Qualidade e Protecção de Dados

Um caminho a percorrer juntos

Sílvio Gomes

silviogomes@complianceway.pt

Consultor da empresa Compliance Way

Resumo

O Regulamento Geral sobre a Protecção de Dados (RGPD) coloca a protecção dos dados pessoais como um direito fundamental, com liberdade de circulação em mercado regulado. Neste seu princípio maior, o regulamento pretende que os dados pessoais deixem de ser tratados como uma mercadoria apetecível em mercado desregulado.

O que deve preocupar uma cidadania consciente são as dificuldades que o tema da Protecção de Dados enfrenta para entrar em algumas sociedades europeias, que aceitam viver à margem de alguns direitos fundamentais. Estes continuam a pairar acima da sociedade, "sem ordem para aterrar".

Nesta fase de incorporação das disposições legais sobre a protecção de dados, pelas organizações que dispõem de um Sistema de Gestão da Qualidade (SGQ), defende-se a implementação de um Sistema de Gestão da Protecção de Dados (SGPD), que cruze horizontalmente todos os fluxos de tratamento de dados operados nos diversos departamentos, acomodando-o como um processo de suporte no mapeamento geral da gestão por processos.

Evoluindo-se para um quadro normativo aplicável a esta área, com requisitos para a certificação, admite-se que esta fase, em que os SGPD "gatinham" como processos de suporte do SGQ poderá esgotar-se, e verificar-se a sua emancipação para uma fase nova e mais madura, em que já "caminham" por si, como um sistema de gestão autónomo, mas compactível com outros sistemas, permitindo a sua gestão integrada.

Palavras-chave: Comissão Nacional de Protecção de Dados (CNPD); Regulamento Geral sobre a Protecção de Dados (RGPD); Sistema de Gestão da Protecção de Dados (SGPD); Sistema de Gestão da Qualidade (SGQ).

Abstrat

The General Data Protection Regulation (GDPR) places the protection of personal data as a fundamental right, with freedom of movement on a regulated market. With this major principle, the regulation aims to stop personal data being treated as a desirable commodity in an unregulated market.

What concerns a conscious citizenship are the difficulties Data Protection theme faces to enter into some European societies, which accept living on the fringes of some fundamental rights that continue to hover above society, "without order to land."

In this stage of the incorporation of the GDPR by the organizations with a Quality Management System (QMS), it is recomended the implementation of a Data Protection Management System (DPMS), which horizontally checks all the data processing flows

operated in the several departments, accommodating it as a support processes of the QMS processes mapping.

Evolving into a regulatory framework, with certification requirements, it is realized it can finish the current stage in which the DPMS "stumbles" as QMS support processes and started emancipating themselves by moving on to a new and more mature stage, allowing them to "walk" by themselves as an autonomous management system, which is compatible with other systems, working as an integrated management.

Keywords: National Data Protection Commission (NDPC); General Data Protection Regulation (GDPR); Data Protection Management System (DPMS); Quality Management System (QMS).

1. Introdução

No artigo intitulado Qualidade e Protecção de Dados – Um diálogo a explorar em debate aberto [1], assinalou-se, no primeiro parágrafo do resumo que,

> "Em 2018, a Qualidade e a Protecção de Dados constituem dois grandes desafios para as organizações. Da consistência da resposta podem advir oportunidades de melhoria em conformidade legal com o Regulamento Geral sobre a Protecção de Dados (RGPD) e em conformidade normativa com a nova versão da norma ISO 9001:2015".

Com o enfase dado à "consistência da resposta" das organizações aos dois desafios, pretendeu-se chamar a atenção para a qualidade desta ideia chave, para uma abordagem adequada de boa governação. Tanto mais que se está à saída de uma crise económica profunda, algo devastadora, e que exige uma nova visão empresarial, qualitativamente diferente de velhos hábitos de gestão.

Os desafios da Qualidade e da Protecção de Dados, têm características próprias, mas que combinadas podem dar um forte impulso às organizações para uma melhor definição da política e dos objectivos, pela optimização dos recursos e das práticas organizativas para a melhoria do desempenho.

Gerar e gerir a mudança nas organizações não pode ser um floreado abstrato e inócuo. É um tema premente, cada vez mais actual, e suficientemente sério para que não esteja sempre presente nas tomadas de decisão.

A gestão da mudança, numa óptica proactiva e de prevenção do risco de imobilismo organizativo, é um factor crítico para qualquer organização, com impactes significativos na tendência para a cristalização das práticas tradicionais.

2. Onde estamos, e como vão as organizações?

Passaram depressa os dois anos de "vacacio legis", desde a entrada em vigor do RGPD [2], em Maio de 2016. Já passou o período concedido, para que os Estados-Membros, as organizações públicas e privadas se adaptassem aos novos paradigmas regulatórios.

O IAPMEI [3] estimou que em 25 de Maio de 2018, data da entrada em aplicação directa do RGPD, apenas 8% das empresas estariam melhor preparadas para responder ao regulamento.

Face a um passado recente, nota-se que já há mais organizações a auscultar o mercado, à procura de soluções com custos suportáveis, admitindo combinar os recursos internos com o recurso à consultoria externa. Outras já iniciaram os processos de formação e diagnóstico, e poucas estão a desenvolver projectos de implemetação.

De facto, foram dois anos desperdiçados pelo Estado e pelas organizações. Não foram aproveitados para a avaliação de impacto do RGPD e elaboração de um plano de implementação para a conformidade exigida. Houve poucas preocupações em adquirirem a competência necessária para governo dos projectos, em especial a formação dos recursos a envolver. Não impulsionaram a gestão da mudança de práticas organizativas para incorporar uma política de privacidade e de protecção de dados. Não avaliaram os riscos nem as medidas técnicas e organizativas mais adequadas para a segurança da informação. Não calcularam os custos do projecto.

"As empresas e o Estado tinham obrigação de preparar o regulamento desde 2016", frisou assertivamente a Dr.ª Filipa Calvão, Presidente da CNPD [4], em entrevista ao Jornal de Negócios em 29.01.2018. E acrescentou: "Pode acontecer que a CNPD considere suficiente, depois de uma fiscalização, fazer recomendações ou uma admoestação. Mas sim, também serão aplicadas as sanções previstas na lei". E terminou com uma oportuna chamada de atenção para que "Independentemente do valor das coimas, eu gostaria de ter visto estas preocupações, que agora existem, nos últimos anos"

Mas chegados aqui, e assim, o que poderá dizer-se sobre as abordagens tardias ao RGPD?

As considerações expostas têm como base a experiência vivida na implementação das exigências do regulamento, em algumas organizações públicas e privadas, com ou sem um SGQ certificado. Consideraram-se ainda as opiniões recolhidas em alguns estudos e debates sobre o tema.

Admite-se que a amostragem é limitada e que é preciso ter cuidado quando, a partir deste pequeno universo, se estimam as características dos processos em curso, de modo a não serem tiradas conclusões precipitas. Mas sim, sente-se que, no essencial, não se andará longe da realidade.

As opiniões e as constatações recolhidas nas organizações são geradoras das maiores preocupações. É certo que reagem ao regulamento de forma desigual, evidenciando diferentes níveis de maturidade e de disponibilidade para atingirem o grau de conformidade que entendem necessário e possível.

Para além do despertar tardio e algo agitado, são poucas as organizações em que a gestão de topo assumiu a responsabilidade de as orientar para aproveitar as oportunidades que estes desafios colocam. Não tem sido fácil realçar oportunidades onde outros só vêm ameaças.

De um modo geral, o nível de disponibilidade é limitado à ideia de conseguir um grau de cumprimento parcelar, orientado para os requisitos jurídicos que imaginam passíveis de serem sancionados.

Apesar da simpatia pelo RGPD, reconhece-se que não é indutor de grande entusiasmo. É um texto para ser aplicável em todos os Estados-Membros da União e a cumprir por qualquer tipo de organização que trate dados pessoais. Não abre as portas a subsídios ou a outras formas de compensações financeiras. Antes pelo contrário, obriga a alguns "custos", ou seja, a algum investimento para desenvolver negócios na sociedade digital. Calcula-se que 32% dos portugueses já recorram a produtos e a serviços desta nova economia.

De qualquer forma, não admira que o RGPD, com os seus 173 considerandos que antecedem os 99 artigos, seja um texto denso, com muitas abstracções, remissões e derrogações, de leitura complicada e de interpretação complexa, muitas vezes sem a certeza jurídica necessária para a adopção de práticas decorrentes.

A sensibilização para o tema é baixa e a contragosto. O desinteresse e o desconhecimento alimentam o adiamento de decisões urgentes e desconfianças infundadas.

Ao falar-se com muitos quadros superiores e intermédios, sente-se o desassossego e o desconforto por só verem no RGPD entraves às práticas seguidas, que absorve recursos.

São sugeridas formas criativas de abordar os seus requisitos e questionadas regularmente e com veemência, as razões de ser de algumas orientações e recomendações, cuja fundamentação desconhecem e são geradoras de alguma estranheza.

Questionam a necessidade de expor o âmbito e fazer referências explícitas aos direitos dos titulares dos dados e às suas obrigações nos considerandos da política e dos objectivos a publicitar. Com mais ou menos esforço vão aceitando a obrigação de implementarem alguns procedimentos internos para garantirem a repetibilidade e a reprodutibilidade das respostas aos pedidos dos titulares ou dos seus representantes, para o livre exercício dos seus direitos, para responder às eventuais notificações de violações de dados que possam ocorrer, para auditar o grau de conformidade, para atenderem aos actos de fiscalização ou aos pedidos que a CNPD venha a solicitar, entre outras obrigações.

A tendência é para sugestões subtis de redução da conformidade a meia dúzia de frases emblemáticas, construídas muito genericamente sobre "os cuidados no tratamento dos dados", a "transparência das informações" e o "consentimento do titular", quantas vezes integrados num vasto lençol descritivo de um varrimento de finalidades.

Sente-se que não pode fugir-se ao grande desafio de sensibilizar a gestão de topo, os quadros intermédios das organizações e contribuir para a formação das pessoas com responsabilidade nas operações de tratamento.

Não será fácil consciencializar uma organização que a conformidade não se atinge no momento em que se cumpre uma checklist. A conformidade é um processo evolutivo, contínuo e controlado, em que todos são chamados a assumir o seu lugar para a responsabilidade demonstrável.

Continua-se à espera de exemplos em que uma política de protecção de dados tenha prejudicado o desenvolvimento económico de empresas ou de países. Já o contrário é verdadeiro, como alguns exemplos recentes comprovam.

3. E o Estado, que papel tem assumido?

Para além de alguma ligeireza e apetência da maioria das organizações para limitar a conformidade a pequenas secantes ao regulamento, estas absorvem facilmente o contágio negativo da forma descuidada com que o Estado continua a abordar as suas responsabilidades nesta área.

Em primeiro lugar, o Estado também iniciou tarde o processo legislativo. Não tem sido a alavanca necessária para mover o mundo da protecção de dados, como seria sua obrigação.

Em segundo lugar o Estado não promoveu o envolvimento e o concurso da CNPD, ignorando o seu papel de autoridade de controlo que concentra competências indiscutíveis e indispensáveis para um processo legislativo em conformidade com o RGPD.

Em terceiro lugar ainda não foram identificados vários impactos em outras leis sectoriais que carecem de consolidação legal, alinhando-as pelo regulamento.

O Estado, com as várias versões da proposta de lei 120/XIII [5], não evitou um contexto de incertezas e de indefinições, na adaptação frágil e na densificação questionável de aspectos do articulado do RGPD à realidade nacional, nem sempre no respeito pela margem legislativa concedida aos Estados-Membros, no regulamento.

A este propósito saliente-se o parecer assertivo, crítico e demolidor da CNPD, cuja fundamentação constitui, só por si, uma peça sobre a conformidade interpretativa do regulamento.

As vicissitudes do processo legislativo abriram portas que deveriam estar fechadas. Desde as hipóteses de incumprimento de prazos obrigatórios para a conformidade, depois da entrada em aplicação directa do regulamento, até ao mau exemplo de isentar os organismos públicos de sujeição ao quadro sancionatório, tem-se assistido a um rol de más opções.

Só a recusa dos deputados em legislar mal e à pressa travou a vertigem de inconformidades da proposta legislativa, o que permitiu abrir uma nova fase, que se espera célere e em conformidade com o RGPD.

Ao não patrocinar um ambiente de rigor e respeito pelo regulamento, o Estado contribuiu para que a maioria das organizações privadas tivessem desacelerado os ténues processos de implementação, invocando a necessidade de esperar pela aprovação da lei.

Se a futura lei e o RGPD constituirão a ordem jurídica nacional aplicável à protecção de dados, não é menos verdade que essa ordem jurídica existe e é assegurada pelo RGPD e pela actual lei 67/98, nos requisitos jurídicos que não conflituem com o regulamento. A referida lei já deveria ter sido revogada, porque decorre da Directiva 95/46/CE que foi revogada pelo RGPD. Entretanto vai-se esperando que o actual quadro legislativo se clarifique, provavelmente até ao fim do mês de Junho, sem se saber se está meio cheio ou meio vazio.

Tal como nos últimos 20 anos, o Estado, as organizações públicas e privadas continuam a viver ao arrepio da actual lei 67/98 que já define um vasto conjunto de direitos dos titulares e de obrigações a observar.

Dir-se-á que Portugal está alinhado pelo ambiente geral da Europa, pois apenas cinco estados (Alemanha, Áustria, Bélgica, Eslováquia e Espanha) têm a sua lei aprovada e a coexistir com o RGPD.

Pelo exposto, o que deve preocupar uma cidadania consciente é o facto do tema da Privacidade e da Protecção de Dados enfrentar tanta dificuldade para entrar na maioria das sociedades democráticas europeias. Continua-se a alimentar um mercado desregulado com os dados pessoais fora do controlo dos seus titulares, perante uma grande indiferença da maioria dos Estados e o desconforto regulatório das organizações, aceitando-se viver à margem de alguns direitos fundamentais que continuem a pairar acima da sociedade, "sem ordem para aterrar".

4. Dados pessoais - um direito fundamental ou uma mercadoria?

Por falar em direitos fundamentais relembre-se que, na primeira frase do primeiro considerando do RGPD é afirmado que "A protecção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental".

Ao colocar a protecção dos dados dos titulares como um direito fundamental, com liberdade de circulação em mercado regulado, o regulamento não está a sugerir nenhum delírio alienígeno. Está a definir o seu princípio maior, contribuindo legalmente para que os dados pessoais deixem de ser tratados como uma mercadoria apetecível, a explorar em mercado desregulado.

Ao fim de anos sem respirar os ares dos direitos dos titulares dos dados e sem hábitos no cumprimento das obrigações dos responsáveis pelo seu tratamento, leiam-se as autoridades e os organismos públicos, as associações económicas sectoriais e as empresas privadas, não admira que o RGPD represente para muitos um grande e desconfortável "salto", e não um pequeno "pulo" no caminho dos direitos humanos nas sociedades modernas, que já deveria estar a ser trilhado há muitos anos.

Como entender a infeliz afirmação na "Exposição de Motivos" da proposta de lei 120/XIII do Governo que "a aplicação deste regulamento resultará em encargos administrativos elevados, que em muitos casos não encontram suficientemente justificados os benefícios obtidos com o novo regime de protecção de dados pessoais relativamente ao actual".

O "actual" regime é o que o Estado não aplica nem faz aplicar. Perante as tensões que o RGPD tem provocado nas empresas, face ao seu tradicional modelo de negócio, ao arrepio dos direitos dos titulares dos dados, não deveria ser o Estado a desautorizá-lo e a reduzi-lo a um estorvo económico para as organizações. O que se esperava é que clarificasse um regime ajustado e proporcionado, mas aplicável e fiscalizável, ajudando a "puxar para cima" o que muitos puxam para baixo.

E no meio de tudo isto, pode perguntar-se mais uma vez, onde fica a CNPD? Com que meios e condições pode continuar a exercer o seu papel de defesa dos titulares dos dados? A ausência de verba inscrita no orçamento geral do Estado, para capacitar a CNPD para as suas novas e acrescidas funções fiscalizadoras, com independência e autonomia, ajuda a perceber a ideia do Estado quanto à importância que tem atribuido aos novos paradigmas regulatórios na protecção dos dados pessoais.

5. A Qualidade e o dia 15 de Setembro

Não sendo objecto do presente artigo, uma abordagem ao atraso e ao modo com se têm desenrolado os processo de transição da norma ISO 9001:2008 [6] para a versão ISO 9001:2015 [7], considera-se que o estado de alma nas organizações não é muito diferente do já descrito para o do RGPD, com riscos similares e com elevados graus de parentesco.

Também é preocupante, ainda que não muito surpreendente, algumas organizações, fortemente pressionadas pelo facto dos certificados caducarem a 15 de Setembro, e perante o "descuido" temporal e de recursos para seguir as boas práticas no processo de transição, sejam tentadas a pensar que a reconfiguração dos respectivos SGQ seja conseguida com alterações de títulos, de referências e de datas dos documentos existentes. Também é preocupante que se estime apenas 30% das empresas com o processo concluído.

Os organismos responsáveis pelas auditorias de certificação serão chamados a olhar, com cuidados redobrados, para as evidências dos processos de transição. Espera-se que verifiquem se não houve pequenas e insignificantes mudanças documentais para que o sistema continue como dantes.

Os clientes e outras partes interessadas esperam que as organizações que cuidaram da boa transição para a nova versão da norma, obtenham uma diferenciação positiva no mercado.

6. Qualidade e protecção de dados

Em diversos artigos e intervenções sobre o tema, tem-se reforçado a ideia de que é necessário recorrer às ferramentas conceptuais da Qualidade, para melhor avaliar o impacto do RGPD nas organizações e aplicá-las no planeamento, na implementação, na verificação e na melhoria da sua conformidade.

Se houve uma fase inicial do despertar para as exigências regulamentares, em que prevaleceu o pendor mais jurídico, depressa se acrescentou outro mito sobre o milagre das tecnologias de informação para garantir a conformidade com o regulamento.

Apareceram firewalls, hard e software para tudo. Assistiu-se a promoções de produtos milagrosos, com um desempenho à margem de vulnerabilidades e à prova de riscos, nunca referidos.

Salvo as grandes organizações dos sectores da banca, dos seguros, da saúde, das operadoras de telecomunicações e da energia, e mais algumas autoridades e organismos do Estado, como a Autoridade Tributária, a Segurança Social, o Instituto Informático e outros, o tecido empresarial português não pode, nem precisa, de matar moscas com luvas de boxe.

Uma abordagem sistémica, que convoque todos os saberes e competências da organização, e que cuide da conformidade diariamente e em todas as operações de tratamento, é o único caminho a percorrer, com todas as áreas que participam nas actividades da organização, para potenciar o desempenho dos recursos humanos envolvidos, únicos garantes da conformidade sustentável.

7. Conformidade para além do curto prazo

Quaisquer abordagens, mais jurídicas ou mais tecnológicas, e por razões intrínsecas aos seus pressupostos, sendo necessárias e com contributos indispensáveis, são sempre parcelares e insuficientes, por estarem fora de uma abordagem holística e sistémica. Pecam por não estarem em sintonia com a maturidade e o pulsar diário dos recursos humanos de que depende qualquer organização.

Ambas as abordagens persistem no mercado com ligeiros deslocamentos em direcção às preocupações com a forma das organizações digerem e respondem às novas exigências regulatórias.

Quanto mais experiência se recolhe nos diversos processos de implementação do RGPD, mais se confirma, que as abordagens acima comentadas são selos de garantia de curto prazo, por não atenderem ao comportamento organizativo dos recursos humanos, e às falhas operacionais no dia a dia das organizações. E sabe-se como é, ao longo do tempo, que vão crescendo os factores geradores de derrapagens da conformidade, criando-se lacunas e vulnerabilidades nas operações de tratamento e na segurança dos dados pessoais.

Não tem sido fácil convencer as organizações que não há vacinas nem kits de conformidade.

Ultrapassada a fase aguda do terror causado pelas nuvens negras das obrigações e das sanções, oportunisticamente exploradas por alguns players, constata-se que nada pode

substituir o processo uterino da implementação de um SGPD [8], pela consciência das necessidades desejadas, para a oportunidade de optimizar processos e práticas organizativas.

8. PDCA, uma metodologia adequada e segura

Batendo à "porta" de uma organização, com base no direito de acesso, por que corredores e salas deverá o titular dos dados ser levado para exercer, de forma consciente e proporcionada os seus direitos? Infelizmente o tsunami de informações e pedidos de consentimento que ocorreu na véspera da data de 25 de Maio não respondeu a esta questão central.

Para que uma organização cumpra as suas obrigações, quanto à protecção dos dados dos titulares, no âmbito da sua actividade económica, tem que conceber e implementar um sistema de gestão que assente em procedimentos para assegurar respostas estáveis e consistentes, para além de "respostas" imediatistas com um elevado grau de variabilidade.

A política e os procedimentos têm que traduzir os requisitos jurídicos do RGPD em requisitos da organização, desenhando um SGPD.

Mesmo em organizações sem experiência na operacionalização de sistemas de gestão, o recurso à metodologia assente no ciclo PDCA [9], tem-se mostrado adequado e propiciador de sinergias e conforto no controlo e na certeza operacional no desenvolvimento dos projectos.

De acordo com o quadro conceptual do ciclo PDCA, os processos de implementação desenvolvidos são divididos em 4 etapas e cada etapa em várias fases, com actividades definidas e em progressão, com objectivos mensuráveis, prazos e responsabilidades atribuídas.

Na Etapa 1, do Planeamento (*Plan*), têm-se sentido maiores dificuldades em despertar e em convocar toda a organização, ultrapassando paradigmas tradicionais. Concentram-se todos os esforços na formação e no diagnóstico da situação actual das empresas quanto aos dados e às operações de tratamemto, com a identificação da sua fundamentação e dos sistemas físicos ou digitais de apoio, assim como a avaliação dos níveis de risco associados e a definição de medidas técnicas e organizativas adequadas.

Toda a informação recolhida nas matrizes de diagnóstico, preenchidas pela organização, é depois validada e completada nas entrevistas presenciais nos diversos departamentos e com todas as partes interessadas, em especial os subcontratantes.

Por fim é elaborado um relatório do diagnóstico, com as constatações e as recomendações que se entendem adequadas, para que a gestão de topo possa tomar as suas decisões sobre a conformidade desejada, a política e os objectivos, o plano geral da implementação, os recursos a afectar e os custos a considerar.

Depois de formada a equipa de projecto, segue-se a materialização do plano aprovado, com a elaboração e a actualização documental, incluindo a revisão de alguns documentos já existentes, como sejam os contratos com os diversos stakeholders.

Todo o corpo documental deverá ser elaborado e organizado sob a forma de um Manual do SGPD que, depois de aprovado pela gestão de topo, deverá ser comunicado a toda a organização a envolver na implementação.

Na Etapa 2, da Implementação (*Do*), sente-se que a organização começa a estar mais receptiva e a ver o sentido das novas práticas. As actividades são a formação sobre a arquitetura do SGPD e a documentação associada, em cuja elaboração participaram e a marcação do início da implementação com a selecção do departamento ou área de negócio, considerada mais crítica. Assim, o projecto começa a ganhar corpo num ponto de apoio modelo, como que num processo de prototipagem a considerar para a operacionalização generalizada a toda a organização, das actividades planeadas, com todos os registos associados.

Na Etapa 3, da Verificação e Auditoria (*Check*), as actividades têm sido focadas em "stress test", para sentir a qualidade da resposta da organização ao sistema em operacionalização. A simulação de exercícios de acesso e de direitos por parte de titulares, assim como de testes de resposta a simulações de violações de dados e de intrusão nos sistemas de informação, assumem um papel fundamental, para evidenciar as mudanças comportamentais e de práticas organizativas indispensáveis à operacionalização dos novos paradigmas regulatórios.

Neste âmbito serão reavaliadas as avaliações de risco e as medidas técnicas e organizativas aplicadas. Por fim, é elaborado um balanço sobre a maturidade, robustez e conformidade atingidas para auditar o SGPD.

A experiência recolhida nas organizações situa-se, sobretudo, na etapa 3, a evoluir para a etapa 4.

Assim, é nossa convicção vir a desenvolver na Etapa 4, de Revisão e Melhoria (*Act*), as actividades de acordo com as constatações da auditoria, para a melhoria, a revisão final e a aprovação do Manual do SGPD, assim como a realização de uma nova acção de formação sobre o SGPD implementado, abrangendo todos os recursos humanos envolvidos nas operações de tratamento de dados.

Por fim deverá sair da equipa de projecto o EPD a designar, se aplicável, ou um responsável pela operacionalização, manutenção e conformidade do sistema.

A figura do EPD não será abordada neste artigo, uma vez que merece, pelo perfil e a importância do cargo, um tratamento especial a dedicar em próxima oportunidade. O mesmo se passa com uma abordagem à avaliação de impacto da protecção de dados e ao registo das actividades de tratamento.

9. Um processo de suporte

A experiência de consultoria nas organizações, tem permitido consolidar a ideia, já defendida em vários fóruns e artigos, sobre a necessidade de se desenhar um SGPD, que cruze horizontalmente todos os fluxos de tratamento de dados realizados nos diversos departamentos, acomodando-o como um processo de suporte no mapeamento dos processos do SGQ.

Como processo, e uma vez definido o objectivo, o âmbito, o caminho, os pontos de controlo e os indicadores para a avaliação do desempenho, deverá ser indicado o EPD como o "*Owner*" natural do processo, ou outro perfil de responsável.

Clarificado o seu lugar no mapa dos processos de gestão do SGQ, perspetivam-se ganhos mútuos de consistência, pelas sinergias que naturalmente se desenvolverão, alavancadas em alguma "obrigatoriedade contagiante" para a conformidade legal e normativa.

10. A Missão do IPQ e a normalização da área da protecção de dados

Por várias vezes tem-se abordado o tema das relações de parentesco admissíveis, entre a Qualidade e o RGPD.

Quanto ao RGPD e de forma abreviada, podem realçar-se algumas semelhanças, como sejam o mapeamento geral dos dados e das operações de tratamento, com a avaliação dos riscos associados, desde a concepção e por predefinição, a obrigatoriedade de demonstrar a conformidade e de auditar o sistema, o perfil do EPD, e outras.

Também a figura da CNPD, como a autoridade de controlo, com as suas atribuições e poderes, o papel de organismos acreditados para a "supervisão de conformidade com os códigos de conduta", assim como as referências aos processos, à existência de requisitos, à norma EN ISO/IEC 17065:2012, aos organismos de certificação e a outros aspectos relacionados com este tema, referidos no RGPD.

Num relance pelo artigo 43º pode ler-se que um organismo de certificação deve evidenciar "um nível adequado de competência em matéria de protecção de dados, emite e renova a certificação, após informar a autoridade de controlo para que esta possa exercer as suas competências…". Refere-se ainda que "Os Estados-Membros asseguram que estes organismos de certificação são acreditados: a) pela Autoridade de Controlo (…) e b) pelo organismo nacional de acreditação", leia-se IPAC [10].

No referido artigo, saído na revista Qualidade, admitiu-se um eventual desenvolvimento normativo, por parte da ISO, sobre o tema da Privacidade e da Protecção de Dados.

No desenvolvimento dessa ideia, sugere-se que o Instituto Português da Qualidade (IPQ) [11], no âmbito da sua Missão de "promoção e coordenação de atividades que visem contribuir para demonstrar a credibilidade da ação dos agentes económicos (…)", possa assumir um papel relevante na área em apreço. Tanto mais que está alinhada pelo objectivo da RGPD, referido no seu considerando 2, que é o de pugnar pela "realização de um espaço de liberdade, de segurança e de justiça e de uma união económica, para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem estar das pessoas singulares".

Realce-se ainda que, "Com vista ao desenvolvimento sustentado do País e ao aumento da qualidade de vida da sociedade em geral, o IPQ prossegue as suas atribuições assente nos princípios da Credibilidade e Transparência, da Horizontalidade, da Universalidade, da Coexistência, da Descentralização e da Adesão livre e voluntária, (…) aplicando e promovendo o uso generalizado de procedimentos, de técnicas, metodologias e especificações reconhecidos a nível europeu e/ou internacional".

Pelos traços gerais expostos, reafirma-se a ideia que o IPQ pode contribuir para uma melhor regulação do mercado, pela diferenciação das organizações que evidenciem o seu alinhamento com requisitos geradores de confiança junto dos titulares dos dados pessoais.

Assim, sugere-se que estude a possibilidade de nomear uma comissão técnica de normalização, com a missão de preparar uma nova família de normas para estabelecer,

implementar, manter e melhorar de forma contínua um sistema de gestão da protecção de dados.

Como é referido no campo da normalização do sítio Web do IPQ, "Qualquer norma é considerada uma referência idónea do mercado a que se destina, sendo por isso usada em processos de legislação, de acreditação, de certificação…As normas são documentos de aplicação voluntária, salvo se existe um diploma legal que as torne de cumprimento obrigatório".

Por fim sugere-se que a comissão técnica inclua representantes de um conjunto significativo de partes interessadas, desde a área jurídica à tecnológica, do sector empresarial ao académico, sem esquecer a CNPD, de modo a reunir o máximo de competências capazes de contribuir para uma abordagem normativa, que alavanque e contribua, de facto, para a progressão da maturidade das organizações.

O processo de normalização será faseado e em progressão, a construir-se com um conjunto de normas, como por exemplo uma norma que descreva uma visão geral, o vocabulário, os termos e as definições relacionados com os sistemas de gestão da protecção de dados, uma norma com orientações a seguir como guia na implementação dos SGPD e outra norma com os requisitos que possam proporcionar a certificação dos sistemas implementados. Poderão seguir-se outras normas que venham a justificar-se.

O âmbito nacional de aplicação das normas a desenvolver pelo IPQ não diminui o seu alcance, uma vez que o RGPD põe termo à dispersão e à fragmentação das ordens jurídicas dos diversos Estados-Membros, assegurando uma ordem jurídica uniforme em todo o espaço da União.

A norma com os requisitos para a certificação deverá adoptar uma estrutura de alto nível, de acordo com os termos e os critérios definidos no Anexo SL, para garantir a compatibilidade com outras normas de sistemas de gestão que tenham adoptado o mesmo anexo.

Num quadro normativo novo, com requisitos para a implementação de SGPD certificáveis, entende-se que poderá terminar a actual fase em que estes devem "gatinhar" como processos de suporte do SGQ, para se emanciparem e evoluírem para uma nova fase, mais avançada e madura, em que já "caminham" por si, configurando-se como um sistema de gestão autónomo, mas compatível com outros sistemas de gestão, permitindo a sua gestão integrada se for essa a opção das organizações.

Referências bibliográficas

(1) Gomes, S. (2018). Qualidade e Protecção de Dados – Um diálogo urgente em debate aberto. Artigo publicado na revista *QUALIDADE #1,* da Associação Portuguesa para a Qualidade.

(2) RGPD - Regulamento Geral sobre a Protecção de Dado, regulamento (EU) 2016/679.

(3) IAPMEI – Instituto de Apoio às Pequenas e Médias Empresas e à Inovação.

(4) CNPD - Comissão Nacional de Protecção de Dados.

(5) Proposta de Lei n.º 120/XIII, de 22 de Março de 2018.

(6) Norma NP EN ISO 9001:2008 – Sistema de Gestão da Qualidade. Requisitos.

(7) Norma NP EN ISO 9001:2015 – Sistema de Gestão da Qualidade. Requisitos.

(8) SGPD – Sistema de Gestão da Protecção de Dados

(9) PDCA – Plan, Do,Check e Act

(10) IPAC – Instituto Português de Acreditação

(11) IPQ – Instituto Português da Qualidade