risco e à severidade do mesmo e ao seu potencial impacto nos direitos e liberdades do titular dos dados pessoais, que se pretendem salvaguardar.

Por fim, depois de identificado um incidente, a organização deverá promover uma variedade de medidas de mitigação que passam por mudanças: operacionais, de processo, de sistemas, promoção do treino de pessoas ou até a rescisão de contratos com trabalhadores e subcontratados. As organizações deverão tomar medidas para futuros incidentes, nas quais se incluem a discussão de lições aprendidas de forma a promover alterações, a monitorização e a utilização de métricas (devem ser revistas todas as provas que foram coletadas e a atuação dos colaboradores para identificar padrões e vulnerabilidades), bem como a apresentação de estudos para explicar o impacto na organização e a definição de soluções para estarem preparadas para o próximo ataque.

Para finalizar entende-se que para a fiabilidade de um reporte de incidente é necessário que a organização tenha um plano de gestão de crise alargado a todos os colaboradores para que, em caso de ataque, não fiquem a aguardar que a tecnologia os suporte. Tem-se como um dos maiores obstáculos à exatidão de um reporte de incidente, que reflita o mais aproximadamente o que aconteceu, o nível de conhecimento em Cibersegurança dos seus intervenientes o que desvirtua, atualmente, o seu propósito que é assegurar a proteção dos dados pessoais.

Mais do que reportar um incidente, é necessário saber que medidas se devem tomar e dessa forma atenuar os danos sofridos pelos titulares, podendo ser uma atenuante na aplicação de uma coima[74] que constitui uma contraordenação grave no ordenamento português[75].

Convém, ainda, referir, que a adoção de medidas de proteção adequadas ainda que possa evitar que se tenha de comunicar ao titular de dados pessoais a referida violação, conforme dispõe o n.º 3 do art. 34.º do RGPD, não estará a ter em conta de um Ciberataque, atendendo às suas caraterísticas e ao facto inerente de ter uma abrangência maior, dada a amplitude do ciberespaço, ser "suscetível" de aumentar o risco para os

---

[74] Alínea c) do n. º 2 do art. 83.º e considerandos 85, 87 e 88 do RGPD.

[75] Alínea j) do n.º 1 do art. 38.º da Lei nº 58/2019.

direitos e liberdades das pessoas singulares irremediavelmente, o que lhe deveria conferir de forma imediata, no nosso entendimento, um caráter de obrigação de comunicação, nos termos do n.º 1 do art. 34.º do RGPD.

Tratando-se de um Ciberataque não podemos deixar de fazer referência, no que diz respeito ao reporte de incidentes de Cibersegurança *tout court,* que a Diretiva UE 2016/1148, de 6 de julho de 2016, encorajou as organizações a pensar de uma forma holística sobre a notificação de incidentes, não incidindo unicamente em incidentes financeiros e a colocar os dados pessoais na ordem do dia[76]. Através da Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço, e transpôs a referida Diretiva, identificaram-se setores e subsetores de operadores de serviços essenciais como fazendo parte do seu âmbito, porém excluiu-se a obrigação da notificação de um incidente por parte da maioria do tecido económico português, limitando-a à notificação voluntária em caso de incidente[77], retirando, desde logo, responsabilidade a quem sofre um Ciberataque aos dados pessoais que trata. Tanto a Diretiva (UE) 2016/1148 como o RGPD representaram um papel importante na obrigação dos atores do ciberespaço aprimorarem as competências em Cibersegurança[78], ainda que peque por defeito pela abrangência reduzida e que poderia ter servido para alavancar a inclusão da Cibersegurança na Proteção de Dados Pessoais, e não ficar reduzido a uma putativa cooperação entre as duas.[79]

Saber como responder a um incidente e qual o passo seguinte é primordial para estabelecer um reporte de incidente fidedigno das possíveis consequências para os dados pessoais.

---

[76] United States Chamber of Commerce and Hunton Andrews Kurth "Aligning Data Breach Notification Rules Across Borders", 2019, p. 12, disponível em: <https://www.huntonprivacyblog.com/2019/04/04/hunton-partners-with-the-u-s-chamber-of-commerce--on-seeking-solutions-aligning-data-breach-notification-rules-across-borders/>, acedido a 3/4/2020.

[77] Art. 20.º Lei n.º 46/2018, de 13 de agosto.

[78] ENISA "Study on CSIRT landscape and IR capabilities in Europe 2025", fevereiro 2019, p.5, disponível em: <https://www.enisa.europa.eu/publications/study-on-csirt-landscape--and-ir-capabilities-in-europe-2025>, acedido a 19/04/2020.

[79] N. º 8 do Art. 7.º da Lei nº 46/2018 de 13 de agosto e Considerando 63 da Diretiva (EU) 2016/1148 de 6 de julho de 2016.

Conclusão

Ao longo deste artigo, pretendeu-se sublinhar a importância que a Cibersegurança deve ter na proteção dos dados pessoais, atendendo a que o RGPD serviu para colocar a Cibersegurança na agenda e para que dependa desta para a sua efetiva execução. Por esse motivo, o RGPD poderá ser o impulsionador que faltava para a implementação da Cibersegurança como parte integrante da proteção de dados pessoais e estabelecer-se como uma prioridade do responsável pelo tratamento, mas também do titular dos dados. Se é evidente que a violação de dados pessoais implica consequências para o titular dos mesmos, consequentemente, a entidade responsável pelo tratamento será responsabilizada em razão disso, com repercussões tanto na reputação, como na continuidade da atividade, em coimas, em prejuízos financeiros, ou em termos legais, fatores que podem ser a pedra de toque para a inclusão da Cibersegurança na proteção de dados pessoais, conferindo-lhe um papel diferenciador e que será aproveitado pelos titulares dos dados, em resultado disso.

O objetivo da inclusão da Cibersegurança na proteção de dados pessoais só pode ser concretizado se os responsáveis pelo tratamento dos dados forem suficientemente "incentivados", através de meios jurídicos ou da ponderação dos riscos reputacionais e financeiros (podendo ser estes últimos a motivação que faltava), a tomar as medidas necessárias para assegurar que esta proteção seja colocada em prática.

No que se refere aos meios jurídicos, as autoridades de controlo de proteção de dados estão no centro do sucesso ou do falhanço da execução do RGPD mas se não possuírem os recursos adequados para aplicar a lei, as organizações acabarão por ignorá-la pelo facto de não ser executada ou ser executada de forma lenta, com repercussões para os titulares dos dados pessoais.

Retira-se ainda do exposto ao longo do artigo que, não é pelo facto de a legislação ser executada que os dados pessoais não deixam de estar em risco. De realçar que se a preocupação de uma organização for apenas cumprir o RGPD, já falhou em grande parte, pois a proteção de dados pessoais, sendo um imperativo legal, deverá ter, impreterivelmente, acoplada uma responsabilidade ética que vai para além de qualquer diploma. Ainda que seja tentador, e nos transmita algum conforto, limitar o cumprimento do art. 32.º do RGPD à avaliação (insuficiente) realizada

por uma autoridade de controlo traduz-se num risco, no estado atual do ciberespaço.

Mais do que ver a proteção dos dados pessoais como uma obrigação legal e percecionando-a apenas com uma visão burocrática, de simples cumprimento de alguns artigos de um determinado regulamento, seja através da criação de politicas de privacidade ou da celebração de acordos de subcontratação com parceiros, por exemplo, deverá ser encarada como a obrigação de estar em *compliance* não apenas com a legislação, mas com a proteção de dados pessoais por si só.

Certamente que o titular dos dados quer que se cumpra a lei, mas, acima de tudo, que se protejam os seus dados pessoais.

O aparente cumprimento que é transmitido pelos documentos em dia, a ficha de atividade de tratamento de dados pessoais, a atribuição de um Encarregado de Proteção de Dados (EPD), etc. (que não são devidamente acompanhadas pelas medidas de segurança) e que, ainda assim, para a autoridade de controlo possa ser suficiente para demonstrar *accountability* e ficar imunes às possíveis coimas, é uma visão simplista do que é a proteção de dados pessoais. Para se cumprir esse propósito é primordial um programa de Cibersegurança de acordo com a realidade atual, não se limitando a medidas avulsas que nos garantam o cumprimento legal mas não possuam a eficácia necessária, dado que a produção legislativa e a sua execução dificilmente acompanharão o ritmo da evolução tecnológica. Porém, não significa que, por essa razão, se deva diabolizar a tecnologia e o ciberespaço, pois retroceder à era do analógico poderá ser um sinal de desistência em acompanhar a evolução, com efeitos irreversíveis para os dados pessoais.

Esta permanente revolução tecnológica e sociológica que vivemos, vem retirar qualquer fé que se possa ter numa lei atualizada e que é potenciada pelos anacronismos de leis avulsas desadequadas à realidade da época que vivemos, cumprindo ao Direito, sem abdicar dos princípios fundamentais do ordenamento jurídico, tentar acompanhar a (inevitável) inovação tecnológica, aproveitando-a em seu favor sem que isso signifique uma "servidão" tecnológica que estimule a isenção de responsabilidade.

Igualmente, os próprios titulares não se podem eximir da obrigação de proteger os seus próprios dados, não devendo jamais desconsiderar estes em detrimento de outros interesses, sendo importante a consciencialização

das pessoas do valor que têm os seus próprios dados e dos que a elas lhes são confiados e que fortalecerá o grau de exigência.

Tendo em conta que os dados pessoais só terão relevância se permanecerem seguros, significa que a Cibersegurança não deve estar em segundo plano, nem ter um caráter facultativo, só podendo alcançar a sua plenitude através de um grau de usabilidade acessível a quem trata dados pessoais, ficando intrinsecamente dependente da existência de uma *firewall* humana robusta. Entendendo-se que para a efetiva execução do RGPD em consonância com a Cibersegurança o responsável pelo tratamento ter-se-á de colocar no lugar tanto de autoridade de controlo, como de um *hacker* malicioso, mas sobretudo do titular dos dados, para dessa forma avaliar onde se está mais exposto garantindo a segurança dos dados pessoais.

Pese embora não exista uma fórmula mágica, a implementação da Cibersegurança na proteção de dados pessoais depende das organizações que os tratam, bem como, ainda que com menor influência, das legislações existentes, mas sobretudo da sensibilização da sociedade civil.

Seria importante para os nossos dados pessoais que depois do advento da implementação do RGPD não viessem a ser negligenciados, não só pelas organizações, mas por cada um de nós, o que dependerá do nível de consciencialização que se venha a ter sobre o assunto, tendo como finalidade evitar o darwinismo da proteção de dados pessoais em que só sobrevivem os mais aptos e que resulta na exclusão da premissa de ter os dados seguros.

O objetivo deste artigo não é fazer juízos críticos sobre oportunidades perdidas com a legislação implementada, mas sim prever soluções para a segurança (Cibersegurança) dos dados pessoais chegando-se, a duas opções claras, ficar-se reduzido à legislação estando à mercê da inércia e descoordenação do legislador e do menor grau de exigência das autoridades de controlo em relação à Cibersegurança ainda que cumprindo a *accountability* ou ter uma atitude proativa de melhorar a Cibersegurança dos nossos dados pessoais e perceber que o propósito é proteger dados pessoais independentemente do que estabeleçam as regras legais e que possam pecar por defeito.

Deste modo, a chamada "autorregulação", com maior ou menor participação legislativa, tem no que concerne à Cibersegurança e à proteção de dados pessoais um papel decisivo, em especial na perspetiva

das organizações que querem preservar o bom nome, a reputação e a confiança do titular dos dados pessoais.

Tem-se por fundamental que a proteção de dados pessoais e a Cibersegurança tenham sempre por base os direitos fundamentais de cada indivíduo dado que qualquer sociedade terá de ter sempre espaço para a autonomia individual e para os direitos fundamentais de cada um e tal depende muito de cada um de nós e não apenas de qualquer lei ou regulamento. A era digital não pode, em momento algum, deixar-nos cair numa letargia em relação aos nossos direitos fundamentais, os quais são requisitos essenciais para o desenvolvimento de qualquer sociedade.

Posto isto, preconiza-se como política sensata em qualquer ciência que se deve procurar a explicação mais simples que for possível para qualquer problema que estejamos a tentar resolver por isso, implementar a proteção de dados pessoais sem a Cibersegurança parece algo desfasado com a era digital da vida social e laboral atual e que revela a dimensão do perigo por um lado e, por outro, a incapacidade dos meios para o neutralizar e que levou a escrever sobre o tema.

Integrar a Cibersegurança na Proteção de Dados Pessoais não é uma opção, é um imperativo na era digital.