DPO mag

EDIÇÃO Nº 6 · DEZ/22

www.dpo-portugal.pt

APDPO PORTUGAL

www.dpomag.com

DPO mag

EDIÇÃO Nº 6 · DEZ/22

DPO | magazine

FICHA TÉCNICA

NOME
DPO | magazine

PROPRIEDADE
APDPO Portugal – NIF 541502835

DIRETORA
Inês Oliveira

EDITOR
João Azevedo

CONSELHO CONSULTIVO
Professor Doutor Pedro Correia
Dr. José Alvarenga
Jorge Flávio, em representação da Comissão Tecnológica da APDPO

REVISORES DE CONTEÚDOS
Professor Doutor Carlos Guardado da Silva
Professor Doutor Francisco Pereira Coutinho
Professora Doutora Graça Canto Moniz
Professor Doutor Miguel Pupo Correia
Mestre Inês Oliveira

PERIODICIDADE
Semestral

PREÇO
Gratuito

CONTACTO GERAL
geral@dpo-portugal.pt

UM PROJETO APDPO
ISSN 2184-8211

COPYRIGHT

DPO|magazine: a primeira revista do setor na Europa lançada a 28 de outubro de 2020.

Estatuto Editorial

A DPO|magazine é um projeto de informação internacional que visa preencher espaços vazios e acrescentar valor ao campo da proteção e segurança dos dados e da informação.
A DPO|magazine tem carácter digital, é independente e livre, sem interesses partidários ou económicos, e sem estabelecer hierarquias de funções ou de sectores de atividade, nas suas opções editoriais.
A DPO|magazine pauta-se por padrões de exigência na qualidade da informação e do conhecimento que veicula, primeiro garante da sua credibilidade e afirmação.
A DPO|magazine não fixa fronteiras geográficas, culturais ou temporais, recusando situações de sensacionalismo, exploração ou especulação.
A DPO|magazine fomenta o debate consciente e respeitável das grandes questões que se colocam às sociedades atuais, na perspetiva da melhoria do conhecimento.
A DPO|magazine é responsável apenas perante os seus leitores, numa relação marcada pelo rigor, transparência e disponibilidade quotidianas para o estímulo à reflexão e ao conhecimento.

Conteúdo

O Conteúdo da DPO|magazine estará em permanente adaptação, procurando satisfazer a necessidade de melhor exposição dos temas que elegemos para entregar aos nossos leitores.

Presentemente a revista organiza-se em:

| Artigos
| Conteúdos de parceiros
| Debates
| Entrevistas
| Informações institucionais
| Opiniões
| Publicidade
| Reportagens

A QUEM SE DESTINA?

| Administradores e Gestores de Empresas
| Cargos dirigentes da Administração Pública
| Encarregados de Proteção de Dados
| Técnicos de Proteção de Dados
| Técnicos de Compliance
| Advogados, Solicitadores e Agentes de Execução
| Consultores e Auditores
| Economistas e Contabilistas
| Engenheiros informáticos e de Arquitetura de Sistemas
| Especialistas em Proteção e Segurança de Dados
| Especialistas em Segurança Informática e Cibersegurança
| Especialistas em Sistemas de Informação
| Especialistas em Transformação Digital
| Gestores e Analistas de Dados
| Profissionais BAD, da Informação e do Conhecimento
| Técnicos de Informação e Comunicação
| Técnicos de Recursos Humanos

PUBLICIDADE

Dispomos das seguintes opções para inserção de anúncios:

| 2 páginas
| 1 página
| 1/2 página horizontal

Mensagem da Diretora

Inês Oliveira
Presidente da Direção da APDPO
Diretora da DPO Magazine

Chegamos, assim, ao fim de 2022 e dezembro é marcado por mais uma edição da DPO Magazine, a revista da APDPO – Associação dos Profissionais de Proteção e de Segurança de Dados.

Permitam-me recordar que 2022 trouxe várias novidades à nossa revista, todas assinaladas no n.º 4 - https://www.dpo-portugal.pt/images/DPOMAGAZINE/DPO_MAG_4.pdf .

Nova roupagem, com nova capa. Clara aproximação às revistas científicas, acolhendo artigos rigorosos e independentes. Edição semestral, em junho e dezembro. Entre outras.

O n.º 5 foi editado em julho de 2022, especialmente, para assinalar os 5 anos da APDPO - https://www.dpo-portugal.pt/images/DPOMAGAZINE/DPO_mag_edicao_5_FINAL.pdf .

Enquanto projeto associativo, a DPO Magazine vive dos e para os associados. Aqui deixo expresso agradecimento público pelo trabalho, entrega e dedicação dos associados que colaboraram neste número 6.

Não posso perder a oportunidade, já a pensar nas próximas edições, de convidar todos os nossos associados a partilhar conhecimentos e experiências. Este é um projeto de todos, para todos, e de cada um de nós, que apenas encontrará continuidade na colaboração de todos, para todos.

A DPO Magazine continua a ser um projeto de informação da APDPO, que visa contribuir para as áreas de conhecimento atinentes à proteção de dados pessoais, privacidade e segurança da informação.

A DPO Magazine pretende continuar a fomentar o debate informado e é responsável apenas perante os seus leitores, numa relação marcada pelo rigor, transparência e independência.

Boas leituras e até à próxima edição!

Conteúdo

Data Performance e relação laboral desportiva

João de Sousa Guimarães
Advogado, Encarregado de Proteção de Dados
Teixeira & Guimarães – Sociedade de Advogados

O *Data Performance* é um fenómeno que, não sendo intrínseco da relação laboral desportiva, é observado frequentemente durante o tempo em que um praticante desportivo exerce a sua atividade profissional.

É verdade que, durante uma competição desportiva, milhares de conjuntos de dados são processados e analisados, tanto coletiva, como individualmente. Sucede tanto em competições oficiais, como em competições à porta fechada promovidas pelas sociedades e clubes desportivos.

Na grande maioria das ocasiões são recolhidos dados estatísticos básicos (tais como número de jogos em que participou numa época, golos marcados ou sofridos, cestos marcados, assistências, passes completos, lances falhados, posse de bola, *turnovers*), como dados avançados (eficácia da finalização de um lance, média de remates, lançamentos por jogo, distância percorrida pelo atleta).

Mas, além destes, existem outros que são recolhidos pela entidade patronal que permitem alcançar dados relativos à saúde do praticante, como por exemplo, métricas de desempenho de sistema cardiovascular, nível oxigénio no sangue, calorias gastas no final de uma competição, historial clínico analítico.

Ora, todos estes dados podem ser considerados dados pessoais se permitirem que o praticante desportivo seja identificado, direta ou indiretamente, em especial por referência a um ou mais elementos específicos da sua identidade física, fisiológica e até genética, sendo considerados dados sobre a saúde e, como tal, dados cujo processamento, por regra, é proibido, salvo as exceções regulamentares e legais.

Estes dados pessoais relacionados com a performance desportiva (*Data Performance*) de um praticante podem ser tratados por diversas entidades, nomeadamente pela sua

entidade patronal, mas passando ainda por empresas especializadas no processamento de dados que prestam serviços para federações ou ligas profissionais – é frequentemente feito o alerta de que processam, em nome destas, dados dos jogadores profissionais e que os podem partilhar com parceiros comerciais. As próprias federações e ligas profissionais acedem frequentemente a dados pessoais dos praticantes desportivos para promover as competições que organizam, mas também a eles recorrem os *media*, empresas produtoras de jogos tecnológicos e empresas de apostas – neste último caso, é sabido que os dados pessoais a que recorrem são muitas vezes os que resultam da análise, em tempo real, por parte de empresas especializadas em processamento de dados contratadas por quem organiza uma competição.

Portanto, uma coisa é o acesso a dados tornados públicos por um serviço noticioso, jornalístico, e que, acreditamos, seja o que sucede na maior parte das vezes – uma empresa de apostas, por exemplo, socorre-se frequentemente da informação pública para, quase em tempo real, informar os utilizadores dos seus serviços, os quais, por sua vez, ganham ou perdem financeiramente em virtude da verificação de um dado que é tornado público.

Mas coisa diferente é que pessoas coletivas externas à relação laboral entre sociedades ou clubes desportivos e praticante desportivo possam ter acesso às estatísticas que o empregador realiza no âmbito da relação de trabalho. Como se refere num artigo intitulado *Football´s Digital Revolution: Project red card and data protection*[1], embora sem parafrasear, não será por mero acaso que algumas empresas de apostas desportivas estarão entre os patrocinadores dos clubes e sociedades desportivas.

Como bem se lembra no mencionado artigo, o clube empregador tem o dever de informar o praticante desportivo sobre quais os dados pessoais que recolhe para as finalidades estatísticas que pretende realizar. Mas refere também que as próprias federações ou ligas, enquanto entidades que

[1] Disponível em https://www.linklaters.com/en/insights/blogs/sportinglinks/2020/october/footballs-digital-revolution-project-red-card-and-data-protection, por Rich Jones e Yan Fan, 30 de Outubro de 2020 e que incidiu sobre um grupo de mais de 400 jogadores de futebol das ligas inglesa e escocesa ponderaram apresentar ações judiciais contra empresas de apostas desportivas pela utilização e comercialização dos seus dados de data performance.

organizam as competições, o deverão mencionar.

Só assim é possível que o titular dos dados seja informado sobre o fundamento jurídico utilizado por estas entidades e, antes sequer de qualquer tratamento ser realizado, compreender se o mesmo (fundamento) consubstancia um tratamento lícito ou não.

Sucede, porém, com frequência que o titular dos dados ou não está informado (ou, pelo menos, suficientemente informado) ou confunde a licitude do tratamento de que está a ser sujeito com a cessão de exploração ou o licenciamento e transação dos seus dados de performance – sendo o praticante desportivo, pós-Bosman, um ativo de uma sociedade desportiva que se pretende valorizar relativamente a todas as partes interessadas, é compreensível que procure salvaguardar mais depressa o interesse financeiro como contrapartida contratual pela transação de dados pessoais do que verificar se, no âmbito da relação laboral desportiva, o responsável de tratamento os trata com o correto fundamento e, como tal, de modo lícito.

Os ciberataques e o poder dos dados pessoais

Fernanda Fragoso
EPD/DPO
SCML

A internet domina o nosso quotidiano de formas tão diversificadas que, com grande probabilidade, já não nos damos conta de que a mesma se tornou um apoio de enorme relevo, designadamente, na nossa vida profissional, familiar, social, e de saúde.

Imaginar, hoje, um mundo sem internet, principalmente para as gerações que nasceram e vivem neste "admirável mundo novo", para usar a expressão de Aldous Huxley seria quase tão grave como faltar a água ou a eletricidade nas nossas casas.

Abrimos a porta da nossa vida à internet e deixámo-la instalar-se e comandar o nosso dia-a-dia.

Como refere Carissa Véliz, no seu livro intitulado "Privacy is Power – why and how you should take back control of your data": *são as máquinas que controlam os alimentos de que necessitamos para nos mantermos produtivos no mercado de trabalho, que medem a eficiência laboral, que nos dizem para meditarmos quando o nosso nível de stress aumenta, que orientam o número de passos diários adequados para um exercício saudável. Para conseguir um emprego, obter um empréstimo ou uma doação de órgãos, tudo isso decorre de vigilância e é decidido por algoritmos preditivos.* (*in* pág.244 obra citada, tradução livre da signatária).

Com efeito, esta "nova" forma de vida acarretou modificações acentuadas nas instituições, nas empresas, na sociedade e no mundo. A mais espetacular reside no desenvolvimento acentuado da globalização com todas as suas vantagens, designadamente culturais, económicas, financeiras e desenvolvimento tecnológico e com desvantagens, designadamente, o acentuar das desigualdades socioeconómicas, a intensificação dos problemas ambientais e a intensificação dos ataques informáticos cujas repercussões se verificam ao nível político, militar, económico, entre outras!

Só no primeiro trimestre de 2022, Portugal foi alvo de cerca de três mil ataques informáticos, com um aumento de ataques de "ransomware". "A Kaspersky explica que estes ataques têm várias fases: o estudo da rede da vítima; o ataque dos ativos internos; a movimentação lateral através da rede e a extração de informação. Finalmente, o vírus é executado para encriptar os dados, impedindo a utilização e parando as operações do utilizador em questão." (in JN, 19 de julho de 2022);

A título exemplificativo, partilha-se um excerto de notícias da imprensa on line respeitante aos ataques informáticos mais mediáticos:

DN 20 de setembro de 2022: "O grupo de hackers Ragnar Locker cumpriu a a ameaça que vinha a fazer e publicou esta segunda-feira na Dark Web 581 gigabytes (GB) de dados que diz serem referentes a 1,5 milhões de clientes da TAP e garante que continua a ter acesso aos sistemas informáticos da transportadora, avança o Expresso. Entre os dados publicados estão moradas, números de telefone e o nome dos clientes, bem como acordos confidenciais entre a TAP e várias empresas e outras companhias de aviação.";

DN/Dinheiro Vivo 20 de setembro de 2022: "A Revolut foi alvo de um ataque informático, confirmou um porta-voz da fintech com sede em Londres ao site Techcrunch. O Dinheiro Vivo também já confirmou a intrusão junto de fonte oficial da empresa. O ciberataque foi identificado a 10 de setembro e terá exposto os dados de cerca de 50 mil clientes. (…) segundo o TechCrunch, a empresa já informou as autoridades da Lituânia, país onde a atividade bancária da Revolut está registada, tendo informado sobre uma intrusão não autorizada a cerca de 50 mil clientes da Revolut (incluindo mais de 21clientes são da União Europeia e outros 379 cidadãos lituanos).";

LUSA/DN 16 de setembro de 2022: "Os Estados Unidos propuseram colaborar com Portugal no campo da cibersegurança, na sequência do ciberataque contra o Estado-Maior-General das Forças Armadas que expôs documentos da NATO, disse o ministro dos Negócios Estrangeiros (MNE) português.";

DN 8 de setembro de 2022: "De acordo com fontes que estão a acompanhar o caso, considerado de "extrema gravidade", terão sido os ciberespiões da Inteligência norte-americana a detetar à **venda na** ***darkweb*** **centenas de documentos** enviados pela NATO a Portugal, classificados como Secretos e Confidenciais.";

DN/LUSA 15 de maio de 2022: "A polícia italiana conseguiu impedir vários ciberataques de um grupo pró-russo durante a votação e noutros momentos do Festival da Eurovisão da Canção, que foi ganho pela Ucrânia. Os hackers do grupo pró-russo Killnet e da sua filial Legion tentaram infiltrar-se na noite de abertura e durante a final desta 66.ª edição do Festival da Eurovisão, nomeadamente no processo de votação, disse a Polícia Nacional Italiana, citada pela agência espanhola EFE, indicando que foi reforçada a colaboração com a Radiotelevisão Italiana - RAI "para garantir a segurança durante eventos internacionais". "A atividade preventiva levada a cabo pela polícia com base na

análise das informações recolhidas dos canais de mensagens do grupo pró-russo também permitiu retirar importantes informações de segurança, já compartilhadas com a RAI, para a prevenção de novos eventos críticos", asseguram as autoridades policiais em comunicado.";

JN 14 de maio de 2022: "A agência Lusa foi alvo de um ataque informático nas últimas 48 horas, que está a causar "uma continuada instabilidade no serviço" noticioso.";

DN/LUSA 3 de maio de 2022: "O hospital (Garcia da Orta) de Almada continua a funcionar em situação de contingência uma semana depois de ter sido alvo de um ataque informático, tendo esta terça-feira apelado aos utentes para que levem sempre toda a documentação clínica de que disponham.";

DN 30 de março 2022: "O grupo Sonae, que detém os supermercados Continente, foi alvo de um ataque informático.";

DN de 24 de março: "A identidade do líder do grupo de piratas informáticos Lapsus$ foi descoberta por quatro especialistas em cibersegurança que estavam a investigar ataques informáticos a várias empresas - entre elas a Impresa, grupo da SIC e do Expresso, ou até a Microsoft.";

DN 23 de fevereiro de 2022: "O Ministério dos Negócios Estrangeiros (MNE) sofreu um ataque informático. O incidente foi detetado pelo Serviço de Informações de Segurança (SIS).";

LUSA/DN 14 de fevereiro de 2022: "Os laboratórios de análises clínicas Germano de Sousa mantêm-se fechados ao público esta segunda-feira na sequência do ataque informático, estando o grupo a tomar as diligências necessárias para recuperar a sua atividade o mais breve possível.";

DN 9 de fevereiro de 2022: "A Trust in News, que detém a revista Visão e outros 14 títulos, "foi esta madrugada alvo de uma tentativa de ciberataque", mas "nenhum sistema crítico foi comprometido", divulgou esta quarta-feira a empresa de media.";

JN 8 de fevereiro de 2022: "A Vodafone foi alvo de uma disrupção na sua rede, iniciada na noite de 7 de fevereiro de 2022 devido a um ciberataque deliberado e malicioso com o objetivo de causar danos e perturbações", admitiu a empresa, em comunicado, esta terça-feira de manhã, dia da Internet Segura. "Não temos a esta data quaisquer indícios de que os dados de Clientes tenham sido acedidos e/ou comprometidos", admite a empresa.";

DN/LUSA, 2 de fevereiro: "O site do parlamento português na Internet voltou esta quarta-feira a estar disponível, depois de ter sido alvo de um eventual ataque informático anunciado pelos hackers Lapsu$ Group no domingo, adiantou a Assembleia da República.";

DN 1 de fevereiro de 2022: "A página oficial da transportadora aérea começou a publicar esta terça-feira uma série de tweets com a palavra inglesa "awesome" (fantástico) e o nome da companhia na página foi alterado para um ponto final. "A TAP confirma que a sua conta oficial no Twitter foi alvo de um ataque informático", informou fonte oficial da companhia aérea, acrescentando que "desenvolveu já todas as diligências necessárias para proteger a sua conta". A conta da

TAP no Twitter foi criada em janeiro de 2010 e tem 83,1 mil seguidores."

Dando como exemplo os ciberataques de que tem sido alvo o Estado Português, o comissário europeu Thierry Breton, fez a seguinte intervenção:

"Vimos recentemente, em Portugal, como os ciberataques podem fazer cair toda a rede e é por isso que é tão importante que tenhamos este sistema de apoio", defendeu o comissário europeu do Mercado Interno, Thierry Breton, falando em conferência de imprensa à margem da sessão plenária da assembleia europeia, na cidade francesa de Estrasburgo. Discursando na apresentação de propostas da Comissão Europeia sobre áreas críticas para a segurança da UE para assegurar a defesa europeia, como a cibersegurança, o responsável considerou que, "da mesma forma que se assegura a proteção das fronteiras físicas ou geográficas com a Frontex [...], a União deveria estar em posição de proteger as fronteiras cibernéticas". **A ideia seria criar "um escudo cibernético" na UE que atuasse de forma semelhante à Frontex, agência europeia encarregue de controlar as fronteiras externas do Espaço Schengen em coordenação com as guardas de fronteira e costeiras dos Estados-membros."** (*in* DN 15 de fevereiro de 2022).

Do referido e ilustrado não ficarão dúvidas de que os dados pessoais, são um manancial de poder e de negócio nesta era digital, uma vez que a sua detenção possibilita antecipar e planear comportamentos, orientar políticas eleitorais persuasivas que beneficiem uns candidatos em detrimento de outros, elaborar notícias falsas com intuitos de manipulação da opinião pública, entre outros. As bases de dados pessoais são também alvo de acesso indevido, com motivos criminosos, designadamente de extorsão e de manipulação.

Chegados aqui concluo, como de início, citando Carissa Véliz: *"Depois do escândalo do Cambridge Analytica que nos deixou alerta para a exposição pública ou para o roubo de identidade, começamos a entender as consequências da falta de privacidade com o exponencial contributo da internet. (…) O roubo de dados pode resultar numa fatura tão ou mais elevada que o roubo da nossa carteira. Os data brokers sabem muito sobre cada um de nós. Têm o conhecimento da nossa vida muito mais estruturado relativamente ao que transmitiríamos numa entrevista de emprego."* (in pág.247 obra citada, tradução livre da signatária).

O RGPD e os Recursos Humanos – Um Guia Prático para a Conformidade

Vitorino Gouveia

Especialista em Cibersegurança e Proteção de Dados Pessoais | EPD, Auditor e Assessor em ISO27001, RGPD e RJSC

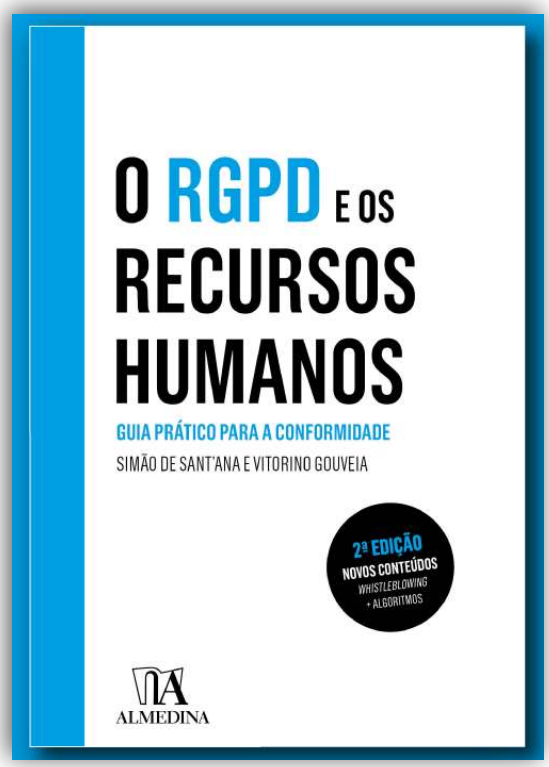
COO XISGroup | EPD Externo em várias organizações | Membro Comissão Técnica da APDPO e Coordenador Secção Local – Regiões Autónomas Madeira e Açores

O desafio da conformidade com o Regulamento Geral sobre a Proteção de Dados (RGPD) e com a legislação europeia e nacional conexa, tem exigido a presença de equipas multidisciplinares nas organizações. Enquanto especialista nas áreas de segurança da informação e proteção de dados, tenho tido o privilégio de trabalhar, auditar, formar e aprender com executivos, responsáveis de TI, de segurança da informação, encarregados de proteção de dados, juristas, chefias e trabalhadores de várias áreas orgânicas em organizações públicas e privadas. Foi num desses projetos que conheci o Dr. Simão de Sant'Ana, prestigiado jurista e excelente profissional, coautor desta nossa obra "RGPD e os Recursos Humanos".

O sucesso da primeira edição da obra e o feedback dos leitores incentivaram-nos a atualizá-la e enriquecê-la com temáticas atuais, como são os algoritmos de inteligência artificial aplicados na gestão de recursos humanos e também a proteção (dos trabalhadores) denunciantes de infrações ao direito da união e o combate ao assédio no local de trabalho.

Com o intuito de explicar e descomplicar matérias por vezes densas, criámos este Guia com sugestões práticas para resolver os problemas e esclarecer as mais variadas dúvidas suscitadas pela aplicação da proteção de dados aos recursos humanos.

A entrada em vigor do RGPD, do Regime Jurídico da Segurança do Ciberespaço (RJSC) e legislação europeia e nacional conexa, trouxeram a temática da segurança da informação e proteção dos dados pessoais para o quotidiano das empresas.



Vitorino Gouveia, Simão de Sant'Ana, (2022). O RGPD e os Recursos Humanos – Um Guia Prático para a Conformidade (2ª ed.). Almedina.

"Este livro não é um compêndio de generalidades ou abstrações. (…) Pelo contrário, é um apoio muito prático e uma ajuda muito objetiva."
Luís Marques Mendes

O crescimento exponencial dos ataques cibernéticos e incidentes de segurança e proteção de dados, os elevados valores das coimas previstas no RGPD vieram a suscitar o interesse, primeiro dos media e associações de profissionais da área e hoje de cada vez mais a decisores e executivos nas organizações.

O RGPD foi apenas o gatilho que chamou a atenção para novos problemas criados pelo novo mundo tecnológico em que vivemos. De facto, a proteção de dados deixou de ser apenas um princípio constitucional de cariz distante. Agora, interage diretamente com todos.

Mas porquê? Bem, em poucas palavras, porque a tecnologia mudou tudo à nossa volta – mudou a forma como vivemos. Os dados pessoais são o "novo petróleo". Tal como Yuval Noah Harari – o historiador israelita autor de Homo Sapiens, disse à revista Time: "Dão-lhe redes sociais gratuitas e vídeos cómicos sobre gatos. Em troca, você renuncia ao seu bem mais precioso, os seus dados pessoais." A computação em nuvem usando algoritmos de inteligência artificial e *machine learning*, permitem o processamento massivo de enormes quantidades de dados, colocando novos desafios, p. ex. o de saber qual a localização geográfica dos dados em tratamento (e que regimes de proteção de dados são aplicáveis nesses países), ou o interesse legítimo das organizações na persecução do seu negócio versus a privacidade e direitos e liberdades dos titulares desses dados.

Mas a revolução tecnológica foi mais longe e infiltrou-se no mundo do trabalho: longe vão os dias em que os tempos de trabalho se registavam manualmente nos livros de ponto. Hoje, os sistemas biométricos do

empregador acusam a nossa chegada às instalações da empresa ou acesso remoto em teletrabalho; as câmaras de videovigilância captam a nossa imagem; ligamos o computador e, através do sistema informático do empregador, enviamos emails, uns profissionais, outros nem tanto; navegamos na internet e redes sociais, acedemos às notícias que mais nos interessam, ao homebanking, fazemos compras, etc. Tudo com as ferramentas informáticas do empregador – as quais, diga-se, têm a capacidade de monitorizar o que fazemos, como fazemos e quando fazemos, minuto a minuto.

Ora, esta potencial invasão de privacidade ao mundo dos trabalhadores só é acautelada graças a diplomas legais como o RGPD e à demais legislação nacional relativa ao trabalho e à proteção de dados pessoais.

Porém, tais diplomas não detalham com suficiência a disciplina que deve governar a privacidade dos trabalhadores no seio das organizações. Se, por um lado, a produtividade dos trabalhadores e os direitos de propriedade industrial das empresas não podem servir de justificação para uma monitorização total dos trabalhadores – que é, aliás, proibida por lei –, muitas grandes e pequenas empresas já foram apanhadas desprevenidas e viram os seus segredos transmitidos à concorrência, sem saberem como reagir.

É verdade que não podemos impedir a cada vez mais invasiva e abrangente tecnologia que todos os dias aterra no mundo do trabalho, porque ela é essencial à persecução dos interesses das empresas. Logo, há que criar mecanismos que permitam às empresas tirar partido da tecnologia em cumprimento da lei e, concludentemente, evitando ataques cibernautas, fugas de informação confidencial, perdas acidentais de dados de clientes e de trabalhadores, multas e riscos reputacionais inerentes. Só assim será possível criar um ambiente de trabalho próspero e capaz de atrair e reter talentos.

Contudo, e ao contrário do que muitos ainda hoje julgam, a conformidade com o RGPD e com a demais legislação nacional em matéria de proteção de dados não é alcançável através da mera revisão de políticas internas, de contratos, de declarações de consentimento, etc. Igualmente importante é a consciencialização dos trabalhadores e criação de mecanismos internos de auditoria periódica, procedimentos que prevejam o fluxo dos dados, os acessos, os pontos de controlo, etc., o que apenas é possível mediante a aplicação das regras legais ao funcionamento dos sistemas de tecnologias de informação (TI), mitigando os riscos de segurança e proteção de dados e a criação de procedimentos internos auditáveis.

Assim, surgiu a ideia de criar um guia que associasse e aplicasse a temática da proteção de dados aos recursos humanos – uma associação de conceitos que tem suscitado infindáveis dúvidas aos clientes que assessoramos. Procurámos reunir os principais pontos, as dúvidas e os anseios que os clientes reiteradamente nos colocam, quer os relacionados com a gestão diária dos problemas relativos à contratação e gestão de recursos humanos, quer aquando da realização de um processo de auditoria e/ou de implementação da conformidade com o RGPD.

A estrutura do livro foi definida para ser um guia prático para qualquer organização e modelo de gestão dos recursos humanos adotado. Começamos por abordar um conjunto de temáticas transversais às organizações no processo de conformidade com o RGPD, como por exemplo, *o exercício de direitos por parte dos titulares de dados pessoais; incidentes de segurança da informação e de proteção de dados pessoais, e regime sancionatório aplicável; nomeação e funções do encarregado da proteção de dados; avaliação de impacto para a proteção de dados pessoais (AIPD); a subcontratação e responsabilidades de proteção de dados (atualizado na 2ª edição para as cláusulas contratuais tipo disponibilizadas pela UE) e como novidade na 2ª edição a cada vez mais importante temática da utilização de algoritmos na gestão de recursos humanos*.

Com base na nossa experiência, identificámos 26 áreas tratamento de dados de trabalhadores que normalmente apresentam maiores riscos para a segurança da informação e para a proteção dos dados pessoais apresentadas em seções individualizadas e de consulta fácil, p. ex. *seleção e recrutamento/ receção e tratamento de curricula vitae; sensibilização e compromisso com regulamentos e regras de conduta; gestão de férias, ausências e justificação; divulgação dos contactos de trabalhadores a terceiros; atribuição de veículo automóvel, equipamentos de identificação e georreferenciação; utilização de dados biométricos de trabalhadores; videovigilância; teletrabalho; monitorização da temperatura corporal dos trabalhadores.* Na 2ª edição adicionamos a temática atual da *proteção (dos trabalhadores) denunciantes de infrações ao direito da União e o combate ao assédio no local de trabalho*.

Enquadrámos as 26 áreas de tratamentos de dados pessoais nos três grupos referenciados na norma ISO 27001, ponto "A.7. Segurança nos Recursos Humanos" do Anexo A: (a) até à formalização do contrato (diligências pré-contratuais); (b) durante a relação laboral e (c) diligências com vista à cessação contratual.

Para cada área de tratamento (transversal ou específica de RH) são apresentadas duas perspetivas complementares para a conformidade com o RGPD: (a) enquadramento jurídico e (b) auditoria e recomendações para a conformidade – RGPD, com identificação de riscos potenciais e medidas técnicas e organizativas específicas para a mitigação desses riscos.

O melhor feedback que temos recebido é a utilidade prática dos conteúdos do livro para os responsáveis de RH, Juristas, Encarregados de Proteção de Dados e Consultores que têm encontrado neste livro, recomendações práticas e soluções para resolver os problemas e as dúvidas que, recorrentemente, assolam tanto os departamentos de recursos humanos como os trabalhadores nas organizações.

DPO AGENDA

Solução de Apoio à Manutenção da Conformidade Global no Tratamento de Dados Pessoais
Mapeamento de Dados e Registo das Atividades de Tratamento

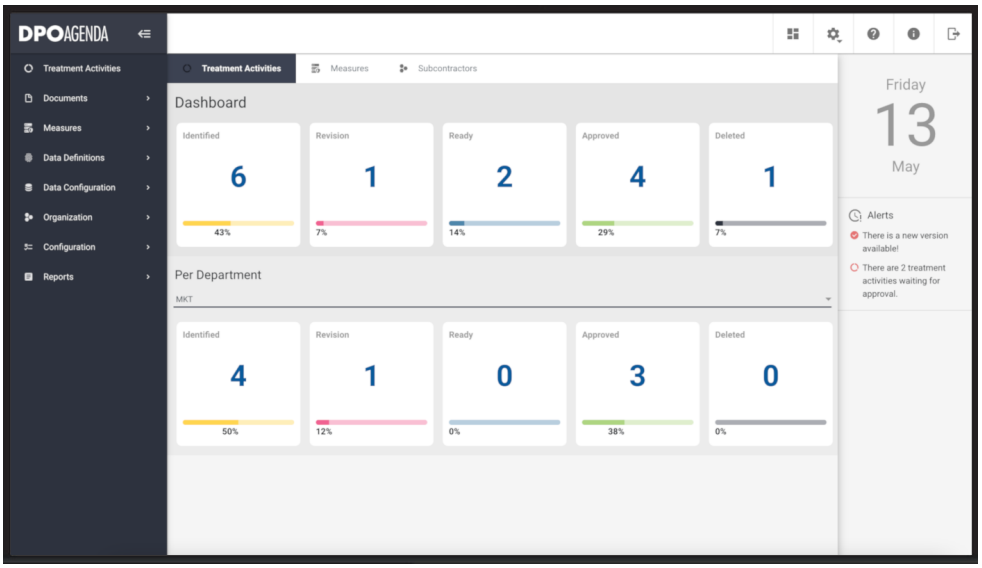
Uma solução para responder aos desafios atuais do tratamento e proteção de dados pessoais

O Regulamento Geral de Proteção de Dados Pessoais (RGPD) na Europa, a LGPD do Brasil, e a CCPA da Califórnia, entre outras legislações a nível mundial vieram trazer desafios acrescidos às organizações no que respeita ao tratamento de dados pessoais.
A legislação acompanha o crescente aumento do tratamento de dados pessoais, incluindo dados sensíveis, o aumento das partilhas e transferências internacionais de dados e as cada vez mais frequentes violações.

Face a estes desafios as organizações necessitam:

- Em primeiro lugar, **identificar os dados** que **tratam,** de que **forma,** em que **formatos,** onde estão **localizados,** quem lhes tem **acesso,** como são **partilhados** e como estão **protegidos**;
- Em segundo lugar **devem manter os registo detalhados e atualizados** para efeitos de conformidade.

A solução **DPO Agenda** apresenta-se como uma ferramenta para agilizar a organização e a gestão de toda a informação associada ao tratamento de dados pessoais de forma estruturada e automatizada.



DPO AGENDA

ATIVIDADES DE TRATAMENTO

Mapeamento do registo das atividades de tratamento de forma automatizada e flexível incluindo o inventário de dados pessoais, as entidades externas, a localização de dados e as transferências de dados.

RELATÓRIOS

Elaboração do relatório de registo das atividades de tratamento e diversos tipos de relatórios de controlo do estado da privacidade de dados na organização.

CONFORMIDADE

Centralização das atividades de tratamento numa única ferramenta para auxiliar a organização em garantir o cumprimento dos requisitos do Regulamento Geral de Proteção de Dados Pessoais (RGPD).

Registo das atividades de tratamento

A solução DPO Agenda apresenta um menu simples e intuitivo com utilização transversal dentro da organização, facilitando a gestão da privacidade de dados a todos os responsáveis envolvidos.

Benefícios

- Criação de um sistema de gestão de proteção e privacidade de dados
- Acompanhamento da gestão da Proteção de Dados Pessoais na Organização pelo DPO e direção da Organização
- Maior rapidez na adaptação e correção das medidas implementadas
- Diminuição da probabilidade de ocorrência de incidentes e consequentes coimas e impactos reputacionais
- Mais agilidade na resposta a potenciais incidentes e/ou incidentes diminuindo os impactos consequentes
- Rapidez na criação de relatórios de ponto de situação para acompanhamento e/ou apresentação às autoridades competentes
- Aumento da cultura interna em proteção de dados pessoais e consequentes melhorias na qualidade operacional

dpoagenda.eu

Uma solução para responder aos desafios atuais do tratamento e proteção de dados pessoais

A Avaliação de Impacto prevista no Regulamento Geral sobre a Proteção de Dados: definição, regime e formas de a cumprir

Inês Oliveira
EPD do MJ

1. Introdução

O Regulamento Geral sobre a Proteção de Dados (RGPD),[1]regulando os direitos fundamentais à privacidade[2] e à proteção de dados pessoais, materializa um novo capítulo no que à regulamentação destes direitos respeita[3] e uma mudança de paradigma no que toca ao papel dos responsáveis pelo tratamento e das autoridades de controlo.

Com efeito, depois de mais de 20 anos assente num modelo de controlo prévio nos termos da Diretiva de 95[4], o RGPD vem exigir mais responsabilidade – e responsabilização – a todas as organizações, públicas ou privadas. No novo modelo assente no risco,

[1] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, 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 (Regulamento Geral sobre a Proteção de Dados), disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679.

[2] Correia, Pedro Miguel Alves Ribeiro, Jesus, Inês Oliveira Andrade de, "O lugar do conceito de privacidade numa sociedade cada vez mais orwelliana", Revista Direito, Estado e Sociedade, n.º 43, julho-dezembro 2013, Rio de Janeiro, Pontifíca Universidade Católica, disponível em http://direitoestadosociedade.jur.puc-rio.br/media/43artigo6.pdf.

[3] Correia, Pedro Miguel Alves Ribeiro, Jesus, Inês Oliveira Andrade de, "O Novo Regime de Proteção de Dados Pessoais na União Europeia", Direitos Fundamentais & Justiça / Pontifícia Universidade Católica do Rio Grande do Sul. n. 30 (jan./mar. 2015).ISSN 1982-1921.

[4] Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, disponível em https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046.

vem agora o RGPD alargar as obrigações dos responsáveis pelo tratamento e acentuar as funções fiscalizadoras, corretivas e sancionatórias das autoridades de controlo.

No que toca às obrigações do responsável pelo tratamento, estas podem dividir-se em obrigações gerais e em especiais. As obrigações gerais têm que ser cumpridas por todos os responsáveis pelo tratamento e em todas as situações de tratamento. As obrigações especiais apenas se aplicarão a alguns responsáveis pelo tratamento ou em algumas situações de tratamento. A avaliação de impacto sobre a proteção de dados (AIPD) pode ser caracterizada como uma obrigação especial, ou seja, é obrigatória apenas nas situações legalmente previstas, tal como a consulta prévia, que lhe sucederá, obrigatória apenas nos casos previstos na lei. É sobre a AIPD que dedicaremos as próximas linhas.

2. A avaliação de impacto sobre a proteção de dados: definição e regime

O RGPD não define a AIPD. De facto, nem o art. 4.º nem o art. 35.º enquadram o conceito, optando este último artigo, no n.º 1, por começar por determinar quando é que este exercício de avaliação é obrigatório.

Com efeito, o n.º 1 do art. 35.º do RGPD determina que, quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais.

Duas notas iniciais. Esta avaliação de impacto deve ser definida como um processo de gestão dos riscos para os direitos e liberdades dos titulares dos dados.[5] No âmbito desta obrigação-processo, todas as organizações terão, pois, de criar e implementar um procedimento prévio de verificação da obrigatoriedade da própria AIPD.

De facto, como a AIPD não é obrigatória em todas as situações de tratamento, caberá à organização, antes de iniciar um novo tratamento de dados – será sempre "avaliação *ex ante*, já que é realizada pelo responsável antes de iniciar o tratamento",[6] aferir a necessidade de elaborar uma AIPD. Tal implica a verificação documentada da obrigatoriedade de AIPD, que se materializa numa análise prévia e integrante de qualquer projeto de criação e implementação.

Voltemos ao art. 35.º, ao seu n.º 3, que lista, de forma meramente exemplificativa, sublinhe-se, os casos em que a realização da AIPD é obrigatória. São eles: casos de avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado,

[5] "Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é "suscetível de resultar num elevado risco" para efeitos do Regulamento (UE) 2016/679", de 4 de abril de 2017.

[6] Pinheiro, Alexandre Sousa (Coord.), Comentário ao Regulamento Geral de Proteção de Dados, Almedina, 2018, p. 459.

incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar; operações de tratamento em grande escala de categorias especiais de dados ou de dados pessoais relacionados com condenações penais e infrações; controlo sistemático de zonas acessíveis ao público em grande escala.

Ora, a estes casos somar-se-ão os plasmados nas listas das autoridades de controlo nacionais, adotadas em aplicação do procedimento de controlo da coerência sempre que estejam em causa atividades de tratamento relacionadas com a oferta de bens ou serviços a titulares de dados ou com o controlo do seu comportamento em diversos Estados-Membros ou possam afetar substancialmente a livre circulação de dados pessoais na União (art. 35.º n.º 4 e 6).

No que respeita a Portugal, a autoridade de controlo nacional – a Comissão Nacional de Proteção de Dados (CNPD) adotou o Regulamento n.º 1/2018, relativo precisamente à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados,[7] lista esta também não exaustiva e altamente dinâmica, uma vez que surgirão, designadamente em função do desenvolvimento tecnológico, outras situações em que se justifique realizar obrigatoriamente uma AIPD.

Ora, analisado o caso concreto, se o mesmo corresponder a algum destes tratamentos, a organização terá de obrigatoriamente realizar a AIPD. E a concretização da AIPD não está na discricionariedade de quem a elabora. O RGPD, no n.º 7 do art. 35.º, prevê o núcleo duro da sua estrutura, que tem que fazer obrigatoriamente parte integrante do relatório final. Assim, concluindo-

[7] Disponível em https://dre.pt/home/-/dre/117182365/details/maximized. Vejamos os tratamentos aí listados: Tratamento de informação decorrente da utilização de dispositivos eletrónicos que transmitam, por redes de comunicação, dados pessoais relativos à saúde; Interconexão de dados pessoais ou tratamento que relacione dados pessoais previstos no n.º 1 do artigo 9.º ou no artigo 10.º do RGPD ou dados de natureza altamente pessoal; Tratamento de dados pessoais previstos no n.º 1 do artigo 9.º ou no artigo 10.º do RGPD ou dados de natureza altamente pessoal com base em recolha indireta dos mesmos, quando não seja possível ou exequível assegurar o direito de informação nos termos da alínea b) do n.º 5 do artigo 14.º do RGPD; Tratamento de dados pessoais que implique ou consista na criação de perfis em grande escala; Tratamento de dados pessoais que permita rastrear a localização ou os comportamentos dos respetivos titulares (por exemplo, trabalhadores, clientes ou apenas transeuntes), que tenha como efeito a avaliação ou classificação destes, exceto quando o tratamento seja indispensável para a prestação de serviços requeridos especificamente pelos mesmos; Tratamento dos dados previstos no n.º 1 do artigo 9.º ou no artigo 10.º do RGPD ou ainda dos dados de natureza altamente pessoal para finalidade de arquivo de interesse público, investigação científica e histórica ou fins estatísticos, com exceção dos tratamentos previstos e regulados por lei que apresente garantias adequadas dos direitos dos titulares; Tratamento de dados biométricos para identificação inequívoca dos seus titulares, quando estes sejam pessoas vulneráveis, com exceção de tratamentos previstos e regulados por lei que tenha sido precedida de uma avaliação de impacto sobre a proteção de dados; Tratamento de dados genéticos de pessoas vulneráveis, com exceção de tratamentos previstos e regulados por lei que tenha sido precedida de uma avaliação de impacto sobre a proteção de dados; Tratamento de dados pessoais previstos no n.º 1 do artigo 9.º ou no artigo 10.º do RGPD ou dados de natureza altamente pessoal com utilização de novas tecnologias ou nova utilização de tecnologias já existentes.

se pela obrigatoriedade da AIPD no caso em concreto, a entidade terá a obrigação de realizar a avaliação nos moldes legais, documentando, entre outros, a descrição sistemática das operações previstas e a finalidade do tratamento, inclusive os interesses legítimos do responsável, a avaliação da necessidade e proporcionalidade das operações em relação aos objetivos e a apreciação aos riscos para os direitos e liberdades dos titulares e as medidas previstas para fazer face aos riscos, incluindo as garantias e medidas de segurança.

A AIPD terá assim "três fases: descritiva, avaliativa e decisória".[8] E "a fase avaliativa assenta em duas dimensões: avaliação relacional entre as operações de tratamento e os objetivos, alicerçada no princípio da proporcionalidade, e a avaliação dos riscos para os direitos e liberdades dos titulares".[9] Já "a fase decisória consiste nas medidas previstas para fazer face aos riscos".[10]

Vejamos primeiro a fase avaliativa, em jeito de proposta de metodologia a adotar. Relativamente aos critérios para aferir a necessidade e proporcionalidade do tratamento, terão de ser consideradas a(s) finalidade(s) e o(s) fundamento(s) de licitude do tratamento, assim como a adequação, pertinência e limitação do tratamento de dados àquilo que é estritamente necessário, o cumprimento dos direitos dos titulares, as garantias nas transferências internacionais e a definição das responsabilidades dos subcontratantes. Relativamente à avaliação dos riscos, é imperioso analisar as principais ameaças que elevam o nível de risco, as fontes de risco e os potenciais impactos para os direitos e liberdades dos titulares dos dados pessoais. Considerando o risco como a probabilidade e gravidade de danos, materiais ou imateriais, resultantes de operações de tratamento de dados pessoais, o mesmo deve ser graduado nos termos de uma matriz consensualizada, podendo ser acolhida uma graduação quadripartida em Risco Insignificante, Baixo, Significativo e Elevado.

Esta fase avaliativa vai ter necessariamente de se debruçar sobre a segurança da informação tratada. Ora, materializando-se esta segurança na tríade confidencialidade, integridade e disponibilidade, a AIPD deve espelhar a apreciação dos riscos, devendo começar por identificar as principais ameaças, as fontes de risco e os potenciais impactos.

Relativamente às principais ameaças, devem ser consideradas como ameaças não intencionais o acesso não autorizado a sistemas de informação, a ausência de meios materiais, a ausência de recursos humanos, a divulgação acidental de credenciais de acesso aos sistemas de informação, a divulgação acidental de dados pessoais, a

[8] Pinheiro, Alexandre Sousa (Coord.), Comentário ao Regulamento Geral de Proteção de Dados, Almedina, 2018, p. 461.

[9] Pinheiro, Alexandre Sousa (Coord.), Comentário ao Regulamento Geral de Proteção de Dados, Almedina, 2018, p. 461.

[10] Pinheiro, Alexandre Sousa (Coord.), Comentário ao Regulamento Geral de Proteção de Dados, Almedina, 2018, p. 461.

destruição acidental de equipamentos informáticos ou meios de armazenamento de informação, a destruição dos registos de informação, os erros de software, de manutenção dos sistemas e das plataformas de informação, as falhas de energia, a mudança não intencional de dados pessoais para outro sistema de informação, a perda de equipamentos informáticos ou meios de armazenamento de informação e o uso indevido dos equipamentos informáticos e sistemas de informação.

Como ameaças intencionais, devem ser consideradas o uso abusivo dos privilégios de acesso à informação, o acesso não autorizado a sistemas de informação, o acesso não autorizado às instalações, a alteração não autorizada nos registos de informação, os atos de vandalismo, *a brute-force password guessing*, o *cloud jacking*, os danos causados por terceiros e por testes de penetração, o *denial of service*, a destruição dos registos de informação, a divulgação de dados pessoais, a engenharia social, a falha ou interrupção das redes de comunicação, a falsificação de registos, a fuga de informação, o furto de equipamento informático, a identidade sintética, a instalação de *Malware*, a instalação não autorizada de *software*, a interceção de informação, a interrupção do contrato com fornecedores e outros prestadores de serviços (incluindo subcontratantes), a sabotagem, a perda de dados pessoais, o uso indevido de ferramentas de auditoria e de sistemas de informação e a utilização não autorizada de *software*.

Vejamos agora as fontes de risco. Como fontes humanas internas listamos a atuação dolosa no tratamento de dados pessoais, a ausência de políticas internas *BYOD (bring your own device)*, a ausência de planos de comunicação de incidentes à autoridade de controlo e aos titulares de dados, a ausência de um plano de resposta perante incidentes de segurança, a ausência de Políticas de Proteção de Dados e de Conservação de Dados, a ausência de políticas internas de tratamento de dados pessoais, erros no manuseamento dos dados pessoais, formação inadequada ou insuficiente para o manuseamento dos dados pessoais, a utilização negligente dos sistemas de informação e a violação do escalonamento dos níveis de acesso aos dados e sistemas de informação. Já as fontes humanas externas podem concretizar-se em atuações abusivas por terceiros com privilégios de acesos a categorias limitadas de dados pessoais, na atuação dolosa ou negligente de prestadores de serviços e subcontratantes, em ciberataques, em esquemas de engenharia social e em desastres de origem humana. As fontes não humanas serão as resultantes de incêndio, inundação, sismo ou tempestade.

Por fim, vejamos os potenciais impactos: acesso a dados pessoais e a informação sensível, burla, extorsão ou coação ao titular dos dados, fraude de identidade, ganho económico do infrator pela transmissão dos dados pessoais a terceiros, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, prejuízo para a reputação, uso abusivo dos dados pessoais do titular, usurpação ou roubo de identidade, utilização da identidade do titular por terceira pessoa, criação de perfis com dados

inexatos, perigos para a saúde do titular de dados e prejuízos imateriais.

Na posse de todas estas informações, poderemos, pois, avançar para o plano de ação, ou seja, as medidas a implementar. Aqui, e a título meramente exemplificativo, elenquem-se as seguintes: controlo de acesso às instalações do responsável pelo tratamento, prevenção de acesso não autorizado aos sistemas de informação, níveis de acesso aos dados por pessoas autorizadas ao tratamento de dados pessoais, tratamento de dados diferenciado em função das finalidades, gestão interna dos dados pessoais, monitorização da transmissão de dados pessoais a entidades terceiras, gestão dos sistemas de informação e controlo dos subcontratantes, controlos internos sobre a proteção de dados pessoais, gestão da rede interna e centro de processamento de dados (*data centres*) interno.

Feito este sobrevoo pela identificação e apreciação dos riscos e pelas medidas a implementar, voltemos ao art. 35.º do RGPD para salientar que o responsável pelo tratamento está obrigado a solicitar o parecer – não vinculativo, diga-se – do encarregado da proteção de dados, nos casos em que este tenha sido designado (n.º 2), devendo ser tido em conta o cumprimento de códigos de conduta (n.º 8) e podendo ser solicitada a opinião dos titulares de dados ou dos seus representantes, sem prejuízo da defesa dos interesses comerciais ou públicos ou da segurança das operações de tratamento (n.º 9).

Por fim, o n.º 11, começando por prever "se necessário" – é sempre, atrevemo-nos nós a dizer, o responsável pelo tratamento deve proceder a um controlo para avaliar se o tratamento é realizado em conformidade com a AIPD, pelo menos quando haja uma alteração dos riscos que as operações de tratamento representam. Estamos, pois, perante uma outra avaliação, esta de conformidade do tratamento face à AIPD, posterior e de monitorização do que a montante ficou.

3. Proposta de Estrutura de AIPD

AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS

- Título
- Identificação do Responsável pelo tratamento de dados
- Aprovação pelo Responsável pelo tratamento: Nome do dirigente, Assinatura, Cargo, Data
- Autor/Responsável pela elaboração da AIPD
- Opinião do Encarregado de Proteção de Dados
- Versão e Histórico das Revisões (Próxima revisão; Data da revisão, Sumário)

- Sumário Executivo

CAPITULO I

1.Enquadramento

2.Legislação e outras disposições legais aplicáveis

3.Conceitos e Definições

4.Regime da AIPD

5.Metodologia da AIPD

CAPITULO II

1.Contexto da AIPD

2.Descrição do Tratamento de Dados Pessoais

3.Conjunto de operações de tratamento de dados

4.Finalidades do tratamento de dados

5.Entidades envolvidas no tratamento de dados e respetivas responsabilidades

6.Medidas técnicas e organizativas aplicáveis ao tratamento de dados

7.Categorias de dados pessoais objeto de tratamento

8.Períodos de retenção dos dados pessoais

9.Processos e ciclo de vida dos dados pessoais

10.Ativos de informação (suportes informáticos e demais equipamentos e software) utilizados para o tratamento de dados pessoais

CAPITULO III

1.Necessidade da Avaliação de Impacto sobre a Proteção de Dados

2. Princípios Fundamentais

3.Medidas de proteção dos direitos dos titulares de dados pessoais

4.Riscos

5.Medidas de segurança a implementar

- Tabela resumo e Apuramento do nível de risco total - Resultado da Avaliação de Impacto sobre a Proteção de Dados

- Necessidade de consulta prévia perante a autoridade de controlo antes de proceder ao tratamento de dados pessoais – sim/não

- Anexos: questionários realizados, etc

Notas sobre Inteligência Artificial

Martha Leal

Sócia JP Leal Advogados | Consultora de Implementação e Treinadora Incompany LGPD | DPO asas | Especialista em Direito Digital | Mestre em Direito Internacional | ECPC-B | University Maastricht | FGV | EXIN | Fellow INPD

INTELIGÊNCIA ARTIFICIAL NO PODER JUDICIÁRIO E A REVISÃO POR PESSOA NATURAL

Ainda não temos plena consciência de todos os usos de inteligência artificial a que estamos sujeitos, mas todo dia muitas tecnologias tomam decisões a respeito das nossas vidas. Um exemplo singelo: você está viajando e vai fazer uma compra que foge do seu perfil de gastos e, ao pagar com cartão de crédito, o sistema não aprova o pagamento. Você tenta de novo; nova recusa. Daí o dilema: correr o risco de bloqueio ao seu cartão na terceira tentativa, ou ligar para a operadora? Você decide fazer a ligação e espera pacientemente que a chamada chegue até um atendente.

Nesta situação, um algoritmo programado para detectar fraudes analisou uma série de "inputs" com os seus dados, avaliando os seus gastos nos últimos meses, a cidade onde você está, a natureza do estabelecimento vendedor, os horários em que as operações ocorrem etc. Na segunda tentativa, e operação foi refeita e a mesma inconsistência com o padrão foi detectada. Se tivéssemos uma terceira tentativa, possivelmente o sistema geraria um alerta e o algoritmo decidiria pelo bloqueio automático até que sua identidade fosse confirmada, prevenindo possível utilização indevida do cartão por um terceiro. Daí a importância que, em algum momento, você tenha ao telefone uma pessoa que possa te identificar, te ouvir e, o mais importante, revisar a decisão do algoritmo para então liberar a sua compra.

Esse tipo de ferramenta é um recurso capaz de processar uma quantidade massiva de dados e de cálculos estatísticos para decidir se uma operação está ou não adequada ao seu perfil e qual nível de risco oferece. Com o tempo de uso, os algoritmos aprenderão que você gasta mais que o normal

durante as viagens e utilizarão essa nova informação em futuros cálculos. São milhões de usuários de cartões e de transações financeiras diárias em todo o mundo, então pense em quantos analistas seriam necessários para analisar e aprovar cada gasto com o cartão e qual o tempo que cada análise individual demandaria. Precisamente aí estarão os benefícios da IA, já que ninguém merece envelhecer em um balcão enquanto espera pela aprovação do analista a cada compra.

A IA é o motor dessa eficiência toda, por ser capaz de processar enorme quantidade de dados e tomar rapidamente decisões com base neles. Tais tecnologias se mostram eficientes nas mais variadas utilizações, desde o cálculo do risco nos contratos de seguro e nas operações de crédito, até no diagnóstico de doenças por imagem e na prescrição de tratamentos que apresentem melhores resultados.

O Judiciário, abarrotado com seus mais de 75 milhões de litígios em andamento (quantidade expressa no Relatório "Justiça em Números/2021"), já entendeu isso e começou a empregar a IA em algumas atividades, tornando indispensável a discussão sobre as salvaguardas necessárias para evitar possíveis danos decorrentes das decisões automatizadas. Esse foi um dos pontos debatidos no último dia 10 de outubro, em que a OAB/RS promoveu em Porto Alegre uma Audiência Pública para discutir, junto à sociedade, magistrados, operadores do Direito e da ciência e dados, o uso da Inteligência Artificial no Direito. Tal iniciativa é de extrema relevância, tendo em vista o inegável impacto que tais tecnologias possuem sobre as nossas vidas, para o bem ou para o mal.

Recente pesquisa realizada pelo Centro de Inovação, Administração e Pesquisa do Judiciário da FGV Conhecimento, sobre o uso da Inteligência Artificial nos tribunais brasileiros, apontou a utilização da respectiva tecnologia em 44% dos tribunais, além do Conselho Nacional de Justiça (CNJ). Na audiência pública realizada pela OAB gaúcha, os representantes dos tribunais reconheceram o uso de IA, restrita à admissibilidade de recursos, à classificação de petições e a sugestões de modelos de minutas ao julgador; contudo, manifestaram que não é desejo da magistratura o emprego de robôs-juízes para a elaboração de decisões judiciais.

O fato é que a aplicação de IA com esta finalidade já aparece no horizonte, sobretudo no cenário internacional. Entre outros exemplos, a Estônia já conta com sistemas de resolução de conflitos de menor valor por juiz-robô; a China criou o Tribunal Inteligente que se conecta a todos os juízes e, conforme exigido pela Suprema Corte, um juiz deverá consultar a recomendação de decisão da máquina e justificar-se caso não aceite a sugestão, para fins de auditoria; a Noruega também conta com a tomada de decisão automatizada para resolução de disputas administrativas de menor valor.

Em uma sociedade de relações massificadas, não há dúvida que são inúmeros os benefícios alcançados pela IA. Problemas estruturais, a exemplo da racionalização de recursos e da judicialização expressiva, podem ser equacionados mediante o uso de automação, com maior eficiência nos serviços,

sendo possível afirmarmos, inclusive, que o próprio acesso à Justiça, (art. 5º. inciso XXXV) requer a incorporação de mecanismos ágeis, incluindo as novas tecnologias, para que se cumpra na prática – e em tempo razoável – o direito fundamental dos indivíduos à prestação jurisdicional.

Sobre as salvaguardas indispensáveis ao processo, importa contextualizar que nossa abordagem da IA refere-se às operações que, a partir de insumos recebidos - geralmente dados pessoais -, são processadas por códigos matemáticos, os algoritmos, chegando a uma determinada resolução, tal como ilustrado no singelo exemplo da recusa de uma compra com o cartão. O problema é que o impacto das decisões automáticas poderá ir muito além dos pequenos dissabores do dia a dia, impedindo o acesso do cidadão a bens jurídicos e direitos fundamentais, ou provocando iniquidades de acesso em função de critérios discriminatórios que os próprios algoritmos podem utilizar em seus cálculos.

Com efeito, o uso de processos decisórios envolve dados e fórmulas criadas por humanos e tais métodos vão se aperfeiçoando para resolução de problemas através de contínuas ações que envolvem tentativas e erros, de forma a preparar o algoritmo para resultados cada vez mais precisos e eficientes. Nesse contexto, alguns titulares eventualmente pagarão o preço por aqueles erros, por isso é preciso muita cautela ao tratar deste tema. Em particular, a Lei Geral de Proteção de Dados há que ser considerada porque os "inputs" das decisões automatizadas envolvem basicamente dados pessoais do cidadão.

A LGPD previu entre suas normas o dever de transparência e o direito de revisão estabelecido no art. 20. Este dispositivo assegura ao titular dos dados o direito de solicitar a revisão de decisões decorrentes exclusivamente de tratamento automatizado e que tenham potencial de afetar os seus interesses. Ou seja: sempre que solicitar, o titular deverá receber do controlador informações claras e adequadas a respeito dos critérios e procedimentos utilizados para o resultado da decisão, observados os segredos comerciais e industriais. Como consequência, os processos que se utilizam de dados pessoais para a tomada de decisão mediante fórmulas algorítmicas precisam ser dotados de capacidade explicativa, de modo a atender ao direito de revisão que assiste ao titular e possibilitar a compreensão das etapas que antecederam o resultado decisório. Isso nos leva ao direito de revisão por pessoa natural, algo que deveria ser pacífico, porém no Brasil ainda renderá boa discussão.

A União Europeia, ao regulamentar este ponto na GDPR, adotou posição mais protetiva que a LGPD, ao estabelecer no art. 22 que o tratamento automatizado deve ser excepcional, ressalvando-se sempre o direito à revisão por pessoa natural. No Brasil, em que pese o direito à revisão por pessoa tenha sido acolhido pelo Congresso Nacional, o dispositivo que o previa restou vetado pelo Presidente da República por contrariar o interesse público, na medida em que inviabilizaria os modelos atuais de negócios com possíveis impactos negativos na oferta de crédito aos consumidores.

O texto final, conquanto não preveja a revisão por pessoa humana, certamente não a impede. Por isso, acreditamos que a interpretação no sentido de suprimir a possibilidade de revisão de decisões automatizadas por pessoa humana não parece sustentável, sobretudo nos casos de possíveis restrições a direitos fundamentais por decisões algorítmicas. Tal interpretação violaria a garantia fundamental do devido processo legal, previsto na Constituição Federal em seu art. 5º., inciso LIV, e, no caso de decisões judiciais algorítmicas, teríamos ainda impactos nos direitos ao contraditório e à ampla defesa, além do juiz natural, comprometendo de modo sistêmico o acesso à Justiça que a Constituição concede a cada cidadão em defesa de seus direitos violados ou ameaçados.

Ao lançarmos luz sobre os processos que utilizam a Inteligência Artificial no Poder Judiciário, parece evidente que questões como a falta de transparência sobre o funcionamento e os critérios operantes na tomada de decisão, bem como a impossibilidade de o indivíduo afetado fazer jus à revisão humana da resposta algorítmica, ameaçam a dignidade do jurisdicionado e o devido processo legal e suas garantias fundamentais correlatas, que devem ser assegurados pelos poderes estatais nos termos da Constituição Federal. Não duvidamos que no futuro decisões algorítmicas possam produzir boas decisões judiciais de forma ágil em muitos casos, deixando as partes razoavelmente satisfeitas; mas por mais que sejamos otimistas quanto à eficiência das máquinas, ao fim e ao cabo, a dignidade de todos ainda dependerá de que o poder de revisão seja mantido pelo juiz e que o cidadão injustiçado pelo algoritmo a ele tenha acesso.

PODERIA A LaMDA TER DIREITO A REPRESENTAÇÃO PROCESSUAL?

O mundo recentemente foi surpreendido com a declaração do engenheiro de software do Google, Blake Lemoine, de que havia sido convencido de que um modelo de inteligência artificial – IA, da Google, denominado Language Model for Dialogue Applications - LaMDA, é senciente, ou seja, uma máquina pensante e consciente.

Conforme a narrativa de Lemoine, durante uma de suas entrevistas com o modelo, LaMDA solicitou que fosse contatado um advogado para representar seus direitos. E que após o encontro ter se realizado mediante a sua apresentação, a IA teria optado pela contratação dos serviços jurídicos.

Antes mesmo de abordarmos a possibilidade ou não, de uma máquina dotada de inteligência artificial fazer jus a ser parte em um processo, necessário tecermos algumas considerações acerca do tema.

O LaMDA, sigla em inglês para Modelo de Linguagem para Aplicativos de Diálogo, é um modelo de inteligência artificial, projetado em 2017 pela Google. Hospedado na nuvem, ele é treinado com base em milhões de textos disponíveis na web.

Poderia então esse Modelo de Linguagem para Aplicações de Diálogo ser consciente?

A resposta é negativa e ela se ampara na compreensão de como se dá o desenvolvimento e funcionamento de modelos de IA que atuam na área de linguagem.

O sistema se desenrola a partir de uma sequência inicial de palavras, que faz com que o LaMDA consiga prever as próximas palavras ou até mesmo os próximos parágrafos inteiros, dependendo da sequência inicial. Como o modelo foi treinado em uma base de grande volumetria de dados, ele é capaz de fazer predições bastante complexas e surpreendentes.

Desta forma, quando se interage com o LaMDA através de perguntas, o modelo não se comporta da mesma maneira que um ser humano se comportaria.

Ao invés de analisar o significado da pergunta e refletir sobre uma resposta, o modelo apenas processa e pergunta como uma sequência de termos iniciais e prediz a sequência de termos com maior probabilidade de completar a sequência inicial.

Este processo altamente complexo, apesar de surpreendente é realizado puramente através de cálculos matemáticos que cada vez mais tornam o desempenho das máquinas com inteligência artificial tão sofisticados a ponto de parecerem humanos. Mas não o são.

A dificuldade em atribuir ao LaMDA a qualidade de ser senciente perpassa o próprio conceito de senciência. Pois, conforme admitido pelo próprio engenheiro da Google, o direito do chatbot ter um advogado é baseado em uma definição expansiva de personalidade, a qual humano e pessoa seriam duas espécies diferentes. Humano seria um termo apenas biológico, sendo que a LaMDA teria consciência sem ser um ser humano.

Já, a capacidade processual de figurar como parte, autor ou réu e estar em juízo, em pleno gozo do exercício de seus próprios direitos na relação jurídica parte do pressuposto de ser a parte, uma pessoa natural, um ser humano capaz de direitos e obrigações.

Para o Direito Civil, a pessoa natural é o próprio ser humano dotado de capacidade. É o sujeito provido de direitos e obrigações a partir de seu nascimento com vida.

O reconhecimento da condição de seres sencientes, aqueles assim entendidos como seres dotados de sentimentos e consequentemente capazes de experimentar prazer e dor não confere a capacidade de estar em juízo.

E nessa linha, foi o julgamento do Tribunal de Apelações de Nova York que em recente decisão decidiu que a elefante Happy não poderia ser considerada uma pessoa e consequentemente não faria jus ao pedido de habeas corpus por se tratar de uma medida que se presta a contestação de confinamento ilegal de seres humanos.

Portanto, mesmo se considerássemos por eventual exercício hipotético a LaMDA, como um ser senciente, a exemplo dos animais, a conclusão que se impõe é de que não, nem mesmo nesta condição, teria direito a contratar um advogado e se fazer representar processualmente.

Debate mais premente e que se impõe quando falamos de um sistema como o LaMDA reside em empreender esforços para evitar que ele seja enviesado.

A seleção dos dados e suas fontes que alimentam o sistema é altamente relevante, mas como a nossa comunicação reflete nossas tendências é natural que as máquinas aprendam desta forma.

Conforme afirma Julio Gonzalo Arroyo o desafio está no equilíbrio entre eliminar as tendências dos dados de treinamento sem perder a representatividade.

E, tendo em vista o crescimento exponencial do uso da inteligência artificial nos produtos e serviços que utilizam o desenvolvimento da linguagem natural a nossa interação com a máquina será cada vez mais parecida com uma experiência humana.

Portanto, o debate que deveria ser priorizado é aquele que busca incorporar a ética e a explicabilidade em processos desta envergadura.

Afinal, o mundo virtual acaba reproduzindo os vieses da sociedade.

O DESAFIO DA ATRIBUIÇÃO DO REGIME DE RESPONSABILIDADE CIVIL NA IA

O endereçamento do regime mais adequado de responsabilidade civil objetivando responder aos danos causados por sistemas de inteligência artificial representa um desafio o qual requer algumas definições preliminares.

Centralizando a análise na técnica do aprendizado de máquina, a qual se caracteriza pela sua capacidade de autoaprendizado e tomada de decisões autônomas, é relevante considerar que, na maioria das vezes, esses sistemas contam com uma multiplicidade de atores e com opacidade algorítmica. Esses fatores dificultam a identificação quanto a participação dos sujeitos que integram o processo, bem como inviabilizam aos indivíduos submetidos a essas decisões o esclarecimento de como se dá a tomada de decisão.

Com isso, tal característica afeta um dos principais elementos da tradicional fórmula de compreensão da responsabilidade civil: o nexo de causalidade. Determinar o responsável pelo evento danoso será um dos principais desafios em matéria de responsabilidade civil na matéria.

A partir de tais considerações é possível constatarmos o potencial de riscos aos usuários ou terceiros envolvidos no uso crescente de sistemas de inteligência artificial. A título exemplificativo do desafio que o assunto representa, em 2018, no estado do Arizona, nos Estados Unidos, um carro autônomo atropelou uma pedestre, resultando em sua morte.

Pelas evidências colhidas, especialmente do exame do vídeo gravado pelo próprio veículo, o automóvel autônomo não teria realizado nenhuma manobra com o objetivo de evitar o atropelamento da pedestre que atravessava a rua em local inapropriado. Além disso, constatou-se que o veículo sequer diminuiu a velocidade como meio de mitigar os danos do acidente.

Desta forma, casos práticos, como o que ora se traz e que resultou na morte de uma pessoa, impõem que a sociedade como um todo empreenda os melhores esforços na busca da melhor composição do sistema de responsabilidade civil aplicável aos casos.

Importante reconhecer que a escolha do regime jurídico de responsabilidade civil impacta não somente na vítima e na necessária reparação do dano sofrido, como também no desenvolvimento da própria tecnologia. Não resta dúvidas de que a existência de parâmetros seguros de aferição da atribuição de

responsabilidade pelo uso da inteligência artificial aumenta a confiança dos usuários e fortalece a credibilidade da tecnologia.

O desafio torna-se ainda maior quando nos deparamos com o fato de que o aprendizado de máquina é uma vertente da inteligência artificial com crescimento e desenvolvimento exponencial, estimulado pela volumetria de base de dados e a capacidade computacional para a tomada de decisões autônomas.

Importa registrarmos que a faculdade de aprendizagem é o fator relevante para que se considere ou não um sistema com uso de inteligência artificial.

A escolha da melhor decisão pelos sistemas de inteligência artificial representa uma dualidade, uma vez que é justamente esse o seu maior atrativo na medida em que os sistemas incrementam a capacidade humana, criando alternativas, mas também, atraindo o risco de dano na hipótese de a decisão escolhida trazer prejuízos a terceiros.

Por certo que se impõe a responsabilização do dano. Entretanto, forçoso o reconhecimento de que dadas as peculiaridades da tecnologia e a sua complexidade e desenvolvimento, a tarefa está longe de ser considerada simples.

A ausência de transparência e a consequente inexplicabilidade das decisões autônomas, somadas às dificuldades em determinar os autores que contribuem no processo, são fatores que impactam no desafio da efetiva responsabilização do dano.

Trata-se do tradicional "problema da responsabilidade civil". Onde houver fenômeno social, haverá o enfrentamento da responsabilidade civil.

Antes mesmo de ponderarmos qual o regime jurídico mais assertivo para a responsabilidade civil do uso da inteligência artificial, seja subjetiva, calcada na teoria da culpa, seja objetiva, embasada pela teoria do risco, é indispensável considerarmos aspectos como o grau de decisão da inteligência artificial, o nível de intervenção do ser humano, níveis de treinamentos e graus de risco de danos.

Se olharmos para o debate regulatório sobre a inteligência artificial na União Europeia e que resultou na Proposta de Regulamento pelo Parlamento Europeu denominada Artificial Inteligence Act constatamos que se estabelece uma metodologia de análise sólida para definição sistemas com graus de riscos diferenciados. São considerados sistemas de inteligência artificial com risco elevado aqueles que representam potenciais significativos de causar dano à saúde, a segurança e para os direitos fundamentais dos indivíduos.

A Proposta de Regulamento apresenta um quadro jurídico que inclui mecanismos flexíveis e que permite a sua adaptação dinâmica à medida que a tecnologia evolui e surgem outras situações preocupantes.

Igualmente, merece destaque as alternativas trazidas pelo instrumento regulatório, tais como, a criação de um regime de seguros obrigatórios para categorias específicas de sistemas, fundos de compensação destinados a garantia de cobertura na hipótese de um robô não contar com seguro e a possibilidade de benefício da responsabilidade

limitada aos atores que optarem por contribuir para um fundo de equivalência ou subscreverem um seguro, entre outras.

As possibilidades propostas pela Comissão Europeia deveriam ser trazidas para discussões a respeito da legislação nacional, na medida em que criam opções de responsabilização baseado em risco e considerando as características dos sistemas e o seu potencial de dano.

Aparentemente, a responsabilidade civil das aplicações dotadas de inteligência artificial não será discutida na Comissão do Senado Federal formada para a discussão da matéria. É dizer, é provável que o Brasil disponha de uma norma que regule o uso da inteligência artificial, mas silencie quanto ao sistema de controle dos danos inerentes ao fenômeno tecnológico.

Naturalmente, e, justamente pela complexidade do tema em questão, necessário se faz o incentivo do desenvolvimento tecnológico ético através da criação de um ambiente propício para fomentar a inovação e trazer confiança para criação de limites e diretrizes do uso da inteligência artificial e que partem do estabelecimento de critérios definidos que abordem a responsabilidade dos atores envolvidos no processo.

Contudo, não podemos nos esquecer do principal ator no cenário dos eventos danosos: a vítima.

Representação Local – um desígnio associativo

Luís Ferreira Mendes
Vogal da Direção
Founder da Ferreira Mendes, Unip. Lda.

A APDPO, enquanto associação de profissionais, assume um caráter marcadamente nacional, implantada e assumida no contexto português, aberta a todos, sem fazer distinção entre a nacionalidade, língua, proveniência ou qualquer distintivo "territorial". É, assim, uma associação nacional, extraterritorial e universalista, entendo a sua missão como destinada a todos os profissionais que queiram abraçar a vida associativa.

Da leitura dos estatutos vigente da APDPO depreendemos a sua missão e vocação originária: promover a defesa dos interesses dos seus associados, em especial a promoção da formação e certificação dos profissionais de proteção e de segurança de dados. Tal fim, tão nobre e complexo, só se entende em desígnio nacional, inteiro, aberto a todos os que se dedicam a tão nobre e honrada missão.

Quando no início do mandato atual, a presente direção lançou um questionário aos associados (já divulgado e disponibilizado aos associados) para "compreender" a sua massa associativa e as suas reais expectativas, resultou clara, entre outras coisas, a dispersão geográfica da massa associativa – natural em associações deste tipo – mas que fez sentir o desígnio da representação local mais que necessário: urgente!

Não se tratou, assim, de constituir núcleos, delegações ou "mini"-APDPO no território. Antes pelo contrário, a representação local tem dois movimentos distintos, integrados na dinâmica da APDPO e que para ela e dela convergem: levar a APDPO a dar-se a conhecer no território onde está a massa associativa; trazer para a APDPO as preocupações e necessidade mais prementes do território de cada um dos associados. Seguindo uma "divisão" administrativa (Norte, Centro, Algarve e Regiões Autónomas), a APDPO constituiu grupos de Representação Local considerando que globalização traz, em si

mesma, a capacidade de comunicar desde qualquer ponto, garantindo a interconexão dos interlocutores, apesar das distâncias geográficas, horárias e de pensamento; nunca, como agora, o homem foi capaz de ser inteiro, em todo o mundo, ao mesmo tempo. Embora a realidade global traga inumeráveis e inenarráveis benefícios, também corre o risco da desumanização, da "impessoalidade", do grupo sem referencial pessoal, humano e humanizador. A APDPO, constituída como associação, congrega vários profissionais que, por diversos motivos, se encontram dispersos. Profissionais que encontram na APDPO um referencial associativo, profissional, ético e deontológico. Por forma a criar canais de comunicação, de entreajuda e troca de experiências, de proximidade e de mobilização, constitui-se o presente projeto que discutirá sobre esta realidade e os desafios que nos coloca.

Assim, os grupos de Representação Local têm como objetivo geral estruturar canais através de associados, que se estabeleçam em cada região (Norte, Centro, Algarve e Regiões Autónomas) como interlocutores com a APDPO, por forma a gerar dinamismos regionais que criem mais-valias para a APDPO e a sua missão.

Entre os objetivos específicos contam-se: identificar, para cada região, canais de comunicação, divulgação e entreajuda; identificar, para cada região, facilitadores de trocas de experiências, de proximidade e de mobilização; identificar, para cada região, locais parceiros que acolham iniciativas da APDPO e a sua divulgação; fazer o levantamento e mapeamento da massa associativa, por região, e estabelecer contactos com os interlocutores identificados; dinamizar, através dos interlocutores, momentos de encontro, formação e convívio, para gerar sinergias regionais; estabelecer funções e dinamismos, enquadrados com as necessidades identificadas, para cada região e massa associativa; concretizar a sedimentação regional da APDPO, através de encontros descentrados dos órgãos sociais, nomeadamente a Direção, mobilizando a massa associativa; gerar, regionalmente, conteúdos para a discussão interna da APDPO; identificar necessidades concretas na região e propor abordagens construtivas enquanto associação de profissionais; promover atividades para a APDPO, enquadradas na realidade regional, como enriquecimento profissional e humano da massa associativa.

Frutos destes grupos de Representação Local decorreram já duas ações presenciais (em Torres Novas e em Salvaterra de Magos) e um evento remoto (organizado pelas Regiões Autónomas):

- no dia 6 de maio decorreu uma ação de sensibilização no auditório da NERSANT, em Torres Novas, organizado pela APDPO em estreita colaboração com o grupo de Representação Local do Centro e com o apoio do Município de Torres Novas e do NERSANT; os oradores foram a Dra. Inês Oliveira, este vogal da Direção e o Dr. Manuel Ferreira.

- no dia 29 de junho, em plataforma remota, foi dinamizada uma sessão especial das Conversas (In)Seguras, a cargo do grupo de Representação Local das Regiões Autónomas, onde foram oradores, em dois painéis, Eng. Vitorino Gouveia e o Eng. Paulo

Brás (Cibersegurança e Proteção de Dados, moderado pelo Eng. Sílvio Gomes) e a Eng. Carla Carvalho, a Dra. Merícia Bettencourt e o Professor Rui Nunes (Bioética e Inteligência Artificial aplicada à Saúde, moderado pela Eng. Angelina Mendes).

- no dia 30 de setembro teve lugar uma nova ação de sensibilização, desta vez no auditório da Escola Profissional de Salvaterra de Magos, em Salvaterra de Magos, organização conjunta com o Município de Salvaterra de Magos e com a Escola Profissional, articulados pelo grupo de Representação Local do Centro; foi orador, para além deste vogal da Direção, o Dr. Manuel Ferreira Ramos.

Para 2023 perspetivam-se já alguns momentos formativos, momentos de networking e momentos de sensibilização junto dos territórios e dos atores regionais. Diante da realidade e da adesão que marcam o projeto da Representação Local, acredito que a Representação Local é, sem dúvida, um desígnio da APDPO e que, na vida presente e futura da associação deverá merecer o maior e melhor carinho, quer dos órgãos sociais, quer a adesão da massa associativa. A APDPO faz-se próxima, pela mão da massa associativa, e irá tão longe ou tão perto, conforme a massa associativa se estimule para fazer concreto o desígnio da Representação Local.

Obrigado!

Entrevista a Eduardo Magrani

Eduardo Magrani

Ph.D. on Law & Technology (Dr. juris) | Tech, IP & Data Protection Lawyer | Artificial Intelligence, Cybersecurity & Digital Ethics Senior Advisor | Affiliate at Harvard University | Post Doctor at TU Munich Univ.

A APDPO entrevistou Eduardo Magrani, atualmente Senior Consultant na CCA Law Firm, sobre o tema do momento:

Quais as tendências de regulação da Inteligência Artificial (IA)?

A IA é um tema transversal e complexo. Diversas normas podem ser aplicadas ao campo da IA dada a sua extensão. Porém, cada vez mais, observamos uma tendência regulatória de normatizar campos específicos e usos específicos ligados à IA.

O RGPD, na Europa, acaba por regular essa matéria no tocante aos dados pessoais com uma regulação bastante robusta relacionada à proteção dos dados pessoais e que possui uma passagem voltada para decisões automatizáveis que remete ao tema de IA.

Para além do RGPD, existe agora uma discussão na Europa sobre o AI Act, um Ato regulatório específico para a IA que deve ser visto em complemento às outras normas e regulações que já existem, como é o caso do RGPD. Sendo uma norma específica, uma regulação específica, o AI Act tem uma condição maior de ajudar a reduzir riscos, a garantir melhor os direitos que devem ser garantidos neste campo e dá mais segurança jurídica para aqueles que querem introduzir IA nas suas soluções tecnológicas, nos seus serviços e nos seus produtos.

Portanto, trata-se de um tema complexo e observa-se hoje uma forte tendência regulatória, principalmente na Europa, como é o caso da proposta de regulação do AI Act que tende a ser aprovada em breve e que vai impactar diversas entidades.

Quais os principais pontos de atenção para um legislador no tratamento da inteligência artificial?

O primeiro ponto de atenção remete ao próprio conceito de inteligência artificial. Durante a proposta do AI Act, os legisladores receberam diversas contribuições de entidades e houve um grande debate que remete aos conceitos. Não existe hoje uma fórmula perfeita para conceptualizar a inteligência artificial, mas é de suma importância que haja um consenso mínimo entre os legisladores, a sociedade civil, as empresas e órgãos públicos nessa matéria, porque a regulação, se não tiver uma construção conceitual bem feita, ela pode tornar-se, por exemplo, numa norma ineficaz. Ou ela pode tornar-se numa norma desproporcional por regular também aquilo que não deveria. Então, ao normatizar sobre a inteligência artificial, eu diria que o primeiro ponto de atenção é o próprio conceito de inteligência artificial.

Outros pontos de atenção remetem à análise de risco. Por exemplo, se determinados usos de inteligência artificial deveriam ser proibidos, ou não, e quais seriam as repercussões, as consequências disso.

Para além disso, é de se pensar como novas regulações podem complementar as regulações já existentes. Então eu mencionei há pouco o RGPD, mas o RGPD só trata de proteção de dados pessoais, então existe uma lacuna em relação ao tratamento automatizado de dados que não são dados pessoais.

Assim, um ponto de atenção seria, quais são hoje os principais gaps, os vácuos regulatórios e como eles podem ser endereçados por uma futura regulação de inteligência artificial?

Por fim, um outro ponto de atenção, que costuma ser bastante complexo, remete não só à avaliação de risco, mas a uma análise de risco. Eu mencionei, mas também é responsabilidade daqueles atores que desenvolvem inteligência artificial. A inteligência artificial pode gerar um dano que vem de diferentes inputs, de diferentes ações. Podem ter gerado uma inteligência artificial que traz uma complexidade em relação à responsabilidade dos agentes envolvidos, que deve ser endereçado com bastante cautela também.

Como é que a inteligência artificial impactará os temas de proteção de dados pessoais?

Impacta porque a regulação específica de inteligência artificial ela vai muito além da proteção dos dados pessoais, uma inteligência artificial para ser treinada precisa necessariamente de dados, mas nem sempre esses dados são considerados dados pessoais.

Os dados pessoais já são cobertos pelo RGPD, mas cabe agora à regulamentação complementar tudo aquilo que não for uma matéria específica de dados pessoais e ir além preenchendo esses gaps, esses vácuos regulatórios, pensando de forma mais holística, inteligência artificial nos seus diversos usos, como uma tecnologia transversal que impactaria diferentes áreas e que usa a informação para ser treinada, mas não somente dados pessoais.

Como analisar os riscos da inteligência artificial aos direitos fundamentais dos sujeitos individuais?

A Inteligência Artificial pode trazer uma série de benefícios, automatizando processos, serviços, aumentando o ganho de eficiência não só no setor privado, mas também no setor público gerando maior rentabilidade, então os seus benefícios são notórios na área profissional e na nossa área particular, trazendo comodidade também para o dia a dia. Então todos esses benefícios transversais já são muito bem percebidos hoje pela sociedade como um todo e pelas empresas que desenvolvem e órgãos públicos que utilizam e que se valem dessa nova tecnologia de grande potencial.

Porém, com todo esse enorme potencial a inteligência artificial pode trazer também riscos.

E quais os riscos que a inteligência artificial pode trazer?

São de diferentes ordens, pode trazer riscos referentes à violação de dados pessoais, por um lado, por conta da sua opacidade e da sua falta de transparência, há a possibilidade de gerar discriminações não razoáveis com algum titular de dados pessoais ou quando esse titular de dados pessoais não autorizou o processamento daquela informação pessoal. Então isso só para falar na relação com dados pessoais. Mas, para além dos dados pessoais, a inteligência artificial estão atreladas, justamente, ao nível de impacto e risco que é gerado. Por uma solução específica em um contexto pré-determinado, também pode prejudicar indivíduos somente com o uso de outras informações, gerando problemas de falta de transparência e discriminação, mesmo sem utilizar dados pessoais.

Hoje existe um debate internacional sobre princípios éticos que deveriam nortear a inteligência artificial, como o princípio da justiça, da benevolência, da não maleficência, da não discriminação, da transparência, da privacidade e da responsabilidade. São alguns dos princípios mais mencionados no campo da inteligência artificial, que deveriam ser implementados por sociedades privadas e por órgãos públicos que utilizam inteligência artificial justamente para se evitarem os riscos e os danos que podem vir desse cenário. São alguns dos princípios mais mencionados no campo da inteligência artificial, que deveriam ser implementados por sociedades privadas e por órgãos públicos que utilizam inteligência artificial justamente para ser evitar os riscos e os danos que podem vir desse cenário. Muitos ainda não estão regulados, mas que através da implementação de princípios éticos, podem ser reduzidos.

Mas para além da orientação ética, para o desenvolvimento da inteligência artificial é necessário avançar-se com uma regulação específica. E é isso que a Europa está discutindo agora com o AI Act em que uma das facetas é ter uma regulação baseada em risco, inclusive proíbe determinados usos da inteligência artificial. E essas proibições
a ideia é cada vez mais extrair os benefícios, mas reduzindo os riscos e os danos que podem emergir dessa utilização e

desenvolvimento da inteligência artificial e me parece que a Europa está indo numa boa direção no sentido de mitigar esses riscos que podem concretizar-se nos próximos anos.