Centre for Information Policy Leadership
Hunton & Williams LLP

Regulamentando para Gerar Resultados

Estratégias e Prioridades para Liderança e Engajamento

Documento de Trabalho

10 de outubro de 2017

Índice

Dez Tópicos para Discussão

"Regulamentando para Gerar Resultados" envolve fazer escolhas difíceis, mas essenciais, sobre estratégias e prioridades. As Autoridades de Proteção de Dados (DPAs) simplesmente não têm como fazer tudo e, portanto, decisões estratégicas são necessárias sobre o que funciona melhor.

1. Quando os desafios e expectativas da era digital são tão grandes – e especialmente quando os recursos são limitados – quais parecem ser as melhores maneiras para as DPAs (de forma independente e com outros) garantir que a regulamentação da proteção de dados irá produzir os melhores resultados?

2. Quais outros caminhos devemos estudar para aumentar os orçamentos das DPAs para níveis mais realísticos?

3. Quais as lições que podemos tirar das abordagens adotadas ao redor do mundo em muitas outras áreas de regulamentação?

4. Podemos construir um modelo eficiente que permita que as pessoas prosperem com dignidade e autonomia em um mundo digital onde usos inaceitáveis de dados, que violam a privacidade, sejam impedidos?

5. Dado o grande número de responsabilidadade das DPAs, quais são as melhores maneiras de conseguir eficácia a nível global?

6. A Abordagem Baseada em Resultados oferece maneiras uteis para estabelecer as prioridades estratégicas e equilibrar o engajamento, fiscalização e o tratamento de reclamações?

7. Está certo atribuir prioridade estratégica às funções de Liderança, com forte ênfase no engajamento construtivo com as organizações reguladas?

8. Na prática, quais são as atividades e técnicas que melhor promovem o engajamento construtivo?

9. Será que as entidades que reunem globalmente, regionalmente e operacionalmente as DPAs irão considerar a adoção sugerida dos Princípios para Abordagem baseada em Resultados?

10. Como esses Princípios podem ser aperfeiçoados?

Regulamentando para Gerar Resultados – Estratégias e Prioridades para Liderança e Engajamento

Introdução e Resumo

O ecossistema para regulamentação da proteção de dados e privacidade está mudando rapidamente, e não somente dentro da UE. Há muitos anos o Centro para Liderança em Políticas de Informação (*Center for Information Policy Leadership* – CIPL) vem defendendo o papel de organizações responsáveis e os méritos de uma abordagem baseada em riscos. A nossa atenção volta-se, agora, para o "encanamento" do sistema como um todo e considera como encaixar melhor suas partes componentes.

O objetivo deste documento é, principalmente, fomentar a discussão sobre como as Autoridades de Proteção de Dados[1] (DPAs) podem maximizar sua eficácia na era moderna da informação.

Quando as funções são muitas, as expectativas são altas e os recursos limitados. Este documento estuda se e como os esforços conscientes deveriam ser implementados para a regulamentação[2] da proteção de dados para que se torne mais "baseada em resultados". Isso envolve fazer escolhas difíceis, mas essenciais, sobre estratégias e prioridades. As DPAs simplesmente não conseguem fazer tudo.

A Abordagem Baseada em Resultados é utilizada pelo CIPL para permitir às DPAs – de maneira tanto independente quanto cooperativa – maximizar sua eficácia pela adoção de abordagens modernas e estratégicas para uma regulamentação que consiga os melhores resultados para os indivíduos, a sociedade e as organizações reguladas. Sobretudo, isso envolve o engajamento responsável com, e o apoio a, essas organizações, tanto no setor privado como no público, que estão tentando "acertar" enquanto, ao mesmo tempo, lidar de forma firme com aquelas que não estão nem tentando.

Este documento sugere alguns Princípios fundamentais para embasar a Abordagem Baseada em Resultados. O objetivo dos Princípios é oferecer subsídios para o

[1] As "Autoridades de Proteção de Dados", conforme utilizado neste documento, equivale a ser membro da Conferência Internacional de Comissários de Proteção de Dados e Privacidade.
[2] O termo "Regulamentação" é utilizado neste documento no sentido de "controle" ou "supervisão".

estabelecimento das prioridades estratégicas, incluindo fazendo o ranking de tipos diferentes de funções, selecionando as ferramentas mais adequadas e focando em determinados setores, atividades ou organizações.

Os Princípios para uma Abordagem Baseada em Resultados

- Regulamentar para Gerar Resultados no Mundo Digital exige que as Autoridades de Proteção de Dados (DPAs) sejam estratégicas, eficazes, coordenadas e transparentes.

- A meta de uma DPA deveria ser produzir resultados eficazes em termos de custo que, na prática, protejam os indivíduos, promovam o uso responsável de dados e facilitem a prosperidade e inovação.

- A primeira prioridade das DPAs deveria ser assegurar a proteção dos indivíduos.

- Cada DPA independente deveria ser responsável por definir, de maneira transparente, os resultados específicos que pretende, e as prioridades e abordagens que irá adotar para conseguir tais resultados através do seu trabalho regulatório.

- As estratégias de todas as DPAs deveriam ser coordenadas, consistentes e complementárias o quanto possível.

- As DPAs deveriam tratar as organizações reguladas de maneira consistente – adotando abordagens similares entre e dentro de setores, independentemente do tipo ou do alcance geográfico da organização.

- Cada DPA deveria adotar uma abordagem baseada em riscos em todas as suas atividades, dando prioridade para lidar com os comportamentos que mais prejudicam as pessoas ou os valores democráticos e sociais.

- Uma abordagem de engajamento construtivo, com ênfase em liderança, informações, recomendações, diálogos e apoio será mais eficaz do que dependência única e exclusiva em intimidação e punição.

- A ênfase em informações e recomendações tem importância especial na área de proteção de dados, devido a seu impacto abrangente em inúmeras organizações e a natureza das exigências que são imprecisas ou descontextualizadas, necessitando avaliação e decisão em casos individuais.

- Relacionamentos abertos e construtivos com as organizações que tratam das informações pessoais, com base em um diálogo honesto e cooperação mútua, com responsabilidades definidas, incrementarão os resultados de *compliance* como um todo.

- As organizações reguladas deveriam ser avaliadas, sobretudo, pela referência de boa-fé comprovável e diligência nos seus esforços voltados ao *compliance*.

- As organizações que buscam atuação responsável e que tentam “agir certo”, deveriam ser encorajadas a se identificarem, por exemplo, demonstrando de maneira transparente sua responsabilidade, seus programas de proteção de dados e gerenciamento de riscos, a influência de seus Encarregados de Proteção de Dados (os “DPOs) e seu uso de programas de selo/certificação, BCRs, CBPR e outras estruturas de responsabilização.

- Sanções punitivas deveriam ser direcionadas principalmente às atividades desconformes que sejam dolosas, deliberadas, seriamente negligentes, reincidentes ou particularmente graves.

- Embora atender reclamações individuais possa ser um componente importante na proteção dos indivíduos, lidar com alto volume dessas reclamações requer recursos substanciais que podem acabar impedindo objetivos estratégicos mais amplos. As reclamações deveriam ser solucionadas firmemente, com critérios claros para determinar a extensão da

investigação, também levando em conta que reclamações são uma ferramenta valiosa de inteligência.

O objetivo principal deste estudo é fomentar a discussão na comunidade de proteção de dados e de privacidade (inclusive reguladores, organizações regulatórios, sociedade civil, acadêmicos e especialistas).;

Embora a intenção deste estudo seja de oferecer uma visão do que seria na prática uma Abordagem Baseada em Resultados, é a própria comunidade de DPAs que tem de decidir se deseja levar isso adiante e como proceder nesse sentido. Se a substância desses Princípios encontrar aceitação ampla, então uma versão revisada poderia ser adotada, promulgada e implementada em quatro níveis:

- Globalmente, pela Conferência Internacional de Comissários para a Proteção de Dados e Privacidade (*International Conference of Data Protection and Privacy Commissioners (ICDPPC*).[3] Uma data possível seria a 40ª Conferência Internacional que terá lugar em Bruxelas em outubro de 2018.
- a nível da UE, pela Conselho Europeu de Proteção de Dados (*European Data Protection Board*)
- a nível da Ásia-Pacífico, pelo fórum das Autoridades de Proteção de Dados da Ásia-Pacífico (*Ásia-Pacific Privacy Authorities -APPA)*.
- a nível operacional, pela Rede Global de Fiscalização da Proteção de Dados (*Global Privacy Enforcement Network -GPEN)* e o Acordo Transfronteiriço para a Garantia da Privacidade da APEC (*APEC Cross-border Privacy Enforcement Arrangement -CPEA*).[4]

Estrutura deste Documento

[3] www.icdppc.org.

[4] O CPEA, disponível em http://www.apec.org/~/media/Files/Groups/ECSG/CBPR/CBPR-CrossBorderPrivacyEnforcement.pdf, é um Memorando de Entendimentos de cooperação em fiscalização, firmado entre as autoridades de proteção de dados membros da APEC. Entre outros itens, pretende-se que as autoridades participantes possam priorizar seus atos de fiscalização, tanto a nível individual como coletivo. Vide CPEA na Seção 9.2.

A Seção 1 apresenta o propósito e natureza deste documento, enfatizando a necessidade de uma abordagem estratégica para determinar as prioridades que irão entregar os melhores resultados. A seção indica os benefícios em potencial para indivíduos, DPAs e os regulados. O estudo pretende servir de ajuda para todas as DPAs globalmente, no mínimo encorajando consistência máxima para uma economia digital global. Uma atenção espeical é dado à União Europeia onde a Regulamentação Geral de Proteção de Dados (o General Data Protection Regulation - GDPR) trará mudanças relevantes na forma em que as DPAs da UE irão trabalhar individualmente e em conjunto.

A Seção 2 examina as muitas funções que recaem sobre os ombros das DPAs, em particular com referência àquelas funções alocadas pelo GDPR. A partir de maio de 2018, isso levará a um foco sem precedentes sobre as DPAs em toda a Europa. O GDPR pretende que elas tenham em torno de 22 "tarefas" distintas e uns 27 poderes definidos, mas sem cunho estratégico. Para auxiliar nas dinâmicas da priorização, as funções foram agrupadas conforme referência a quatro tipos:

1. **"Líder"** – as funções que dependem da especialização, autoridade e suporte e informações prestadas pela DPA;
2. **"Policial"** – onde houver segurança pública disponível para lidar com infrações, especialmente descumprimento deliberado ou doloso;
3. **"Processador de Reclamações"** – onde as reclamações podem levar, direta ou indiretamente, a uma sanção ou reparação;
4. **"Autorizador"** – quando algum tipo de autorização prévia da DPA for necessária.

A Seção 3 mostra os escassos recursos disponíveis para as DPAs. Para ilustrar, tomamos o exemplo da UE, onde 26 milhões de empresas estão sob a jurisdição das DPAs da UE. Os últimos números disponíveis mostram que os orçamentos para as DPAs em 26 países da UE foram em média inferior a €0.41 por cidadão e aproximadamente €8 por empresa. Outro estudo apontou que somente 9 de 19 DPAs contaram com equipe de mais de 40 funcionários em tempo integral e seis com menos que 30 pessoas em suas equipes. A seção conclui que uma chamada é necessária para aumentar os orçamentos das DPAs, sugerindo que a simples

cobrança de uma taxa anual de meros €20 de cada entidade regulada na UE poderia alavancar no mínimo €500 milhões para as DPAs da UE.

A Seção 4 analisa as evidências de regulamentação eficaz em outras estruturas regulatórias. Essa análise é feita na sua grande parte com base em uma gama de estudos recentes, especialmente a obra do Professor Christopher Hodges *A Lei e o Comportamento Empresarial*" (*Law and Corporate Behaviour)*[5]. Trata-se de uma pesquisa aprofundada das abordagens modernas com relação a regulamentação, fiscalização, cumprimento e ética. O Professor Hodges enfatiza que o melhor resultado para qualquer sistema regulatório é produzir comportamento aceitável e impedir comportamento inaceitável. Em termos práticos, uma regulamentação eficaz significa obter o cumprimento máximo por parte dos regulados. A maioria das organizações busca "acertar" quando desempenhando suas responsabilidades. Isso significa que se os reguladores estão determinados a serem eficazes, devem priorizar suas funções de suporte, formando relações abertas e construtivas entre os órgãos reguladores e seus administrados. A intimidação e punição têm eficácia limitada e devem visar principalmente aqueles que, de forma deliberada ou dolosa, descumprem a lei.

A Seção 5 é o núcleo deste estudo, buscando aplicar essas lições à regulamentação da privacidade e proteção de dados. Procura-se aqui discutir o que realmente significa eficácia e resultados. Este estudo sugere que, indo além da simples observância dos requisitos formais, a regulamentação de proteção de dados significa almejar um mundo digital onde as pessoas prosperem com dignidade como indivíduos autônomos. Assim, os resultados globais pretendidos poderiam ser desenvolvidos nas seguintes linhas:

- O impedimento do uso de dados que prejudica a qualidade de vida do indivíduo ao lhe recusar a proteção que tem por direito;
- A promoção de uma sociedade onde uma boa qualidade de vida para o indivíduo advém da proteção ampla e genuína, onde o uso de dados em um mundo digital é tanto universal como popular.

A seção detalha, no contexto do aumento de funções e dos parcos recursos, a necessidade de prioridades estratégicas para as DPAS que busquem esses

[5] https://www.bloomsbury.com/in/law-and-corporate-behaviour-9781782255826/.

resultados. Embora exista imbricamento considerável, os quatro tipos básicos de função estão agrupados e se referem aos quatro principais objetivos regulatórios: **Prever-Impedir- Detectar - Aplicar**. O conceito de uma Abordagem para Proteção de Dados com base em Resultados advém dessa análise e de evidências de outras áreas regulatórias. Sugere-se especificamente que o papel de **Liderança,** em diálogo máximo com o **Engajamento Construtivo** junto às entidades reguladas, seja a prioridade principal.

A Seção 6 apresenta o que significa Engajamento Construtivo na prática e oferece exemplos de atividades e técnicas que possivelmente produziriam os melhores resultados. Ênfase é dada a transparência, consulta, conversas francas e a aproveitar as tendências ditadas por líderes na matéria e a pressão de pares e da concorrência.

A Seção 7 apresenta uma primeira minuta dos Princípios sugeridos para uma Abordagem Baseada em Resultados e sugere como poderiam ser adotados (após extenso debate e revisão).

A Seção 8 trata de possíveis problemas, oferecendo sugestões de como lidar com as mesmas. Encontramos respostas às preocupações quanto às consequências de tratar algumas funções com baixa prioridade, os riscos de "captura regulatória" e o temor de que alguns regulados possam ter reservas quanto a uma maior proximidade com seus reguladores.

Tópicos para Discussão

Este é um documento de trabalho. Assim, questões chave foram levantadas como tópicos de discussão ao final das respectivas seções. O CIPL espera colocar oportunamente esses dez tópicos em cartas abertas aos líderes da Conferência Internacional, o *Article 29 Working Party (WP29) / EDPB (European Data Protection Board)*, o forum APPA, GPEN e a CPEA. Para fins de conveniência, os Dez Tópicos para Discussão foram agrupados na página 4 acima.

Reconhecimentos

Este documento de trabalho foi desenvolvido para ser um processo dinâmico e suas perguntas significam que se ainda procuram respostas. Inúmeras pessoas – inclusive várias que já atuaram ou estão hoje servindo em alguma função em uma DPA – deram contribuições que aperfeiçoaram este documento significativamente. Menção especial tem de ser feita à Secretaria da Conferência International de Autoridades de Proteção de Dados e Privacidade por disponibilizar dados de seu censo DPA mais recente.

Em junho de 2017, na cidade de Dublin, o CIPL realizou uma oficina com a participação das DPAs, indústria e acadêmicos para analisar uma minuta deste estudo. Todos lá concordaram quanto a importância do assunto e fizeram sugestões valiosas, especialmente articulando o que “Engajamento Construtivo” seria na prática..

O CIPL é extremamente grato a todos que ajudaram com tanta disposição neste projeto.

1. O Propósito e Natureza deste Documento de Trabalho

A proteção de dados encontra-se em uma encruzilhada. Com a quarta revolução industrial[6] e as práticas de informação em rápida evolução, bem como a nova geração de leis e regulamentos de proteção de dados, incluindo o GDPR da UE, os riscos nunca foram tão grandes.

Cada autoridade independente de proteção de dados (DPA) tem um papel crucial a desempenhar em fazer da proteção de dados uma realidade. Às vezes, no entanto, o papel geral das DPAs e suas funções específicas são assumidos sem uma análise detalhada sobre como eles deveriam ser desincumbidos na prática.

O objetivo deste documento de discussão é levantar questões sobre como - diante dos inúmeros desafios e altas expectativas - a eficácia do quadro regulatório pode ser maximizada. O documento faz isso buscando respostas a uma Abordagem Baseada em Resultados, em linha com os desenvolvimentos que ocorreram em muitas outras esferas de regulamentação. Isso envolve a adoção de uma abordagem estratégica para a definição de prioridades que entregam os melhores resultados.

O conceito e a natureza de uma Abordagem Baseada em Resultados para proteção de dados foram elaborados abaixo. Mas, primeiro, seria útil determinar quais os benefícios almejados com esta discussão. Esses benefícios podem ser agrupados da seguinte forma:

a. Benefícios para o indivíduo

O objetivo básico da regulamentação da proteção de dados deve ser proteger o indivíduo, enquanto facilita o fluxo livre de dados.[7] A regulamentação da proteção de dados promove a confiança que é essencial para o progresso e o crescimento digital, a inovação de dados e o uso benéfico de dados.

A abordagem da UE, e a de várias outras jurisdições, expressa isso em termos de defesa dos direitos e liberdades fundamentais. Em outros lugares, o objetivo é visto

[6] Consoante o Forum Econômico Mundial.

[7] Corte Europeia de Justiça exige que as DPAs implementem um "equilíbrio justo entre a proteção do direito à vida pricada e o movmento livre de dados pessoais." (Caso C-518/07 – para 30).

mais em termos de prevenção de danos ao indivíduo. Em todos os casos, há também um contexto mais amplo de "bem social". Seja qual for o idioma utilizado, o quadro regulamentar deve dar prioridade máxima à proteção de pessoas.

Qualquer marco regulatório deve ser efetivo e a eficácia deve ser avaliada principalmente em termos de impacto sobre os indivíduos. Estão protegidos na prática, não apenas no papel? Eles estão recebendo os benefícios a que têm direito? São pessoas - consumidores, cidadãos, funcionários - capazes de aproveitar ao máximo a sociedade digital com confiança que os seus interesses estão sendo devidamente salvaguardados? Eles podem esperar que as organizações, na realidade, lidem com suas informações pessoais corretamente?

Há também equilíbrios a serem avaliados em termos da sensibilidade das necessidades e desejos dos indivíduos quando se trata de órgãos comerciais e públicos. As pessoas geralmente não têm o poder, o conhecimento ou a capacidade de proteger seus próprios interesses inteiramente. Mas as características, atitudes e preferências dos indivíduos variam consideravelmente e a presunção deve ser que sejam os melhores juízes de seus próprios interesses. Além disso, as pressões do mercado e dos pares/ concorrência podem ter um grande impacto na reputação e comportamentos organizacionais. Qualquer órgão regulador deve ter cuidado para evitar sugerir que "conhece melhor" quando se trata de decidir os melhores interesses das pessoas. Uma abordagem moderna dá precedência para proteger e fortalecer os indivíduos, e não é condescendente nem desempodera os mesmos.[8]

Um foco nas pessoas também é vital para se comunicar em linguagem simples com a mídia com o objetivo explícito de promover a conscientização pública e construir suporte popular para atividades de proteção de dados.[9] A menos que as pessoas entendam a importância da proteção de dados e possam relacioná-la com suas próprias vidas, ela nunca será totalmente eficaz.

b. Benefícios para as DPAs

As DPAs enfrentam muitos desafios. Tornaram-se, de fato, os principais reguladores da sociedade digital e os dados que os impulsionam. Espera-se que exerçam o

[8] A Estratégia EDPS contém um compromisso bem vindo de comunicar até os conceitos difícieis em linguagem simples e clara.
[9] Conforme determinado no Art. 57(1)(b) GDPR.

controle sobre milhões de organizações - grandes, médias e de pequeno porte, operando em setores privados, públicos e terciários e muitas vezes para além das fronteiras nacionais. Tecnologia inovadora se desenvolve diariamente. Os indivíduos estão se tornando cada vez mais expressivos sobre suas expectativas de privacidade e uso de dados responsáveis. As DPAs devem equilibrar muitas tarefas e potenciais objetivos de políticas públicas concorrentes - proteção de dados, outros direitos fundamentais (incluindo a liberdade de expressão), o livre fluxo de informação , inovações, benefícios sociais, segurança e assim por diante.

Além disso, em termos absolutos e em comparação com a maioria das outras áreas de regulamentação, as DPAs contam com escassos recursos. Um desafio fundamental para qualquer DPA é como maximizar a eficácia quando há tanto que eles podem fazer e tão pouco recurso para fazê-lo. Os recursos podem ser aumentados em situações individuais, mas não é controverso afirmar que os recursos nunca serão adequados. As DPAs também devem manter sua credibilidade e sua legitimidade. Não tem como as DPAs fazerem tudo.

O que se procura, então, são abordagens que aumentem a eficácia e a influência das DPAs e fazem o melhor uso possível dos recursos disponíveis, concentrando-se nas atividades reguladoras que prometem os melhores resultados. Dito de outra forma, a credibilidade e até mesmo a legitimidade das DPAs podem ser questionadas se não tomarem medidas ativas para maximizar a eficácia.

A necessidade de abordagens consistentes torna-se ainda maior com as demandas de cooperação e colaboração transfronteiriças. A globalização dos fluxos de dados e a necessidade de proteger os direitos dos indivíduos a nível mundial devem ser acompanhadas de esforços voltados a harmonizar os deveres e os poderes das DPAs. Na União Europeia, o GDPR está trabalhando nisso.

Para que essas ambições funcionem de forma eficaz, será necessário ter a máxima clareza sobre as estratégias e as prioridades de todas as autoridades participantes. Uma Abordagem Baseada em Resultados não significa uma abordagem padronizada e de tamanho único. Mas significa, sim, que pelo menos a comunidade internacional das DPAs deve ter a confiança de que irão atuar de forma complementar e convergente. Embora as DPAs operem em diferentes sistemas legais e façam parte de diferentes culturas reguladoras, é essencial no mundo digital

sem fronteiras que as prioridades das DPA sejam mutuamente consistentes e mais fluidas quanto possível. Isso também irá melhorar o uso eficiente dos recursos da DPA.

Dentro da UE, essas necessidades são ainda mais evidentes. O mecanismo de cooperação e consistência introduzido pelo GDPR precisará de consistência entre as prioridades e as abordagens de *enforcement*, tanto quanto a consistência da interpretação legislativa.

A coordenação internacional já demonstrou o seu potencial com iniciativas como a Rede Global de Enforcement da Privacidade (GPEN) e o Acordo de Enforcement da Privacidade Transfronteiriça da APEC (CPEA), com investigações coordenadas e uma Varredura Internacional da Internet.

Também vimos esforços maiores para cooperar com consumidores, concorrência, telecomunicações e outros órgãos reguladores. A Autoridade Europeia para a Proteção de Dados (EDPS) propôs o estabelecimento de uma Câmara de Compensação Digital para "reunir as agências das áreas da concorrência e da proteção dos consumidores e dos dados, dispostos a compartilhar informações e a discutir a melhor maneira de aplicar as regras nos interesses do indivíduo". A primeira reunião da câmara de compensação ocorreu em maio de 2017.[10]

c. Benefícios para os Regulados

Todas as organizações - grandes e pequenas empresas, governos, agências públicas, ONGs - digitalizam suas atividades, produtos e serviços; processando dados pessoais e sendo regulado em maior ou menor grau pelas leis de proteção de dados. Por sua natureza, as leis nem sempre podem ser claras e muitas vezes são baseadas em princípios e elementos contextuais. No entanto, os regulados precisam saber como se comportar e quais ações devem praticar para proteger os

[10] https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en.

indivíduos e quais comportamentos eles devem evitar. Todos os regulados, sejam eles grandes organizações, PMEs ou start-ups precisam e têm o mesmo direito a toda a coerência e previsibilidade possível dos órgãos reguladores dentro e para além das fronteiras nacionais. Isto é especialmente importante, dada a crescente velocidade dos desenvolvimentos tecnológicos e as leis modernas de proteção de dados, colocando um peso cada vez maior na responsabilização e na gestão de riscos.

Um marco regulatório eficaz para a economia digital - com fluxos de dados fluidos e gratuitos, mas bem ordenados - é essencial para promover a inovação, o crescimento econômico e a prosperidade. A regulamentação não deve, no entanto, impor encargos desproporcionais, especialmente onde os custos são repercutidos em preços mais altos, salários mais baixos ou impostos mais elevados.

d. Global em Geral, Europa Especificamente

As DPAs em todo o mundo têm muito mais em comum do que as diferenças detalhadas que podem separá-las. A análise e as sugestões deste documento são, portanto, pretendem ser útil para todas as DPAs, para pelo menos incentivar a consistência máxima para uma economia digital global.

Ao mesmo tempo, as atividades das DPAs na UE serão transformadas em breve muito significativamente pelo GDPR. Isso terá grandes implicações para as DPAs na EU, mas também para outras DPAs que serão direta ou indiretamente afetadas pelo GDPR. A reformulação das funções da DPA - e em particular o *one-stop-shop* (centralização) com uma DPA principal e os mecanismos juridicamente vinculativos de cooperação e consistência - cristaliza a necessidade de um consenso máximo sobre como maximizar a eficácia. Todas as DPAs da UE precisarão reajustar as suas prioridades estratégicas e fazê-lo de forma consistente em toda a UE. Conforme forem enfrentar os desafios, o CIPL espera que a análise e as sugestões apresentadas neste documento sejam especialmente úteis para essas DPAs, para o WP29 e (oportunamente) para a EDPB.

Pode-se esperar que a abordagem da UE nos próximos anos tenha um efeito significativo no resto do mundo. Embora este documento, por conseguinte, ilustre muitos dos seus pontos por referência ao GDPR e antecipe que a EDPB poderia

assumir a liderança na adoção das suas sugestões, ressaltamos que a abordagem global não se limita ao contexto europeu.

2. Funções das Autoridades de Proteção de Dados

Embora os detalhes das funções DPA específicas variem em todo o mundo, existem grandes semelhanças. Em 2001, a Conferência Internacional dos Comissários para Proteção de Dados e Privacidade adotou processos e critérios formais para reconhecer as credenciais das autoridades de proteção de dados.[11]

Grande peso foi associado à verdadeira independência e autonomia das DPAs. Elas podem ser independentes e autônomas, mas precisam desempenhar suas tarefas em prol do interesse público. No caso *Commission x Alemanha* em 2010,[12] a Corte Europeia de Justiça enfatizou a forma como as DPA se enquadram no sistema de controles, pesos e contrapesos numa democracia baseada no Estado de Direito.

As DPAs podem ser vistas como corpos "híbridos", que asseguram que as organizações atinjam suas obrigações, que os direitos dos indivíduos sejam respeitados e (mais em termos gerais) que altos níveis de privacidade e proteção de dados sejam mantidos em toda a sociedade. Seu objetivo estratégico pode ser descrito em termos de equilibrar a proteção dos direitos fundamentais - ou a prevenção de danos - com o fluxo livre e o uso benéfico da informação. Na UE, a Corte Europeia de Justiça descreveu a essência da tarefa DPA como sendo "estabelecer um equilíbrio justo entre a proteção do direito à vida privada e a livre circulação de dados pessoais".[13] As DPAs foram descritas como "precursoras qualificadas".[14]

Na UE, as DPA têm status constitucional com a tarefa ampla de "controlar" ou "supervisionar" o processamento de dados pessoais e assegurar o cumprimento das regras de proteção de dados.[15] Os artigos 57 e 58 do GDPR estabelecem as

[11] https://icdppc.org/wp-content/uploads/2015/02/Criteria-and-Rules-for-Credentials-Committee-and-the-Accreditation-Principles.pdf.
[12] C-518/07 - para 41-43.
[13] C-518/07 - para 30.
[14] Bennett and Raab, *The Governance of Privacy*.
[15] Article 16(2) do Tratado da União Europeia e o Article 8(3) da Declaração de Direitos Fundamentais.

funções - algumas novas - de cada autoridade de supervisão de proteção de dados. Essas podem ser vistos como uma mistura de punição e recompensa. Elas estão divididas em tarefas e poderes. Cerca de 22 "tarefas" diferentes podem ser identificadas, onde a DPA "deverá" realizar a atividade prevista. Estas são ampliadas em cerca de 27 poderes, dos quais 6 são "investigativos", 11 são "corretivos" e 10 (com alguma replicação de tarefas obrigatórias) são "autorização e assessoria".

Na realidade, o GDPR apresenta essas 22 tarefas obrigatórias e 27 poderes como uma lista de compras com pouca ou nenhuma tentativa de priorizar ou indicar como elas se relacionam, nem qualquer articulação sobre a missão geral de cada DPA em termos dos resultados que se espera que irá atingir. Cada função é explicável por si só, e a maioria não é controversa nem surpreendente. Em uma análise crítica, o GDPR não estabelece qualquer sentido de estratégia geral.

Todavia, nada no GDPR ou nas leis em outros lugares do mundo impede o desenvolvimento de uma abordagem mais estratégica baseada em resultados. Também é possível identificar diferentes **tipos** de função - um elemento essencial para qualquer pensamento estratégico.

Embora existam inter-relações e interdependências, sem fronteiras difíceis, o Anexo A deste documento de discussão agrupa cada uma das funções do GDPR em um dos quatro tipos mais amplos:

1. **“Líder”** – as funções que dependem da especialização, autoridade e suporte e informações prestadas pela DPA;
2. **“Policial”** – onde houver segurança pública disponível para lidar com infrações, especialmente descumprimento deliberado ou doloso;
3. **“Processador de Reclamações”** – onde as reclamações podem levar, direta ou indiretamente, a uma sanção ou reparação;
4. **“Autorizador”** – quando algum tipo de autorização prévia da DPA for necessária.

3. Poucos Recursos para as DPAs

Embora nunca sejam suficientes, os recursos disponíveis para as DPAs devem ser avaliados antes de explorar estratégias e prioridades para maximizar a eficácia da regulamentação.

a. Nível de Recursos

O levantamento comparativo mais recente dos orçamentos das DPAs foi realizado como um censo pelo ICDPPC em 2017.[16] Os dados relevantes da pesquisa são apresentados e analisados com mais detalhes no Anexo B e contra algumas das exigências impostas aas DPAs.[17]

As respostas da pesquisa incluem dados de recursos para 87 Autoridades de Proteção de Dados de 58 países. Dos países que forneceram informações sobre recursos financeiros, o orçamento total global das DPA para 2016 foi de € 887.320.351.

Para 26 países da UE,[18] os números mostram um orçamento total em 2016 de € 205.703.574 para uma população total para esse ano de 507.471.970.[19] Isto indicaria que, para todos estes 26 países como um todo, o orçamento por cidadão foi inferior a € 0,41.

Ainda mais indicativo das demandas sobre cada DPA é a necessidade de relacionar recursos com o número de organizações reguladas. O Eurostat estima que "em 2014, a economia empresarial da UE28 era constituída por cerca de 26 milhões de empresas ativas".[20] Supondo-se que praticamente todas as empresas processem dados pessoais, isso sugere que as DPAs têm um orçamento médio de cerca de 8 € apenas por empresa.

---

[16] Os dados do censo são disponibilizados mediante solicitação à Secretaria da Conferência Internacional de Comissários para a Proteção de Dados e Privacidade, https://icdppc.org/the-conference-and-executive-committee/icdppc- census/.
[17] O CIPL agradece a ICDPPC por disponibilizar os dados da pesquisa para uso neste documento antes de sua publicação formal.
[18] Faltam os números da Austria e da Corácia, sendo que os números para a Alemanha estão abaixo do valor efetivo já que somente 7 dos 16 estados germânicos forneceram dados.
[19] Números da população para os respectivos 26 paiíses da UE foram pesquisados junto ao Banco Mundial em 27 de julho de 2017, http://data.worldbank.org/indicator/SP.POP.TOTL.
[20] http://ec.europa.eu/eurostat/statistics-explained/index.php/Business_demography_statistics

O número de pessoas que compõe as equipes é outra indicação de recursos e capacidade. O recente estudo da PHAEDRA sobre *Fazendo Valer a Proteção*[21] constatou que apenas 12 DPAs na União Europeia tinham mais de 40 funcionários em tempo integral em 2015, com a maior contando com 350 pessoas e a menor com 14 na equipe. Seis das DPAs da UE tinham menos de 30 funcionários.

A limitação de recursos não é novidade e é fato totalmente reconhecido pelas próprias DPAs. Um reconhecimento coletivo recente do problema encontra-se em uma resolução[22] adotada na Conferência Europeia de Autoridades de Proteção de Dados em maio de 2015. Destacamos alguns trechos do preâmbulo e do conteúdo dessa Resolução:

- "... As Autoridades Europeias de Proteção de Dados estão sendo confrontadas com muitos novos desafios, com implicações para a forma como elas desempenham suas funções ..".

- "... As Autoridades de Proteção de Dados enfrentam cada vez mais restrições de recursos financeiros e outros, enquanto as demandas sobre elas estão aumentando".

- "... os direitos e obrigações no papel devem ser sempre exigíveis e entregáveis, caso contrário não passam de tentativas de iludir ou, pior, enganar os cidadãos".

- "[A Conferência] invoca os governos dos países europeus a assegurar que o financiamento das Autoridades de Proteção de Dados seja suficiente para atender às crescentes demandas sobre elas e garantir que os requisitos estabelecidos pelos legisladores sejam devidamente atendidos na prática".

Apesar da escala de responsabilidades que o GDPR coloca nos ombros das DPAs, o GDPR inclui poucos esforços para aumentar os recursos financeiros e humanos extremamente limitados que estão disponíveis para as DPAs. O n.º 4 do artigo 52.º prevê apenas em termos gerais que "[e] cada Estado-Membro deverá assegurar que cada autoridade de supervisão disponha dos recursos humanos, técnicos e

[21] http://www.phaedra-project.eu/wp-content/uploads/phaedra1_enforcing_privacy_final.pdf.
[22] https://edps.europa.eu/sites/edp/files/publication/15-05-20_manchester_resolution_1_en_0.pdf.

financeiros, instalações e infraestruturas necessários para o desempenho efetivo das suas funções e exercício de suas competências ... ".

Isso é pouco mais do que uma exortação geral com mais aspiração do que precisão ou obrigação real. Não é específico e será difícil de aplicar por meios legais, políticos ou outros.[23] A Comissão Europeia está pressionando os Estados-Membros a fornecerem financiamento adequado, mas não desenvolveram critérios para avaliar o que é adequado ou "necessário".

Há alguma evidência de movimento ascendente real e potencial. O orçamento do Comissário Irlandês para a Proteção de Dados foi aumentado substancialmente - o censo do ICDPPC reporta um aumento de mais de 20% para 2015-16 sozinho. Nos Países Baixos, a Autoriteit Persoonsgegevens (AP) encomendou consultores para avaliar quais os recursos necessários para cumprir suas responsabilidades GDPR. O relatório dos consultores[24] concluiu que a nova situação será completamente diferente, tendo ressaltado o aumento dos volumes e responsabilidades de reclamações e dados, a necessidade de um maior controle sistêmico e mais investigações decorrentes dos mecanismos de cooperação da UE, os custos de promover a conscientização pública e organizacional, a necessidade de consultas prévias da DPIA e os custos associados à certificação e acordos de acreditação. De acordo com este cenário, essa nova realidade poderá necessitar triplicar o efetivo de pessoal de 72 para 185-270. O relatório está atualmente com o Ministério da Segurança e Justiça e as decisões orçamentárias são aguardadas.

As indicações de aumentos de orçamento reais ou possíveis na Irlanda, nos Países Baixos e em outros lugares são bem-vindas. No entanto, a imagem geral ainda não parece estender-se além dos aumentos incrementais e continua a ser muito preocupante.

Finalmente, pouca atenção foi dada para a necessidade das DPAs de recrutar mais profissionais de tecnologia, comunicação e outros especialistas para ir além das habilidades legais que a maioria das DPAs tem.

[23] No caso da *Commission v. Austria* a Corte de Justiça da União Europeia nem considerou o argumento de que uma DPA deveria tersua própria dotação em separado he CJEU did not even adopt the argument that a DPA should have its own separate budget.
[24] https://www.tweedekamer.nl/kamerstukken/detail?id=2017D15344&did=2017D15344.

b. Recursos adicionais?

Sem sombra de dúvida, independente da abordagem adotada pelas DPAs europeias, elas precisarão de recursos adicionais. O estudo PHAEDRA[25] concluiu que "hoje- para garantir um nível adequado de proteção de privacidade e dados pessoais e para investigar e processar violações, caso elas ocorram - essas autoridades de supervisão enfrentam restrições em razão de escassez humana e / ou orçamentária ..." . Cita a visão de 2014 da Agência dos Direitos Fundamentais da União Europeia de que "o problema dos recursos representa um dos maiores obstáculos que limitam a sua atividade".

Os recursos estão muito defasados em comparação àqueles disponíveis para as autoridades de concorrência / antitruste. Um exercício recente, mas não abrangente, conduzido por Politico concluiu que "cães de guarda famintos demoram em se preparar para a maior lei de privacidade da UE".[26] Em março de 2017, Isabelle Falque-Pierrotin, em nome do WP29, enviou uma carta[27] ao Conselho de Ministros pedindo aumento de recursos para permitir que as DPAs "realizem com eficácia suas novas tarefas, treinem seus próprios funcionários, atualizem seus sistemas de TI, promovam a conscientização e prestem orientação sobre as novas regras ".

O GDPR não aborda possíveis fontes de financiamento da DPA, mas deixa isso para os Estados Membros. Existem aproximadamente três fontes possíveis:

- **Fundos governamentais** - Os fundos públicos, provenientes de impostos ou de empréstimos, formam a fonte orçamentária tradicional para a maioria das DPAs. Mas, com a maioria dos governos enfrentando desafios econômicos em uma "era de austeridade", é preciso perguntar o quão realista ou possível seria os governos nacionais providenciarem um aumento significativo de recursos públicos a mais dos recursos já disponíveis para DPAs. Além disso, onde os orçamentos dependem do financiamento governamental, especialmente onde faltam garantias constitucionais de

[25] Na página 16.
[26] http://www.politico.eu/pro/starving-watchdogs-will-police-eu-biggest-privacy-law-general-data-protection-regulation-europe/?utm_source=POLITICO.EU&utm_campaign=edc4d71000-EMAIL_CAMPAIGN_2017_04_04&utm_medium=email&utm_term=0_10959edeb5-edc4d71000-189890157.
[27] http://ec.europa.eu/newsroom/document.cfm?doc_id=43668.

orçamento suficiente, a possibilidade de uma ameaça à independência sempre existe.

• **Multas** - O GDPR contempla multas substanciais para as organizações que violem suas obrigações. Mas, qualquer tentativa de financiar DPAs diretamente das penalidades que elas mesmas impõem será fortemente contestada como implementação de incentivos distorcidos. Qualquer tentativa desse tipo será altamente controversa e aberta a desafios éticos, políticos e legais.

• **Regulamentação** - O custo da regulamentação pode ser suportado diretamente pelos regulados, seja por meio de taxas ou outros meios. Essa abordagem "o poluidor que paga" é cada vez mais comum em outras áreas de regulamentação. Alguns DPAs já recebem renda de serviços cobrados, como auditoria, treinamento e publicações. A abordagem reconhece que a regulamentação beneficia as organizações, aumentando a confiança da sociedade em suas atividades e evitando a oneração dos cofres públicos. Também pode ser administrativamente simples e barato para arrecadar. O GDPR não impediria, por exemplo, que um Estado-Membro introduzisse um requisito simples mediante o qual todas as organizações que processam dados pessoais teriam de pagar uma taxa on-line modesta, direta ou indiretamente, à DPA competente a cada ano.

Assumindo novamente que praticamente todas as empresas estão hoje processando dados pessoais, uma taxa nominal de apenas € 20 cobradas das 26 milhões de empresas na UE geraria um orçamento total de € 520 milhões por ano - um enorme aumento de recursos. O total seria ainda maior se a taxa fosse mais para organizações maiores.[28]

TÓPICO PARA DISCUSSÃO

1. Quais outros caminhos devemos estudar para aumentar os orçamentos das

[28] No Reino Unido, mais de 400,000 controladores de dados estão registrados. A taxa para as organizações maiores é £500.

DPAs para níveis mais realísticos?

4. Regulamentação eficaz

O desafio da eficácia é obter os melhores resultados de qualquer recurso disponível. A proteção de dados não existe no vácuo e há muito a aprender com a experiência em outras esferas reguladoras. Muitos estudos de eficácia regulatória surgiram nos últimos anos - e a Bibliografia menciona alguns desses. Infelizmente esses estudos têm largamente ignorado a proteção de dados e, por sua vez, talvez não tenham sido suficientemente levados em consideração pela comunidade de proteção de dados.

Antes de discutir o que uma Abordagem Baseada em Resultados para regular a proteção de dados pode parecer, esta seção se baseia em uma série de estudos significativos.

a, Temas-chave

Embora não exista um consenso único sobre "o que funciona melhor", e o pêndulo regulatório balance para lá e para cá, uma série de temas-chave podem ser identificados. Esses incluem:

• A prática regulatória - o comportamento dos reguladores - é tão importante quanto o conteúdo das leis e regulamentos.

• objetivar a obtenção de resultados bem definidos - ou regulamentação baseada em resultados - é hoje amplamente reconhecido como um princípio regulatório de alto nível. Em outras palavras, qualquer modelo efetivo de entrega regulamentar deve focar, na medida do possível, nos resultados, indo mais além do que "aplicação da lei" e resistindo as pressões para buscar *o compliance* por sua própria causa ou para impor prescrição regulamentar excessiva.

• Reguladores eficazes adotam uma "abordagem baseada em risco". Isso significa que o quadro de supervisão, incluindo a interpretação e a execução, é direcionado para gerenciar os principais riscos para os objetivos regulatórios.[29]

• Os reguladores efetivos selecionam a abordagem mais apropriada de uma ampla gama de ferramentas de produção de *compliance* (conformidade), engajando-se com os regulados e preferindo sempre que possível o "compliance voluntário" em lugar de imposição. Esta abordagem torna-se ainda mais relevante quando os regulados precisam ser ou se espera que sejam responsáveis.

• Eles também exploram uma variedade de alavancas além de seus próprios poderes formais para garantir que os padrões sejam mantidos. Essas alavancas incluem as influências que vêm de usuários, consumidores e cidadãos (especialmente onde eles podem fazer escolhas em um mercado competitivo e arenas democráticas), da pressão dos pares entre os regulados, das mídias convencionais e sociais e da esfera política.

b. Direito e Comportamento Empresarial

Um dos estudos mais recentes e abrangentes desenvolve mais esses temas e vale a pena citar com mais detalhes. Em seu livro de 2015, Direito e Comportamento Empresarial,[30] o Prof. Christopher Hodges, professor de sistemas de justiça na Universidade de Oxford, reúne cerca de 800 páginas de evidências e análises para

[29] Isso é especialmente relevante para as disposições com base em risco da GDPR. Veja também *"A Risk-based Approach to Privacy: Improving Effectiveness in Practice*", CIPL 2014, disponível em http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf; e "*Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR"*, CIPL 2016, disponível em http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf.

[30] Na página 8.

informar a discussão sobre regulamentação eficaz. Nas palavras de seu subtítulo, trata-se de "integrando teorias de regulamentação, execução, *compliance* e ética".[31]

O Prof. Hodges, posteriormente, avançou o conceito de “Regulamento da Empresa Ética” ("Ethical Business Regulation" (EBR), que, com base em dados empíricos sobre o porquê as pessoas observam ou quebram as regras e sobre como a cultura pode apoiar a melhoria contínua e a inovação, visa construir sucesso comercial no cumprimento dos valores sociais.[32]

Compliance ao máximo

Hodges argumenta que a regulamentação é fundamentalmente sobre o comportamento. O resultado ideal é produzir comportamentos aceitáveis e parar comportamentos inaceitáveis. Em termos práticos, a regulamentação eficaz significa garantir o máximo de *compliance*.

Um conjunto substancial de evidências demonstra como os reguladores nas democracias contemporâneas devem procurar como melhor afetar o comportamento empresarial, a fim de garantir o máximo de *compliance*. Isso inclui os resultados de psicologia comportamental e análise de incentivos econômicos e culturais. A regulamentação, por si só, não consegue alcançar *o compliance*, especialmente porque é fortemente influenciada pela pressão do cliente, pelo comportamento dos concorrentes, por comentários de mídia e por considerações de reputação. As normas sociais, os valores éticos e a pressão dos pares também desempenham partes importantes. O interesse próprio esclarecido - onde o *compliance* é visto como oferecendo um caminho para aumentar a rentabilidade ou o cumprimento de outros objetivos empresariais - é muitas vezes um fator dominante.

A regulamentação eficaz envolve o aproveitamento dessas forças e outras similares, sem resistir às mesmas nem trabalhando isoladamente delas.

A Abordagem Moderna para Regulamentação

[31] Um resumo breve dos temas chave está disponível em https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/497539/16-113-ethical-business-regulation.pdf.

[32] *Ethical Business Regulation; Growing Empirical Evidence*, Christopher Hodges, Wolfson College, University of Oxford.

A essência de uma democracia moderna baseia-se no respeito pelos outros, não menos expressa através do apoio aos direitos humanos fundamentais. Aplicar essa política a uma economia de mercado vibrante produz o resultado de que a sociedade apoia negócios honestos para melhorar o bem comum. Negócio honesto e uma sociedade harmoniosa funcionam com base na confiança. Por conseguinte, um objetivo fundamental da regulamentação é permitir uma confiança generalizada nas empresas, com base em que uma economia saudável, sustentável e crescente pode existir, o que, por sua vez, apoia o emprego, a estabilidade social e a inovação. Essa filosofia é igualmente aplicável sejam os objetivos regulatórios primordialmente econômicos ou sociais.

Em consonância com essa ampla filosofia, a regulamentação mais moderna ultrapassou o modelo histórico - onde um poderoso indivíduo ou organização "comanda e controla" as ações de inferiores, exercendo autoridade através de punições severas ou temidas sobre aqueles que não obedeceram. Agora é universalmente aceito - e geralmente legalmente executável - que, mesmo que os órgãos reguladores detêm um poder significativo para fazer cumprir a lei, eles devem agir de forma justa e proporcional, observar o devido processo legal e serem responsáveis por suas ações.

A abordagem moderna, inevitavelmente, também exige um bom entendimento sobre o porquê das organizações e as pessoas se comportarem de determinada maneira e como elas podem ser ajudadas a melhorar.

Pesquisas empíricas descobriram que as pessoas obedecem a regras quando:

a. as regras correspondem a sistemas de valores reconhecidos;

b. as regras foram feitas de forma justa; e

c. as regras são aplicadas de forma justa.

Regulamentação Responsiva

Uma grande pesquisa agora endossa a regulamentação "responsiva", onde a ênfase é no engajamento através de informações, recomendações e apoio, em vez

de dissuasão e punição. A pesquisa cobriu uma ampla gama de atividades reguladas, incluindo saúde e segurança ocupacional, poluição da água, proteção ambiental, indústria de mineração, processamento de alimentos, cuidados para idosos e aviação civil.

Resultados, não Compliance

Em resposta a taxas de acidentes obstinadamente elevadas na construção civil na década de 1990, o regulador do Reino Unido (o Health & Safety Executive (HSE)) decidiu por uma nova abordagem – onde os envolvidos passariam a ter a responsabilidade pelo problema. Em vez de inspeções de cada site em dezenas de milhares de sites de construção, a nova abordagem envolveu alavancar a influência em áreas de alto risco e engajar e formar parcerias com partes dentro da indústria capazes de afetar mudanças generalizadas.

A abordagem obteve grande sucesso. De 2000-01 a 2012-13, o número de acidentes fatais e graves caiu de 4.410 para 2.161 (49%).

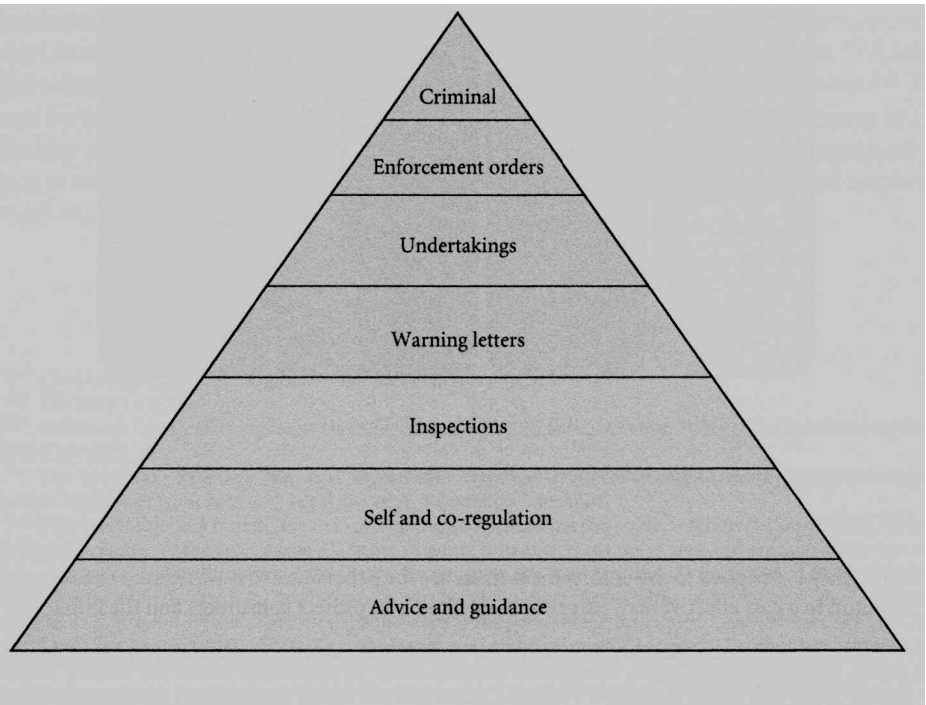
Um estudo comparando as políticas de *enforcement* de vários países com as mesmas leis ilustrou claramente que a diferença de eficácia não está nas regras, mas na abordagem das autoridades.[33] A abordagem do Reino Unido reduziu permanentemente a ocorrência de graves incidentes de segurança. A mesma abordagem foi seguida na Alemanha, com o mesmo resultado. A abordagem na França, no entanto, ainda depende de inspeções e penalidades por descumprimento das regras. O "x da questão" ali é ter as empresas passarem as inspeções, não para tornar os locais de trabalho seguros. O histórico de segurança no local de trabalho da França permaneceu um dos piores da Europa.[34]

A experiência nestes e em outros campos enfatiza os benefícios de uma cultura em que os reguladores adotam uma abordagem positiva e pró-ativa para garantir *o*

[33] F Blanc, *From Chasing Violations to Managing Risks. Origins, challenges and evolutions in regulatory inspections* (Edward Elgar, a ser publicado).
[34] Ibid.

compliance. Isso envolve reguladores que realizam suas atividades de forma a apoiar e ajudar aqueles que eles regulam a cumprir. Em particular, deve ser dada alta prioridade a garantir que informações claras, orientações e recomendações estejam disponíveis para ajudar as organizações a cumprirem suas responsabilidades. Esse apoio é ainda mais importante para as PME, onde a pesquisa indica que eles geralmente acreditam que estão cumprindo a lei até que uma pessoa que eles respeitem (por exemplo, um órgão regulador ou sindicato) aponte que eles poderiam melhorar, após o que eles geralmente acatam a recomendação.

Regulamentação Responsiva - a abordagem da Autoridade de Aviação Civil do Reino Unido[35]



[do topo para a base da pirâmide: criminal, ordens de execução, ajustes de conduta, avisos de alerta, inspeções, auto-regulamentação e co-regulamentação, aconselhamento e orientação]

c**. Conclusões de outras áreas de regulamentação**

A partir das evidências e esta análise, o Prof Hodges chegou a cinco conclusões básicas:[36]

1. Um sistema regulatório é mais efetivo onde é consistente e apoia comportamentos que são considerados justos, proporcionais e éticos.

[35] A Política Regulatória de Fiscalização CAA (*CAA Regulatory Enforcement Policy*), baseada no modelo "responsivo" de regulação desenvolvido pelo Prof John Braithwaite, conforme citado na obra *Law and Corporate Behaviour*.
[36] Itens desenvolvidos no Anexo C.

2. As organizações devem ser responsáveis por comprovar seu compromisso com comportamentos que atrairão a confiança dos reguladores, bem como sua própria administração e equipe, clientes, fornecedores, investidores e outras partes interessadas.

3. O aprendizado é fundamental e é encorajado pelo engajamento aberto e construtivo entre reguladores e organizações reguladas, mas fica prejudicado quando houver ênfase na "culpa" e / ou punição.

4. Os sistemas reguladores devem basear-se no diálogo e na cooperação mútua, que são explicitamente orientados para maximizar o *compliance*, a prosperidade e a inovação.

5. Quando as organizações quebram as regras, é necessária uma resposta proporcional, com as penas mais duras reservadas para delitos deliberados, repetidos ou intencionais.

TÓPICO PARA DISCUSSÃO

1. Quais são as lições que podemos tirar das abordagens adotadas ao redor do mundo em muitas outras áreas de regulamentação**?**

5. Uma Abordagem Baseada em Resultados para a Regulamentação da Proteção de Dados

As evidências e análises contidas em vários estudos, resumidas acima, estão em linha com o pensamento assunto-específico que está começando a emergir na comunidade de proteção de dados. Tanto as DPAs quanto as organizações reguladas entendem, cada vez mais, que *compliance* faz parte da responsabilidade e sustentabilidade corporativa.

Enquanto a nossa sociedade digital se transforma através da quarta revolução industrial, surge um novo ecossistema de proteção de dados – baseado em organizações responsáveis e reguladores efetivos baseados em resultados.

A nível da UE, há um reconhecimento crescente dos desafios fundamentais para as DPAs que podem ser resumidos em termos simples:

- A partir de maio de 2018, as funções das DPAs aumentarão de forma substancial;
- Os recursos das DPAs são poucos para as funções existentes, e serão insuficientes para atender a larga gama de tarefas previstas pelo GDPR [Regulamento Geral sobre a Proteção de Dados];
- Há pouco ou nada em termos de previsão para aumentos nos recursos governamentais; e
- Até mesmo aumentos importantes não diminuiriam a necessidade de abordagens estratégicas.

A fundação da responsabilidade organizacional sendo o fator impulsionador de *compliance* em termos da privacidade de dados, que o CIPL articulou durante muitos anos e que foi reconhecido oficialmente no Parecer sobre o Princípio da Responsabilidade do WP29,[37] agora é o foco central do GDPR. A responsabilidade também é considerada essencial nas diretrizes da OCDE sobre a privacidade. No mundo inteiro, a orientação dada pelas autoridades de proteção de dados do Canadá, Hong Kong e Austrália ao programa de gerenciamento da privacidade tem sido bem recebido e influente, bem como as referências à responsabilidade nas leis de proteção de dados mexicana e colombiana.

[37] Parecer 3/2010 sobre o princípio da responsabilidade, WP 173.

Em 2015, a Autoridade Europeia para a Proteção de Dados (EDPS) publicou seu Parecer, *Towards a New Digital Ethics* (Rumo a uma nova ética digital**)**,[38] que foi uma extensão das atividades da EDPS, encorajando sinergias com as leis de proteção dos consumidores e leis sobre a concorrência.[39] O Parecer de 2015 prevê um regime efetivo de proteção de dados em termos de um "ecossistema" onde todos os atores relevantes (mas principalmente as DPAs e controladores) atuam melhor em conjunto para reforçar os direitos.

A importância do interesse próprio esclarecido como impulsionador do comportamento empresarial vem sendo estudado de maneira explícita pelo antigo comissário interino de privacidade do Canadá. No seu documento para discussão, Chantal Bernier[40] mostra a maneira pela qual o conceito de "Licença Social para Operar" (SLO) poderia se tornar "o fator mais forte para garantir *compliance* com as leis sobre a privacidade". Esse documento defende o caso de tratar a aceitabilidade social como fator comum entre reguladoras e empresas, sobretudo na medida em que as pessoas se tornem mais assertivas nas suas expectativas, e as empresas se tornem mais preocupadas com os impactos da reputação sobre o manuseio de dados no balanço.

Mais recentemente, uma reportagem[41] publicada pela Câmara de Comércio dos EUA, em fevereiro de 2017, defendeu que os riscos e desafios oriundos da ubiquidade e crescente valor dos dados na econômica global, fazem com que seja imprescindível entender como regulamentar a proteção de dados de maneira eficaz. Porem, um estudo das DPAs no mundo inteiro demonstra que "suas metodologias, práticas e escopo de autoridade variam muito". A reportagem conclui que ".o tema comum entre todas as DPAs é que as DPAs realmente eficazes tratam os regulados como parceiros em vez de adversários". Com uma abordagem que corresponde à análise e às sugestões contidas neste documento do CIPL, a reportagem identifica sete Atributos Chave para a governança eficaz da proteção de dados. Eles colocam forte ênfase na educação, conscientização, orientação e assistência.

---

[38] EDPS Parecer 4/2015.
[39] Por exemplo: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf
[40] *The Concept of Social Licence to Operate: A Common Ground to Apply Privacy Law? - Dentons, Ottawa*.
[41] *Seeking Solutions*, US Chamber of Commerce, Feb. 2017, https://www.uschamber.com/sites/default/files/023052_dataprotectionhuntonpaper_fin.pdf.

a. Eficácia

Não há consenso estabelecido sobre o que significa a eficácia no contexto de proteção de dados. A nível geral, há referências frequentes a conceitos tais como “defender os direitos fundamentais das pessoas”, “conseguir um alto nível de proteção de dados” ou “garantir o cumprimento das exigências”. Mas essas aspirações podem ser insubstanciais, faltando objetivos mais concretos. Da mesma forma, as referências a riscos, prioridades, metas e lemas tais como “Seletivo para ser Eficaz” não têm significado a não ser, e até que, haja clareza e concordância sobre o que significa ser “Eficaz”.

Como ponto de partida, todos os reguladores eficazes se perguntam:

- “Quais resultados estamos tentando conseguir?”
- “O que significa o sucesso?”
- “Como saberemos que fizemos um bom trabalho?”

O CIPL não tem as respostas a essas perguntas, que, de qualquer jeito, ficam para as DPAs acordarem, seja coletiva ou individualmente. O objetivo básico de proteger as pessoas, na prática, já foi discutido, mas, similar à proteção do meio ambiente, existe uma dimensão mais ampla do “bem social”. Na oficina do CIPL em Dublin, emergiu um consenso amplo sobre a importância de buscar e garantir resultados claramente articulados, em vez do simples cumprimento. Também foi reconhecido que a regulamentação realmente eficaz envolve o monitoramento e a mudança de comportamentos, e, às vezes, culturas, e não simplesmente assegurando que as formalidades e a papelada estejam em dia.

Portanto, além do simples cumprimento, regulamentar a proteção de dados significa almejar um mundo digital onde as pessoas prosperam com dignidade como indivíduos autônomos. Os resultados gerais pretendidos poderiam, assim, ser desenvolvidos nas seguintes linhas:

- O impedimento do uso de dados que prejudica a qualidade de vida do indivíduo ao lhe recusar a proteção que tem por direito;

- A promoção de uma sociedade onde uma boa qualidade de vida para o indivíduo advém da proteção ampla e genuína, onde o uso de dados em um mundo digital é tanto universal como popular.

Porém, enfatizamos que isso fica para as próprias DPAs articularem os resultados que pretendem.

b. Estabelecendo Prioridades Estratégicas

Qualquer DPA bem gerenciada precisará estabelecer prioridades claras, em geral em um Plano Estratégico transparente. Se as prioridades não forem articuladas de maneira explícita, ainda assim haverá uma priorização de fato na forma do trabalho feito e do trabalho que não foi feito. A própria Resolução da Conferência, referida acima, reconheceu a necessidade de uma abordagem direcionada:

- "Porém, não é apenas uma questão de recursos. Também, as Autoridades de Proteção de Dados deverão adotar uma abordagem sustentável a nível nacional, da UE e dos demais países europeus, para desenvolver suas funções, direcionando suas atividades para onde a necessidade de proteção de privacidade for maior…".

Isso não é fácil. Usar a bem conhecida linguagem de "direcionar" ou adotar uma "abordagem baseada em riscos" é relativamente fácil, mas é muito mais difícil ir além da retórica e desenvolver critérios, princípios ou outras medidas significativas para escolher as prioridades, as metas ou riscos que deveriam ser abordados. Isso se aplica em pelo menos duas dimensões:

- Como deveriam ser classificadas as funções (ou as tarefas ou atividades) entre si?
- A partir de uma determinada função, como selecionar aquelas que precisam de atenção dentre os diferentes setores, atividades ou organizações?

Todas as entidades regulatórias, em todos os setores e em todas as jurisdições enfrentam essas questões. As evidências de outras áreas de regulamentação, conforme resumido na seção anterior, indicam como as mesmas estão sendo respondidas. Há lições a serem aprendidas para a proteção de dados. Em

particular, existe uma quantidade considerável de evidências para orientar os processos de priorização.

A estrutura abaixo poderá ser útil em responder a essas questões:

PREVER – IMPEDIR – DETECTAR – APLICAR

Essas são metas chave para qualquer regulador, mas é preciso estabelecer o equilíbrio entre elas e onde priorizar. As evidências de outras áreas de regulamentação indicam que “Impedir” deveria ser de suma importância, apoiado por “Aplicar” quando for necessário. Uma estratégia poderá, então, ser desenvolvida ao criar relacionamento dessas metas com todas as funções da DPA.

A Abordagem Baseada em Resultados, relativa à regulamentação, envolve um máximo de engajamento com as organizações reguladas e, conforme demonstrado na tabela abaixo, a Liderança é crucial para a consecução eficaz de todas as metas:

	Líder	**Autorizador**	**Policial**	**Processador de Reclamações**
PREVER	✓			
IMPEDIR	✓	✓		
DETECTAR	✓		✓	✓
APLICAR	✓		✓	✓

Essa análise também sugere uma classificação ampla de prioridades:

1. **“Líder”** – onde a ênfase está na expertise, autoridade, influência e informações da DPA.

2. **“Policial”** – onde a ênfase está na punição, nos casos em que houve, ou talvez tenha havido, violação do regulamento.
3. **“Processador de Reclamações”** – onde a ênfase está no tratamento das reclamações das pessoas, que poderia levar, direta ou indiretamente, a uma sanção ou retificação.
4. **“Autorizador”** – quando for preciso algum tipo de autorização prévia da DPA.

c. Liderança e Engajamento

“A orientação dada às DPAs hoje irá produzir amanhã os resultados pretendidos”.

Deveria ser indiscutível a partir desta análise que o papel de Liderança – orientando para as boas práticas – é a prioridade estratégica mais elevada, e que sua importância somente poderá crescer na era moderna da informática. Ela está presente em todas as metas que precisam ser atingidas.

A liderança engloba aquelas funções que dependem da expertise e da autoridade da DPA. Uma DPA eficaz vai querer ser – e ser vista como – o líder em explicar claramente os resultados e comportamentos que espera dos regulados. Isso envolve entender o ambiente tecnológico, comercial e político, antecipando as controvérsias, interpretando a lei e fornecendo orientações que tenham uma visão do futuro e que sejam práticas e estratégicas. Embora tenham aqui um papel a fazer, não é um papel que possa ser delegado a advogados, consultores ou outros conselheiros, nem deixado nas mãos dos próprios regulados. É fundamental que as DPAs ***engajem*** diretamente em diálogos, e tomem a liderança no fornecimento de informações, recomendações e apoio, fazendo da proteção de dados uma realidade prática. As DPAs poderão alavancar as contribuições que vierem de dentro das organizações reguladas – nos setores privado e público – para ajudar a cumprir sua missão.

O engajamento exige confiança mútua e reforça o princípio de Responsabilidade do GDPR. É um processo bidirecional – com as organizações responsáveis dispostas e capazes a demonstrarem seu cumprimento, ser transparentes sobre suas próprias atividades e compartilhar conhecimento sobre as tendências e inovações tecnológicas e comportamentais. Embora a liderança envolva primariamente diálogo com os regulados, as informações, recomendações e conscientização para os membros da sociedade também têm aqui seus papeis para desempenhar.

Exemplos de Engajamento das DPAs

- O WP29 tomou a medida muito bem vinda de consultar sobre minutas de Opiniões e Orientações antes que sejam adotadas. Exemplos recentes incluem autoridades principais, portabilidade de dados e as DPAs.

- Várias DPAs têm discutido questões sobre a Inteligência Artificial (IA) com empresas interessadas e, agora, reconhecem que uma abordagem que requer "transparência dos algoritmos" poderá ser menos produtiva do que uma ênfase em "Responsabilidade e Verificações Específicas de IA".

- Os "*FabLabs*", organizados pelo WP29 para discutir a implementação do GDPR, têm sido muito bem vindos.

- A EDPS tem um programa estruturado de visitas de alto nível às instituições da UE as quais supervisa. Essas visitas resultam frequentemente em um roteiro acordado para o *compliance* "voluntário", o que evita a necessidade de execução formal.[42]

- A EDPS também consulta com frequência as DPAs sobre minutas das Orientações.

[42] Vide relatórios anuais sucessivos da EDPS.

- A iniciativa "*Pack de conformité"* da CNIL [*Commission Nationale de l'Informatique et dês Libertés*] convidou empresas de determinado setor para, juntos, definirem com o CIPL as melhores práticas para a proteção de dados para tal setor e para simplificar as formalidades administrativas.

- A FTC [*Federal Trade Commission*] dos EUA promove workshops e consultas temáticas frequentes sobre novidades tecnológicas específicas ou temas que visam o futuro, para solicitar contribuições e compartilhar aprendizagens com atores, acadêmicos e líderes chave.

- As DPAs que participam das reuniões bianuais da APPA, convidam com frequência organizações reguladas para compartilhar conhecimentos sobre temas chave de interesse para os reguladores.

Cada vez mais as DPAs reconhecem os benefícios de engajamento e cooperação com as organizações reguladas, sobretudo aquelas organizações que seguem uma abordagem responsável para *compliance*. Embora existam, é claro, muitos "tons de cinza", é amplamente reconhecido que poucas organizações estejam tentando evitar proativamente o *compliance*. Embora muitas, sobretudo as SMEs, tenham dificuldades por causa de desconhecimento, a maioria dos regulados aceita que deveria cumprir com suas obrigações legais. Muitas das organizações maiores adotaram programas elaborados de gerenciamento da privacidade para prover autoconfiança eficaz ou "reconhecimento merecido", indo além da síndrome mais tradicional de "papelada da privacidade", onde os esforços raramente foram além de políticas acumulando poeira na prateleira. Essas tendências têm o apoio do GDPR com sua ênfase em Responsabilidade e Gerenciamento de Risco e sua promoção de planos de Certificação e selos. No mínimo, um programa compreensivo de proteção deveria mostrar evidências de tentativas sérias para conseguir o *compliance*.

Outra parte do papel de liderança das DPAs é encorajar as organizações a adotarem estruturas de responsabilidade e incentivar bons comportamentos. Isso pode ser feito provendo formalmente mitigações para aquelas organizações que conseguirem demonstrar responsabilidade sustentada, ou simplesmente por meio

de divulgação de exemplos de melhores práticas para criar momentum no mercado e pressão dos pares para os outros acompanharem. Por exemplo, a PDPC de Cingapura, na ocasião da grande conferência internacional e a Semana Cingapura DP, em 2016, distribuiu uma cartilha simples que destacava as melhores práticas de meia dúzia de organizações em Cingapura, desde grandes empresas multinacionais até organizações do setor público e startups locais.

Ao mesmo tempo, as DPAs precisam ser sofisticadas na sua abordagem. Por exemplo, deveriam entender os princípios e a lógica do gerenciamento de risco e do melhoramento contínuo de políticas e procedimentos de compliance, sem usar os mesmos como provas de fraqueza, que as organizações reconheceram abertamente mas, de maneira justificada, trataram como de baixa prioridade. Da mesma maneira, orientação das DPAs sobre atividades mínimas, de baixo risco, provavelmente será bem vinda como parte de uma abordagem baseada em risco.

d. Policial

O papel do Policial – investigando, ameaçando ou entrando em ação contra organizações que não estejam em conformidade – é importante, mas – se resultados comportamentais bem difundidos é o que se pretende, então não deveria ser a prioridade mais alta e não deveria ser a primeira ação de qualquer DPA. As evidências resumidas na seção 4 acima indicam que essa atitude seria tanto ineficaz quanto contraproducente. Há riscos significativos de que os regulados adotarão atitudes defensivas, mais reservadas ou abertamente hostis, que provavelmente não melhorarão os resultados para aqueles que, supostamente, estão sendo protegidos. Recursos escassos poderiam, facilmente, acabar sendo desviados para batalhas longas nos tribunais. Nenhum regulador pode esperar ser eficaz se sua primeira opção é governar pelo temor.

Isso não quer dizer que não seja para aplicar a lei. Às DPAs ao redor do mundo, em anos recentes, foram dadas dentes muito mais afiados, particularmente pelo GDPR que prevê multas de até 20 milhões de euros ou 4 % da receita anual mundial. Essas penalidades aumentam a credibilidade e legitimidade, e fazem com que as mentes das pessoas se concentrem. A possibilidade de ações para fazer cumprir e

penalidades mais fortes certamente irão influenciar muitas organizações, sobretudo quando houver prejuízos comerciais ou à reputação. As DPAs terão que exercer seus poderes de punição de vez em quando para não perder a relevância, mas, é claro, com o devido respeito à proporcionalidade. Quando ações decisivas forem tomadas, sobretudo quando há multas enormes envolvidas, é fácil atrair a atenção (incluindo via canais políticos e da mídia).

Certas violações poderão ser tão sérias que as sanções serão inevitáveis. Porém, evidentemente, os principais alvos para a enforcement da lei (preferivelmente estabelecidos como meta explícita) deveriam ser aquelas organizações que estiverem envolvidas em atividades dolosas, deliberadas, seriamente negligentes, reincidentes ou gravemente negligentes em desconformidade com a lei. Essa abordagem é consistente com o GDPR, que inclui fatores múltiplos a serem levados em conta ao decidir se haverá multa e o valor da mesma. Esses incluem a gravidade da violação, seu caráter intencional ou negligente, e quaisquer outras violações relevantes anteriores.[43] Na maioria dos casos, algum tipo de aviso seria desejável, tanto para alertar a organização quanto para facilitar a decisão da DPA de demonstrar intenção ou negligência. Se uma DPA pretender ter sucesso como Líder, o uso da 'vara' é razoável, sobretudo em situações em que avisos sobre comportamento infringente tenham sido ignorados, e exista um risco real de prejuízos às pessoas.

e. Processador de Reclamações

Embora a lei da UE considere o mecanismo de reclamações como elemento importante do direito do indivíduo à proteção de dados, e que o processamento de reclamações também esteja incluído em algumas leis sobre a proteção de dados ao redor do mundo, não é usual em outras esferas de regulamentação, que uma entidade reguladora acumule também funções de processador de reclamações.

Na UE, o GDPR estabelece como obrigatório que uma DPA "processe" as reclamações. Isso não é novo e, na lei vigente da UE, as reclamações devem ser

[43] GDPR, Article 83(2).

processadas de forma diligente, uma questão que estava no cerne do caso *Schrems*.[44]

Porém, problemas sérios e ameaças à eficácia podem surgir, se ao papel de Processador de Reclamações for atribuído uma prioridade excessiva ou se não for bem gerenciado. Primeiro, esse papel é impulsionado pela demanda – que fica fora do controle das DPAs – e pode exigir muitos recursos, prejudicando as outras funções. Se os casos não forem selecionados cuidadosamente, corre-se o risco de desviar o olhar da atividade mais estratégica e (não importa quão bem feito seja) o processamento de reclamações em massa raramente conseguirá os resultados comportamentais desejados em todo um setor. Em vez de focar nas reparações de determinados indivíduos, os reguladores deveriam se concentrar em proteger os direitos de maneira mais universal, antes de algo dar errado. Há riscos reais de se criar um ambiente de decepção ou desilusão da sociedade – seja por causa de atrasos ou por resultados indesejáveis – prejudicando o apoio popular que as DPAs precisam.

Isso não significa que o Processador de Reclamações deveria – ou poderia – ser totalmente ignorado. O GDPR impõe um dever nas DPAs de "processar e investigar" reclamações. Mas isso implica uma competência ampla. "Processar" é um conceito flexível que não está explicado em detalhe. O artigo 57(1)(f) do GDPR exige que a investigação seja "na medida apropriada", o que, sem dúvida, permite acordos de triagem, distinções entre tipos diferentes de reclamação, prioridade para os casos mais sérios e o encaminhamento para outro órgão quando apropriado.

Uma Abordagem Baseada em Resultados deveria envolver vários elementos relativos às reclamações:

- O papel de Processador de Reclamações deve ser bem gerenciado para evitar que a DPA fique sobrecarregada;
- As DPAs precisam saber dos riscos à eficácia geral criados pelo desvio e o uso ineficiente de recursos;
- O valor das reclamações como fonte de inteligência deve ser destacado;

[44] Caso C-362/14, Schrems, EU:C:2015:650.

- Consultas e pedidos de informação devem ser separados das reclamações reais;
- Critérios objetivos devem ser desenvolvidos para poder decidir quais reclamações devem ser “processadas e investigadas” em passo além do reconhecimento e monitoramento;
- Acordos robustos de triagem devem ser introduzidos para garantir que os critérios sejam aplicados de maneira consistente e justa;
- As DPAs devem identificar rapidamente as reclamações abusivas, frívolas ou de má fé;
- Os reclamantes devem ser encorajados (ou, quando possível, direcionados) a planos de Resolução Alternativa de Controvérsias (ADR)[45], que poderão oferecer soluções;
- os reclamantes devem ser encorajados a, primeiro, dirigir suas reclamações para a organização envolvida, que, como organização responsável, deveria ter políticas e procedimentos para o processamento de reclamações e ter a capacidade de lidar efetivamente com a reclamação; e
- Os programas de certificação e selo devem ser encorajados a oferecerem procedimentos de resolução de controvérsias de terceiros.

Tudo isso aliviaria o peso nas DPA de lidar com um grande número de reclamações que poderiam ser melhor resolvidas na fonte ou através de mecanismos de ADR. Isso permitiria que as DPA se concentrassem em reclamações mais graves ou naquelas que não foram resolvidas pela organização em questão.

As DPAs devem, em todo caso, publicar suas políticas de recebimento de reclamações. Com essa abordagem, e de acordo com os princípios de "extensão apropriada" e "forma diligente", uma atenção detalhada pode ser direcionada, por exemplo, para as reclamações que:

1. indicam cumulativamente uma desconformidade generalizada afetando muitas pessoas;

[45] Vide também o regulamento mais recente da UE para resolução de controvérsia consumerista (*Consumer Alternative Dispute Resolution (CADR*).

2. indicam um prejuízo particularmente grave para o reclamante;

3. alegam uma falta de *compliance* grave e contínua;

4. poderiam levar a melhorias essenciais no comportamento organizacional; ou

5. indicam que um importante ponto de princípio precisa ser discutido.

Uma abordagem nestas linhas é um uso eficiente de recursos escassos que também trata as reclamações como uma importante fonte de inteligência para complementar e apoiar outras funções mais importantes. Ao mesmo tempo, deixa claro que as DPAs não devem desviar seu foco para lidar com um serviço de resolução de reclamações de alto volume e demanda.

Uma objeção à abordagem descrita acima pode ser seu impacto potencial no direito do indivíduo a uma solução eficaz. O direito à proteção de dados é um direito que os indivíduos devem poder exercer efetivamente. O CIPL sugere, no entanto, um maior foco na melhoria da conduta organizacional. Isso, de fato, aumentaria a substância deste direito, melhorando a eficácia da lei de proteção de dados em geral (como o CJEU enfatizou em Costeja).[46] É importante lembrar que a lei de proteção de dados é frequentemente vista, como proteção ambiental, como um bem público que beneficia a todos. Em um ambiente mais estratégico, outros métodos de reparação também podem desempenhar um papel importante na obtenção de um remédio efetivo para o indivíduo.

Diligência Devida no contexto da EU

No caso Schrems,[47] o Tribunal de Justiça da UE decidiu que as DPAs devem analisar as alegações de pessoas em relação ao seu direito à proteção de dados "de forma diligente " (*due diligence*). Embora o significado da expressão “de forma

[46] Caso C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*.
[47] Caso C-362/14, Schrems, EU:C:2015:650, at 63.

diligente” não seja totalmente claro, pode-se argumentar que essa expressão “exige que todas as reclamações sejam investigadas por uma DPA, de forma apropriada à reclamação em questão. A exigência “de forma diligente” é essencialmente o meio termo entre a grande margem de discricionariedade que as DPAs têm e a proteção dos reclamantes. As DPAs, com recursos limitados, devem garantir um alto nível de proteção, mas também proporcionar um remédio legal para aqueles que afirmam que, em seus casos individuais, a lei foi violada. A atuação “de forma diligente“ poderia funcionar como um compromisso, desde que não seja interpretado como uma obrigação de dedicar recursos para investigar todas as reclamações. O valor agregado de uma DPA independente não é apenas a sua ampla gama de tarefas, mas também a capacidade de executar essas tarefas da maneira que considere mais eficaz.

f. Autorizador

O papel de Autorizador da DPAs também é amplamente gerado pela demanda e potencialmente intensivo em recursos e não estratégico.

Abrange as situações em que é necessária alguma forma de consulta formal, autorização prévia ou aprovação do DPA. Esta abordagem *ex ante* significa que as atividades afetadas não podem ter lugar sem essa autorização. Exemplos no GDPR incluem aprovações BCR, contratos ad hoc para transferência de dados, consulta prévia em caso de DPIAs onde o risco não pode ser atenuado, códigos de conduta, etc. Os processos reais de autorização podem não contribuir necessariamente para a eficácia em termos de alcançar altos padrões de comportamento. Embora os volumes sejam difíceis de prever, esta poderia ser uma função significativamente intensa em termos de recursos, especialmente se cada pedido de autorização for tratado individualmente e examinado em profundidade.

Tal como acontece com o tratamento de reclamações, a função em si e sua lógica não podem ser ignoradas. No entanto, existe uma margem para que as DPA considerem como simplificar e desempenhar esta função de forma mais eficaz,

especialmente no tocante ao processamento transfronteiriço, enquadrando nos procedimentos de centralização de serviços e consistência. A EDPB poderia desempenhar um papel de liderança aqui, através da promulgação de orientações, recomendações e melhores práticas, tal como previsto no n.º 1 do artigo 70.º do GDPR, com a participação também das DPAs fora da UE.

Mais uma vez, é necessária uma abordagem estratégica e cooperativa. O uso de alguma forma de aprovação "baseada em classe" para certos tipos já estabelecidos de atividade, talvez em conjunto com condições apropriadas, pode ser promissor.[48] Para cada caso em que a autorização é necessária, isso pode ser facilmente dado com base em critérios publicados para a atividade. O cumprimento dos critérios e condições levaria à autorização automática e de rotina a menos que a atividade incluísse características incomuns ou excepcionais. Isso poderia estar relacionado com a abordagem "Cumprir ou Declarar" cada vez mais adotada em outras áreas da regulamentação. À medida que a DPA-como-Líder se torna mais envolvida com regulados responsáveis, cresce de forma considerável a margem de consulta sobre a substância e a enforcement dos critérios e até mesmo para os mecanismos de autocertificação, que podem ser verificados *post facto* pelas DPAs ou terceiros credenciados. Obviamente, isso não substitui a aprovação prévia quando especificamente exigido pela lei, mas alivia significativamente o processo.

TÓPICOS PARA DISCUSSÃO

1.Quando os desafios e expectativas da era digital são tão grandes – e especialmente quando os recursos são limitados – quais parecem ser as melhores maneiras para as DPAs (de forma independente e com outros) garantir que a regulamentação da proteção de dados irá produzir os melhores resultados?

2. A eficácia pode ser elaborada em termos de permitir que as pessoas prosperem com dignidade e autonomia em um mundo digital onde as utilizações de dados inaceitáveis que prejudiquem sua privacidade sejam evitadas?

[48] Isso poderia desenvolver de forma parecida com as “isenções de categoria” previstas na lei de concorrência da EU..

3. Já que as responsabilidades da maioria das DPAs são tão numerosas, quais são as melhores maneiras de alcançar a eficácia em termos globais?

4. A Abordagem Baseada em Resultados oferece maneiras úteis de estabelecer prioridades estratégicas e equilibrar o engajamento, a fiscalização e o tratamento de reclamações?

5. É correto dar prioridade estratégica máxima às funções de liderança com forte ênfase no engajamento construtivo com organizações reguladas?

6. **Engajamento construtivo na prática**

A análise na seção anterior sugere que as funções de Liderança das DPAs devem ser tratadas como principal prioridade estratégica, com o maior envolvimento construtivo possível entre DPAs e aqueles que elas regulam. Na UE, isso está previsto no artigo 57 (1) (d) do GDPR, que reconhece implicitamente que ambas as partes poderiam fazer muito auxiliando a outra a obter resultados regulatórios melhores.

Esta conclusão central foi apoiada durante a oficina organizado em Dublin pelo CIPL em junho de 2017, que também enfatizou o interesse mútuo dos reguladores e entidades reguladas em garantir uma regulamentação real de privacidade de dados, juntamente com a inovação de dados e o crescimento da economia digital. Em outras palavras, reguladores efetivos e baseados em resultados e organizações responsáveis podem trabalhar mais um ao lado do outro como dois pilares essenciais da moderna proteção de dados.

"*Se as empresas nos mostrarem [somos uma DPA] que estão investindo em auto-*

compliance, vamos relaxar - a menos que constatemos alguma ilegalidade ".

"É tudo uma questão de confiança. Reguladores e regulados devem ter os mesmos objetivos ".

"Isso faz uma enorme diferença - e o assunto é levado a sério no topo da hierarquia- quando os reguladores reconhecem abertamente os valiosos esforços e os sucessos da proteção de dados".

"Nós já trabalhamos com empresas para melhorar seus comportamentos. Recebemos 100.000 chamadas de PME no ano passado ".

Participantes da oficina de CIPL em Dublin

Nesse workshop, analisou-se o que envolvimento construtivo seria realmente na prática. Uma tendência bem-vinda e crescente para o engajamento construtivo por parte de muitas DPAs em todo o mundo já começou e isso pode expandir. Muitas atividades e técnicas (tanto atuais quanto potenciais) podem ser identificadas:

• **Transparência máxima** - As DPAs devem ser transparentes ao estabelecer suas prioridades, expectativas e métodos de trabalho, o que ajudará as DPA a serem eficazes e ajudará as organizações a "acertar de primeira". Do mesmo modo, as organizações devem estar prontas para serem transparentes quando lidando com as DPAs, sem medo ou ameaça de auto-incriminação.

• **Orientação prática** - Geralmente feita na web, a orientação é dada sobre a interpretação e aplicação de requisitos da regulamentação, que também está aberta para consulta e resposta por organizações reguladas. A melhor orientação é dada em linguagem simples, com muitos exemplos e segmentada para máxima facilidade de uso por cada público-alvo, por exemplo, pequenas empresas, empresas médias, multinacionais, setores comerciais específicos, órgãos públicos, etc.

• **Participação ativa** - Em reuniões abertas e fechadas, para comunicar preocupações e expectativas, a participação pode ser tão importante quanto para descobrir também incertezas, tendências, desenvolvimentos comerciais e tecnológicos, etc.

• "**Auto-Garantia Regulada"** – deposita total confiança nos DPOs, nos códigos de conduta, nos esquemas de certificação, na capacidade de demonstrar responsabilidade, etc., para promover a auto-*compliance* confiável e reduzir as pressões sobre as DPAs.

• **Consulta Máxima**, com uma abordagem "Sem surpresas", por exemplo, buscando opiniões sobre a minuta de orientação ou recebendo feedback sobre um plano estratégico proposto antes da sua adoção final. Esse diálogo é especialmente benéfico quando há novos requisitos ou não há visões únicas sobre o que é "o certo" para cumprir, ou mesmo o que deve ser evitado.

• **Trocas Francas** – disposição para participar de discussões confidenciais, muitas vezes com um líder de mercado, sobre as implicações e aceitabilidade - ou não - de uma inovação tecnológica.

• **Explorando o Instinto de Manada -** Cada vez mais as DPAs estão reconhecendo que as organizações tendem a seguir um líder da manada. Se uma ou duas empresas receberem uma forma especial de aprovação ou autorização para seguir um curso de ação desejável, os concorrentes, os pares e muitos outros (especialmente as PME) seguirão o *benchmark* e farão o mesmo. Existe um espaço considerável para que as DPAs explorem essa tendência, promovendo os melhores comportamentos da categoria, destacando transparência bem sucedida, DPIA e outros modelos, apresentando melhores práticas de organizações responsáveis (campanhas de treinamento ou conscientização, liderança de DPO, etc.), influenciando deliberadamente os principais consultores legais e outros e destacando on-line exemplos de boas práticas.

• **Incentivos** - Líderes corporativos levarão a proteção e privacidade de dados mais a sério se as DPAs puderem criar e comunicar incentivos para programas de

privacidade de boa fé e *compliance*. Esses incentivos podem incluir a capacidade de compartilhar dados além das fronteiras, engajar de forma mais ampla em *big data* e atividades de aprendizado de máquinas e, fundamentalmente, na mitigação em caso de execução.

• **Criando espaço para inovação responsável -** Existe um espaço considerável para construir soluções de *compliance* cooperativamente. A Caixa de Areia Regulatória (veja abaixo) oferece uma possibilidade. "*Design Thinking*", onde os requisitos de privacidade de dados e os desafios de conformidade podem ser escaláveis e desenvolvidos de baixo para cima por equipes multifuncionais, pode fornecer outras oportunidades para participação e engajamento regulatório com organizações reguladas e especialistas de outras áreas (economistas comportamentais, designers centrados no usuário, engenheiros de tecnologia, especialistas em marketing e relacionamento com clientes).[49]

• **Reiterativa e Conformidade Dinâmica** – Tal qual o desenvolvimento de tecnologia e software, seria útil se as DPAs e as organizações reguladas tratassem *compliance* como uma jornada e um processo reiterativo e dinâmico, em oposição a um evento único e singular. O *compliance* dinâmico é particularmente adequado para a proteção de dados, em vista da velocidade dos desenvolvimentos tecnológicos e a adoção de soluções digitais. Ele permite melhorias, com base nos comentários dos usuários, desenvolvimentos internos e externos e aprendizagens da indústria e dos reguladores. As organizações devem ser encorajadas a adotar o *compliance* dinâmico e as DPAs não devem punir aqueles que ficam buscando acertar com o tempo.

• Os **indicadores de desempenho** são essenciais para medir e mostrar o sucesso da DPA em influenciar diretamente a disseminação das boas práticas, de preferência com métricas comuns e / ou comparáveis.

A Caixa de Areia Regulatória - Espaço para Inovação Responsável

[49] Um exemplo atual de iniciativa de inovação responsável é a iniciativa " design jam" do Facebook, que busca novas abordagens e soluções para transparência e controle individual.

O engajamento construtivo inclui a criação de espaço para inovação responsável por organizações responsáveis. Como isso pode ser alcançado?

O modelo Caixa de Areia Regulatória (*"Regulatory Sandbox"*) que está sendo desenvolvido pela Autoridade de Conduta Financeira do Reino Unido[50] pode ser uma maneira interessante de permitir que as empresas regulamentadas experimentem e inovem em um "abrigo seguro" supervisionado pelo órgão regulador.

A caixa de areia regulatória permite às empresas testar produtos inovadores, serviços, modelos de negócios e mecanismos de entrega no mercado real, com consumidores reais.

A caixa de areia é um "espaço supervisionado" que dizem é capaz de oferecer às organizações:

• tempo-a-mercado reduzido a um custo potencialmente menor; e
• Proteções adequadas de proteção ao consumidor incorporadas a novos produtos e serviços.

A caixa de areia oferece ferramentas como autorização restrita, orientação individual, isenções e cartas de ação de execução. A FCA supervisiona de perto os ensaios utilizando um ambiente regulatório personalizado para cada piloto.

Espera-se que os testes de caixa de areia tenham um objetivo claro (por exemplo, reduzir custos para os consumidores) e sejam realizados em pequena escala, de modo que as empresas testarão sua inovação por um período limitado com um número limitado de clientes. Poderia se dizer que inovação técnica afeta a proteção de dados em uma extensão ainda maior do que os serviços financeiros.

Este modelo pode ser particularmente bem adaptado e bem recebido na comunidade de proteção de dados, onde é crescente o reconhecimento de que

[50] https://www.fca.org.uk/firms/regulatory-sandbox.

compliance deve ser tratado como um processo iterativo.

O possível uso do modelo caixa de areia neste contexto foi levantado pelo ex-secretário geral da CNIL em um artigo em Les Echos no início de 2017.[51]

Mais recentemente, em julho de 2017, foi anunciado que o PDPC de Singapura está preparado para trabalhar com empresas responsáveis para criar bancos de dados regulatórios para testar mudanças legislativas propostas e permitir que as empresas continuem sendo inovadoras e competitivas.[52]

O diálogo construtivo deve ser um processo bidirecional, com grande confiança, compromisso e respeito mútuo entre as DPAs e organizações responsáveis. A menos que as organizações estejam dispostas a ajudar as DPAs a desenvolver uma melhor compreensão da paisagem que eles regulam, elas não podem esperar que as DPAs sejam abertas e compreendidas. As empresas reguladas e os órgãos públicos devem estar prontos e dispostos a se engajar de forma construtiva com as DPAs. Isso significa avançar - de forma proativa e reativa - com uma abordagem que é tão aberta e franca quanto possível. As organizações empresariais e governamentais precisam ser capazes de explicar e demonstrar da forma mais transparente possível seus processos e soluções tecnológicas e estarem prontas para explicar e demonstrar modelos de negócios. Esta é também uma questão de Interesse Próprio Esclarecido e é especialmente promissor em um ambiente em que mais e mais entidades responsáveis se orgulham de sua responsabilidade. Quando uma proposta obviamente inovadora ou controversa está sendo desenvolvida, o diálogo é particularmente valioso para identificar com antecedência quaisquer modificações que garantam a aceitabilidade - muito melhor do que o desafio após o lançamento. Na UE, os mecanismos inovadores no GDPR na centralização (*one-*

[51] https://urldefense.proofpoint.com/v2/url?u=https-3A__www.lesechos.fr_idees-2Ddebats_cercle_cercle-2D165613-2Dlinnovation-2Dlautre-2Darme-2Ddu-2Dbrexit-2D2061519.php&d=DwIFAw&c=jxhwBfk-KSV6FFIot0PGng&r=Fk3CDN4QpXmXZZ7F2MuwcJTW5M0wnTw0gqFJV2no8r8&m=Yd8qNquweowj_8BlDbM5Ljgl43DBuw5ZitB6SZdhk7E&s=UHTdvy5zVo0ee3dA1N5JRiq8X9UDsOY4hU1BgUuAcUc&e

[52] https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2017/7/personal-data-protection-seminar-2017.

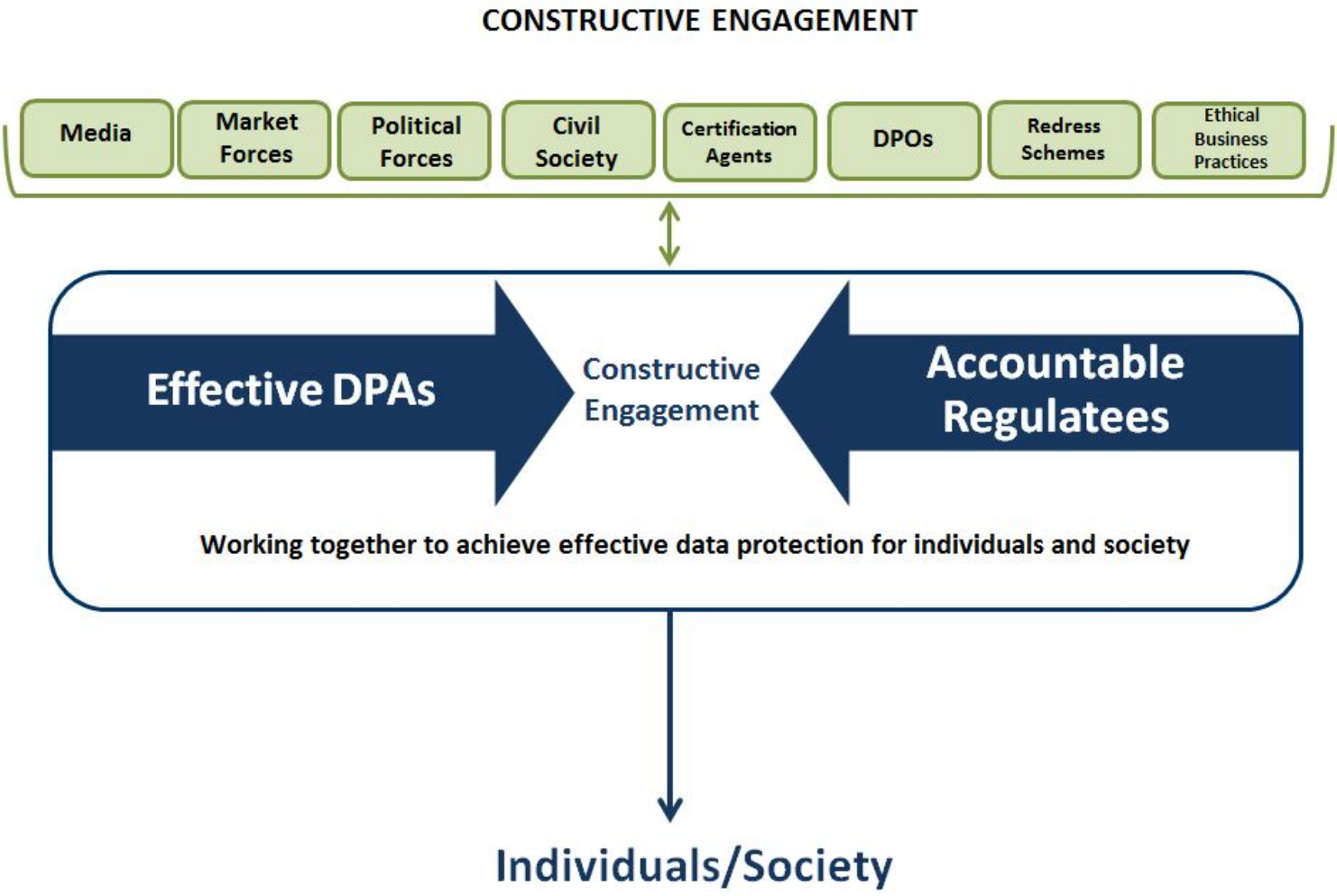
stop-shop), lideram as DPAS, bem como os procedimentos de cooperação e consistência, devem encorajar esse diálogo bidirecional, que é mais transparente e baseado em confiança mútua e respeito.

"Precisamos que os reguladores sejam independentes, assim como precisamos que juízes e árbitros sejam independentes. No entanto, a independência não pode vir ao preço da responsabilização ou do envolvimento e os reguladores precisam manter seus dedos no pulso do mercado através da interação com a indústria e os consumidores. Em poucas palavras, os reguladores devem estar comprometidos, mas não enredados, isolados, mas não insulares".[53]

A oficina que o CIPL realizou em Dublin também enfatizou que o engajamento construtivo deve se estender para além do relacionamento direto de regulador / regulado. Além da óbvia importância de interagir com os indivíduos que são beneficiários da proteção de dados, existem muitos outros jogadores e forças que podem ser aproveitados na busca dos resultados regulamentares desejados. Como já mencionado, DPOs, órgãos de certificação terceirizados e mecanismos de reparação podem ser usados para reforçar o papel de Liderança das DPAs. Aproveitar a mídia e as forças políticas é vital para transmitir mensagens. As pressões de um mercado competitivo, onde as organizações colocam um enorme valor na reputação, também precisam ser totalmente compreendidas e aproveitadas.

O engajamento construtivo pode ser caracterizado como operando dentro de um "Quadro" que captura as contribuições desta rica rede de partes interessadas. O diagrama na próxima página ilustra o escopo para que as DPAs se envolvam diretamente com esses regulados, mas também trabalhem com uma ampla gama de outras organizações e forças.

[53] '*Are regulators the new Men in Black*?' Cavassini, Naru & Below, in *Risk & Regulation* (LSE, 2016) citando o OCDE, Tornando um Regulador Independnete.



[Mídia, Forças do Mercado, Forças Políticas, Sociedade Divil, Agentes Certificadoras, DPOs, Mecanismos de Reparação, Práticas Éticas de Negócios] DPAs Eficazes » Engajamento Construtivo « Regulados Responsáveis Trabalhando juntos para alcançar uma proteção de dados eficaz para indivíduos e sociedade] » Indivíduos/Sociedade

TÓPICO PARA DISCUSSÃO

1. Quais atividades e técnicas promovem melhor o engajamento construtivo na prática?

7. Princípios para uma Abordagem Baseada em Resultados

Uma abordagem estratégica para estabelecer prioridades e fazer escolhas difíceis é essencial para a eficácia das DPAs. Isso se aplica a cada DPA individual, mas - à medida que a necessidade de coordenação e consistência globais aumenta inexoravelmente - também é necessário ter a maior discussão e consenso possível sobre a melhor maneira de maximizar a eficácia.

A partir da evidência geral sobre a regulamentação eficaz resumida na seção 4 e a análise mais específica das prioridades para a proteção de dados na seção 5, é possível consolidar os tópicos e sugerir uma primeira minuta para discussão de Princípios de alto nível para fornecer a base para uma Abordagem Baseada em Resultados. Os Princípios sugeridos apresentados abaixo estão em conformidade com abordagens já adotadas por algumas DPAs. Os Princípios, sugeridos para discussão nesta fase, visam auxiliar na definição de prioridades - tanto em termos de funções de classificação umas contra as outras quanto para a segmentação de setores, atividades ou organizações específicas.

Além de fornecer uma estrutura para uma Abordagem Baseada em Resultados, o projeto de Princípios tem como objetivo promover a consistência máxima da estratégia entre as DPAs. Os Princípios foram, portanto, elaborados para ter ampla aplicação para proteção de dados e reguladores de privacidade a nível mundial e regional. A importância de trabalhar em conjunto para assegurar *compliance* para além das fronteiras já foi mencionada. Mas deve haver consistência de estratégia, bem como compartilhamento de informações e comunhão de recursos.

Se o conteúdo dos mesmos for amplamente aceito, prevê-se que uma versão revisada dos Princípios possa ser adotada e promulgada em quatro níveis:

adotada, promulgada e implementada em quatro níveis:

- Globalmente, pela Conferência Internacional de Comissários para a Proteção de Dados e Privacidade (*International Conference of Data Protection and Privacy Commissioners (ICDPPC*). Uma data possível seria a Conferência Internacional marcada para o outono de 2018.
- a nível da UE, pela WP29 e, oportunamente, pelo Conselho Europeu de Proteção de Dados (*European Data Protection Board*). O melhor seria antes da data início de GDPR, marcado para maio de 2018.
- a nível da Ásia-Pacífico, pelo fórum das Autoridades de Proteção de Dados da Ásia-Pacífico (*Ásia-Pacific Privacy Authorities -APPA)*.
- a nível operacional, pela Rede Global de Fiscalização da Proteção de Dados (*Global Privacy Enforcement Network -GPEN)* e o Acordo Transfronteiriço para a Garantia da Privacidade da APEC (*APEC Cross-border Privacy Enforcement Arrangement -CPEA*)

Princípios para uma Abordagem Baseada em Resultados

- Regulamentar para Gerar Resultados no Mundo Digital exige que as Autoridades de Proteção de Dados (DPAs) sejam estratégicas, eficazes, coordenadas e transparentes.

- A meta de uma DPA deveria ser produzir resultados eficazes em termos de custo que, na prática, protejam os indivíduos, promovam o uso responsável de dados e facilitem a prosperidade e inovação.

- A primeira prioridade das DPAs deveria ser assegurar a proteção dos indivíduos.

- Cada DPA independente deveria ser responsável por definir, de maneira transparente, os resultados específicos que pretende, e as prioridades e abordagens que irá adotar para conseguir tais resultados através do seu trabalho regulatório.

- As estratégias de todas as DPAs deveriam ser coordenadas, consistentes e complementárias o quanto possível.

- As DPAs deveriam tratar as organizações reguladas de maneira consistente – adotando abordagens similares entre e dentro de setores, independentemente do tipo ou do alcance geográfico da organização.

- Cada DPA deveria adotar uma abordagem baseada em riscos em todas as suas atividades, dando prioridade para lidar com os comportamentos que mais prejudicam as pessoas ou os valores democráticos e sociais.

- Uma abordagem de engajamento construtivo, com ênfase na liderança, informações, recomendações, diálogos e apoio será mais eficaz do que dependência única e exclusiva em intimidação e punição.

- A ênfase em informações e recomendações tem importância especial na área de proteção de dados, devido a seu impacto abrangente em inúmeras organizações e a natureza das exigências que são imprecisas ou descontextualizadas, necessitando avaliação e decisão em casos individuais.

- Relacionamentos abertos e construtivos com as organizações que tratam das informações pessoais, com base em um diálogo honesto e cooperação mútua, com responsabilidades definidas, incrementarão os resultados de *compliance* como um todo.

- As organizações reguladas deveriam ser avaliadas, sobretudo, pela

referência de boa-fé comprovável e diligência nos seus esforços voltados *o compliance*.

- As organizações que buscam atuação responsável e que tentam “agir certo”, deveriam ser encorajadas a se identificarem, por exemplo, demonstrando de maneira transparente sua responsabilidade, seus programas de proteção de dados e gerenciamento de riscos, a influência de seus Encarregados de Proteção de Dados (os “DPOs) e seu uso de programas de selo/certificação, BCRs, CBPR e outros quadros de responsabilidade.

- Sanções punitivas deveriam ser direcionadas principalmente às atividades desconformes que sejam dolosas, deliberadas, seriamente negligentes, reincidentes ou particularmente graves.

- Embora atender reclamações individuais possa ser um componente importante na proteção dos indivíduos, lidar com alto volume dessas reclamações requer recursos substanciais que podem acabar impedindo objetivos estratégicos mais amplos. As reclamações são uma ferramenta valiosa de inteligência mas deveriam ser bem geridas com critérios claros para determinar a extensão da investigação.

.

<u>Um protocolo?</u>

Qualquer conjunto de princípios deve ser de alto nível e de aspiração. Pode até ser prematuro considerar em dar mais substancia efetiva a esses princípios e trazer a Abordagem Baseada em Resultados para a vida como a norma regulatória moderna para as DPAs. Além disso, o risco é real de que qualquer tentativa de articular padrões específicos venha a ser vista como algum tipo de imposição externa.

Não é absolutamente a visão deste documento de trabalho propor qualquer tipo de requisito obrigatório. O CIPL é bastante claro em dizer que os movimentos em direção a uma Abordagem Baseada em Resultados para proteção de dados devem vir das próprias DPAs. Isso não é apenas uma questão de independência. Essa abordagem só terá êxito se sua fundamentação central for abarcada pela comunidade DPA. Ela jamais poderá ser imposta.

Para ajudar neste processo e reunir as principais ideias apresentadas neste documento e estimular a discussão, o CIPL produziu uma primeira minuta de um Protocolo para uma Abordagem Baseada em Resultados para a Regulamentação da Proteção de Dados. Essa minuta do Protocolo está apensa como Anexo D a este documento.

Tal qual os Princípios, qualquer Protocolo para as DPAs só pode ser acordado e adotado de forma coletiva e voluntária com consenso sobre a estrutura básica e a redação. Um possível caminho a seguir – e importante no contexto do desenvolvimento do Mecanismo de Consistência - seria o EDPB desenvolver seu próprio Protocolo para tornar os Princípios algo concreto e, em seguida, incentivar a sua adoção por todas as DPAs da UE.

Em todo o mundo (particularmente através da rede APPA e / ou operacionalmente através do GPEN e do CPEA), o mesmo Protocolo poderá ser adotado por DPAs ou a minuta do Anexo D pode ser tomada como ponto de partida para o desenvolvimento de algo mais customizado.

TÓPICOS PARA DISCUSSÃO

1. Será que as entidades que reunem globalmente, regionalmente e operacionalmente as DPAS irão considerar a adoção sugerida dos Princípios para Abordagem baseada em Resultados?

2. Como esses Princípios podem ser aperfeiçoados?

8. Possíveis Problemas

Todas as estratégias envolvem escolhas difíceis. É necessário reconhecer abertamente que uma Abordagem Baseada em Resultados pode trazer alguns desafios e riscos. Qualquer ranking de prioridades deve ter seus "perdedores", bem como "vencedores". O envolvimento com organizações reguladas pode ser contra-intuitivo e suscitar preocupações genuínas - tanto as DPAs podem ser "capturadas" como alguns regulados não verão com bons olhos o envolvimento excessivo de DPA em suas atividades passadas, presentes e futuras.

a. Relutância em Relegar Funções

As próprias DPAs ficarão nervosas com a diminuição de qualquer função que seja lançada em termos de um dever estatutário. Conforme mencionado acima, na UE, muitas das funções GDPR são escritas como "tarefas" que a DPA "deve" executar.
Como o GDPR não fornece metas estratégicas abrangentes para as DPAs ou qualquer autoridade explícita para classificar algumas funções acima de outras, as DPAs podem relutar em fazê-lo por conta própria.

No entanto, existem várias respostas a essas preocupações. Apesar da falta de autoridade explícita, algumas DPAs já adotam seus próprios valores ou objetivos de alto nível. Uma abordagem transparente e estratégica é preferível a mudanças ad hoc e imprevisíveis, impulsionadas por eventos, de uma atividade para outra. O ranking baixo, ou o gerenciamento apertado da demanda, não significa abandonar qualquer função na sua totalidade - e isso não é sugerido aqui.
Mesmo quando não há discricionariedade explícita, ainda há espaço para julgamento e proporcionalidade. Esta sendo cada vez mais a regra, por exemplo, que outros órgãos reguladores deem prioridade às funções de liderança como sendo mais eficazes na mudança de comportamentos do que o papel de Polícia. Na verdade, pode ser impróprio que qualquer regulador tome medidas de execução,

buscando impor sanções severas, por comportamentos que anteriormente não identificavam como inaceitáveis.

Do mesmo modo, ter uma política geral de gestão rigorosa das reclamações em geral, mas dando atenção especial a determinados casos, é inteiramente possível. Por exemplo, as reclamações são comumente recebidas e registradas como prova *prima facie* de um problema e, no entanto, a grande maioria não pode ser submetida a uma investigação ou resolução detalhada. A profundidade da investigação em cada denúncia é, portanto, proporcional à gravidade potencial dos assuntos envolvidos. Isso requer arranjos de triagem robustos para que as principais características de cada reclamação possam ser rapidamente avaliadas e (na maioria dos casos) os reclamantes podem ser informados por que recursos escassos e esforços desproporcionais não podem ser especificamente dedicados para seus casos.

b. **Captura Regulatória**

Pode haver preocupações quanto a atribuir maior prioridade ao engajamento com os regulados. Pode haver apreensão com relação a uma "Captura Regulatória" se as DPA se aproximarem muito das organizações que elas regulam. A Captura Regulatória é descrita como o processo pelo qual o setor regulado pode influenciar e manipular as agências que deveriam controlá-las. Isso pode ser visto como uma ameaça tanto para a independência quanto para a integridade dos reguladores.

Sem dúvida, os reguladores devem sempre gerenciar adequadamente seus relacionamentos com aqueles que eles regulam, e limitar o risco de "Captura Regulatória". Eles devem estar prontos para lidar com as pressões que poderiam resultar, por exemplo, em influência imprópria na seleção de "alvos" para regulamentação, simpatia excessiva com as necessidades dos regulados ou penas mais indulgentes.

Com a máxima transparência e outras salvaguardas, os temores da Captura Regulatória devem permanecer em grande parte na teoria. Como acontece em todos os campos, os reguladores independentes devem ter um relacionamento

"adulto" com aqueles que regulam. Isso requer contato com o setor regulado. Uma "cultura de integridade" consciente e aberta ajudará as DPAs a resistir a quaisquer pressões do setor regulado. As DPAs têm orgulho de sua independência e são maduras o suficiente para saber que a independência também significa imparcialidade - olhando cuidadosamente os dois lados de cada questão e ponderando todos os fatos. Uma cultura corporativa que promova a integridade e altos níveis de probidade, talvez com alguma separação interna de funções, permitirá que as DPAs tomem as decisões corretas sobre os níveis adequados de engajamento com o setor regulado, tanto formal como informal.

c. **Resistência do Regulado**

Pode haver preocupações correspondentes da comunidade regulada de que o envolvimento excessivo com os reguladores pode ser problemático. Algumas organizações reguladas podem preferir manter distância de uma DPA, talvez por medo de uma penalidade por má conduta passada, tendo documentos ou práticas suas divulgadas para a DPA durante as consultas e depois utilizados contra elas em uma ação por descumprimento ou medo de vetarem uma inovação planejada. Isso, no entanto, seria um erro. As organizações mais reservadas podem ironicamente chamar mais atenção para si mesmas e é melhor ser avisado sobre a não conformidade de antemão, em vez de descobri-la, a um custo pesado, em momento posterior. Além disso, seria prejudicial para a própria reputação e estratégia de uma DPA, se insistisse de forma dura em fazer valer o cumprimento em resposta à informação divulgada no decurso de um relacionamento supostamente construtivo.

Em termos gerais, como já dito, o envolvimento está intimamente relacionado com a responsabilidade organizacional e deve ser um processo bidirecional baseado na confiança mútua. Os regulados não podem esperar que as DPA se envolvam em uma Abordagem Baseada em Resultados, a menos que eles também desempenham sua parte.

Anexo A - Funções DPA sob GDPR

Na tabela a seguir, as principais tarefas e poderes atribuídos às DPAs foram agrupados em uma dessas quatro categorias. A seção 5 deste documento de trabalho usa essa divisão no contexto da definição de prioridades.

TAREFA / PODER	**ARTIGO**
LÍDER	
Promover a conscientização pública dos riscos, regras, salvaguardas e direitos	57(1)(b)
Promover a conscientização das obrigações dos controladores / processadores	57(1)(d)
Aconselhar o parlamento ou governo nacional, etc.	57(1)(c)
Fornecer informações aos sujeitos dos dados quando solicitadas	57(1)(e)
Monitorar a aplicação dos Regulamentos	57(1)(a)
Monitorar tecnologias e práticas comerciais pertinentes etc.	57(1)(i)
Aconselhar sobre operações de processamento que necessitam de DPIA	57(1)(l)
Encorajar e facilitar os códigos de prática, mecanismos de certificação e selos e marcas	57(1)(m)-(q)
AUTORIZADOR	
Autorizar processamento de alto risco com base no interesse público	58(3)(c)
Autorizar cláusulas contratuais para transferências internacionais	58(3)(h)
Autorizar medidas administrativas para transferências internacionais	58(3)(i)
Autorizar Regras Corporativas Vinculativas	58(3)(j)
Aprovando / reconhecendo códigos, mecanismos de certificação e selos e marcas	42, 43, 57, 58 & 64 *passim*
POLICIAL	
Aplicar o Regulamento	57(1)(a)
Realizar investigações da aplicação do Regulamento	57(1)(h)

Determinar que o controlador / processador forneça informações	58(1)(a) & (e)
Obter acesso às instalações, equipamentos e meios do controlador / processador	58(1)(f)
Emitir avisos e reprimendas	58(2)(a)-(b)
Determine conformidade	58(2)(c)-(e)
Impor limitações e proibições ao processamento	58(2)(f)
Determinar retificação, apagamento etc.	58(2)(g)
Impor multas administrativas	58(2)(i)
Suspender fluxos internacionais de dados	58(2)(j)
PROCESSADOR DE RECLAMAÇÕES	
Lidar com e investigar as reclamações	57(1)(f)

Anexo B - Recursos das DPAs

A pesquisa comparativa mais recente dos orçamentos das DPAs foi realizada pela Conferência Internacional de Comissários para a Proteção de Dados e Privacidade (*International Conference of Data Protection and Privacy Commissioners (ICDPPC*) em 2017.[54] As respostas da pesquisa incluem dados de recursos para 87 autoridades de proteção de dados de 58 países. Dos países que forneceram informações sobre recursos financeiros, o orçamento total global das DPAs para 2016 foi de € 887.320.351.[55]

A informação relativa aos recursos financeiros está disponível para todos os Estados-Membros europeus, com exceção da Áustria, Croácia e de alguns dos estados germânicos. O CIPL tomou os dados financeiros dessa pesquisa para os 26 países da UE[56] que estão incluídos e definiu os números em relação aos números de população relevantes. Estes números mostram um orçamento total em 2016 de € 205,703,574 para uma população total para aquele ano de 507,471,970.[57] Isto indicaria, em todos estes 26 países como um todo, que o orçamento por cidadão foi inferior a € 0,41. O valor real provavelmente teria sido um pouco maior se os orçamentos para a Áustria, a Croácia e todos os estados germânicos estivessem disponíveis. Os números para 2017 serão, sem dúvida, mais elevados: o orçamento das DPAs de 2016 dos Estados-Membros aumentou em relação ao seu número de 2015, com exceção de Portugal, Chipre, Letônia e um estado alemão, mas é duvidoso que o orçamento por cidadão seja significativamente maior.

É ainda mais indicativo das demandas de cada DPA para estabelecer o número de organizações reguladas. Ao contrário da maioria dos órgãos reguladores, as responsabilidades das DPAs não são setoriais e abrangem todos os setores da

[54]Os dados do censo são disponibilizados mediante solicitação à Secretaria da Conferência Internacional de Comissários para a Proteção de Dados e Privacidade, https://icdppc.org/the-conference-and-executive-committee/icdppc- census/.
[55] Vários países reportaram suas dotações em moeda local. A conversão foi feita para euros usando a taxa de cambio de 27 de julho de 2017.
[56]os números para a Alemanha estão abaixo do valor efetivo já que somente 7 dos 16 estados germânicos forneceram dados.
[57] Números da população para os respectivos 26 paiíses da UE foram pesquisados junto ao Banco Mundial em 27 de julho de 2017 http://data.worldbank.org/indicator/SP.POP.TOTL.

economia. Além disso, a maioria dos organismos públicos pertence à jurisdição das DPAs e, de fato, o GDPR impõe requisitos mais rigorosos com as responsabilidades correspondentes da DPA.

O Eurostat estima que "em 2014, a economia empresarial da UE28 foi de cerca de 26 milhões de empresas ativas".[58] Isso presumivelmente exclui a maioria dos órgãos públicos. Poucas empresas agora estão fora do escopo dos requisitos de proteção de dados. Mesmo a PME (Pequena e Média Empresa) menor que seja provavelmente estará processando os dados pessoais dos clientes e outros contatos em um telefone celular ou laptop. Isto sugere que, em toda a UE, as DPAs têm um orçamento médio de cerca de € 8 por negócio empresarial.

[58] http://ec.europa.eu/eurostat/statistics-explained/index.php/Business_demography_statistics.

Anexo C - Conclusões Básicas de "Direito e Comportamento Empresarial"

1) Um sistema regulatório é mais eficaz quando é consistente e apoia comportamentos que são amplamente vistos como justos, proporcionais e éticos.

Os reguladores devem adotar os incentivos e ações corretas que apoiem e não prejudiquem os esforços dos indivíduos e das empresas para se comportarem corretamente. Por exemplo, os reguladores devem adotar estratégias de *enforcement* publicadas que reconheçam tentativas comerciais para fazer o que é certo.

Os reguladores devem ser cautelosos em se concentrar demais em regras detalhadas ou prescritivas ("abordagem de caixa de seleção") que reduzem a capacidade daqueles na linha de frente de pensar por si mesmos e diminuem tanto o poder quanto o alcance para agir de maneira responsável. Os reguladores devem influenciar a propensão de empresas bem-sucedidas de adotar culturas com base em valores em que todos estão alinhados para se concentrar na obtenção dos resultados desejados. Essa cultura, por exemplo, aprenderá com os erros, evitará atribuir culpa, corrigirá as coisas quando estiverem dando errado, receberá reclamações e gerará ideias de melhoria e inovação.

2) As organizações devem ser responsáveis por comprovar seu compromisso com comportamentos que atrairão a confiança dos reguladores, bem como sua própria administração e equipe, clientes, fornecedores, investidores e outras partes interessadas.

Um negócio deve ser encorajado - e às vezes exigido - a adotar práticas empresariais responsáveis e se responsabilizar por tudo o que é feito em toda a organização. Os códigos sobre aspectos individuais não são suficientes - a abordagem deve ser holística. Deve ser conduzido desde o topo, mas existir em todos os níveis dos grupos sociais dentro de uma organização.

Os reguladores devem procurar evidências de que uma organização opera com integridade e possui uma abordagem positiva para o *compliance*. A mera afirmativa de uma empresa que pode ser confiável claramente não será suficiente. A evidência pode assumir formas como estruturas de governança que colocam ênfase n*o compliance*, adesão consistente aos padrões comportamentais, uma alta proporção de clientes satisfeitos, *enforcement* consistente de sistemas de auditoria e auditoria e uma abordagem transparente ao escrutínio externo.

3) O aprendizado é fundamental e é encorajado pelo engajamento aberto e construtivo entre reguladores e organizações reguladas, mas fica prejudicado quando houver ênfase na "culpa" e / ou punição.

Os sistemas de regulamentação em que o aprendizado e a manutenção do desempenho são criticamente importantes - como a aviação civil, a farmacovigilância e a saúde e segurança no local de trabalho - tratam a "regulamentação" como um quadro comportamental que atua para apoiar as pessoas a tomar as decisões certas através da aprendizagem constante.

Um problema crítico é identificar por que um risco ou problema ocorreu, quais fatores foram fatores causais reais ou potenciais e como o risco de um evento similar pode ser reduzido. O foco é o monitoramento constante e a aprendizagem de eventos, para melhorar o desempenho e reduzir o risco.

No entanto, as pessoas não oferecerão informações voluntárias se temerem atrair críticas ou culpas. Assim, com salvaguardas adequadas, é essencial incentivar uma "cultura aberta" de compartilhamento e questionamento, em vez de uma "cultura de culpa" ou uma relação adversa com os reguladores. Essa deveria ser a regra, exceto nos casos de irregularidades óbvias ou graves.

4) Os sistemas reguladores devem basear-se no diálogo e na cooperação mútua, que são explicitamente orientados para maximizar o *compliance*, a prosperidade e a inovação.

O diálogo contínuo e a cooperação mútua que sejam transparentes para as pessoas de fora, em vez de uma relação contraditória e distante, são consistentes com os

sistemas de gerenciamento, *compliance* e de risco. Todos envolvem mecanismos baseados na circulação de informações que monitora o desempenho, identifica riscos e implementa melhorias.

Se o objetivo principal é acionar os comportamentos certos através de *compliance* máxim*o*, isso é melhor feito combinando sistemas regulatórios com arranjos de co-regulamentação estruturados e supervisionados. Essas estruturas de co-regulamentação podem ser desenvolvidas para incluir compromissos em relação a comportamentos e mecanismos éticos e conformes, que geram a evidência para apoiar uma relação de confiança.

5) Quando as organizações quebram as regras, é necessária uma resposta proporcional, com as penas mais duras reservadas para delitos deliberados, repetidos ou intencionais.

Embora existam, obviamente, muitos "tons de cinza", um regime regulatório moderno distingue entre pessoas que basicamente tentam fazer o que é certo e aqueles que não estão - em grande parte por uma questão de motivação. É importante ter respostas justas e proporcionais à execução.[59] Se as pessoas praticarem atividades desconformes que sejam deliberadas, intencionais ou gravemente negligentes, a lei deve ser mantida com uma resposta proporcional. Mas onde as pessoas estão tentando agir certo ou foram geralmente, mas não intencionalmente, desconhecedoras de suas responsabilidades, a adoção de uma resposta punitiva seria considerada injusta e não ajudaria na promoção da vontade de cumprir.

A abordagem moderna da execução baseia-se na proposição de que "a maioria das organizações está tentando fazer o que é certo na maioria das vezes". Essa abordagem é oposta a uma abordagem dominante que é repressiva, dissuasiva ou pesada. A psicologia comportamental, especialmente no contexto empresarial, não apoia a ideia de que o cumprimento futuro ou a dissuasão do descumprimento são aumentados pela ameaça ou imposição de fortes penalidades. A ideia de que as

[59] Vide GDPR, Artigo 83(2).

pessoas no mundo empresarial obedecerão à lei devido ao medo de que uma violação seja punida - por isso, é melhor se conformar do que sofrer - mostrou-se eficaz somente quando se percebeu que era um alto risco de identificação seguido por perda de reputação corporativa ou pessoal. A perspectiva de uma penalidade financeira no negócio não é um forte motor de *compliance*. Governar pelo medo em uma democracia moderna é, em qualquer caso, uma política pouco atrativa.

Anexo D - Primeira Minuta de um Possível Protocolo

Minuta de Protocolo para uma Abordagem Baseada em Resultados para Regulamentar a Proteção de Dados

1. **A eficácia das Autoridades de Proteção de Dados é avaliada principalmente na medida que os indivíduos são protegidos na prática.**

2. **As Autoridades de Proteção de Dados devem assegurar-se que informações claras, orientações e recomendações estão disponíveis para auxiliar aqueles que elas regulam a satisfazer suas obrigações de cumprimento.**

• As DPAs devem fornecer aconselhamento e orientação concentrados basicamente em auxiliar aqueles que elas regulam para entender e cumprir suas obrigações. Ao dar recomendações e orientações, o impacto da recomendação ou orientação deve ser considerado para que não imponha encargos desnecessários a si mesmo.

• As DPAs devem escrever informações, orientações e recomendações em linguagem simples e usar formatos e mídias claras, acessíveis e concisas, apropriadas para cada público-alvo. Elas devem consultar (o mais cedo possível) sobre as orientações que planejam produzir.

• As DPAs devem procurar criar um ambiente no qual aqueles que elas regulam confiem nas suas recomendações e possam procurar recomendações sem medo de desencadear ações de execução.

3. **As Autoridades de Proteção de Dados devem fornecer maneiras simples e diretas de se envolver com aqueles que elas regulam e ouvirem suas opiniões.**

• As DPAs devem ter mecanismos para se envolver com aqueles que elas regulam, permitindo que cidadãos e outros possam oferecer opiniões e contribuir para o desenvolvimento de suas políticas e padrões de serviço.

• Ao reagir a um descumprimento, as DPAs devem explicar claramente qual o item ou atividade não conforme, a recomendação dada, as ações necessárias ou as decisões tomadas e os motivos para isso. As DPAs devem proporcionar uma oportunidade de diálogo em relação às recomendações, requisitos ou decisões, com o objetivo de garantir que eles atuem de forma proporcional e consistente.

• Este parágrafo não se aplica quando a DPA puder demonstrar que é necessária uma ação de execução imediata para prevenir ou responder a uma violação grave ou, quando proporcionando essa oportunidade, provavelmente o objetivo da ação de execução proposta ficaria prejudicado.

• As DPAs devem garantir que exista um procedimento imparcial e claramente explicado para recorrer de suas decisões regulatórias.

• As DPAs devem regularmente convidar e receber *feedback*, incluindo, por exemplo, através de pesquisas de satisfação sobre aqueles que elas regulam.

4. **As Autoridades de Proteção de Dados devem realizar suas atividades de forma a apoiar aqueles que procuram cumprir.**

• As DPAs devem escolher abordagens proporcionais para seus regulados, com base em fatores relevantes, incluindo, por exemplo, porte e capacidade da atividade, os volumes e a natureza dos dados pessoais processados.

• Ao conceber e rever políticas, procedimentos e práticas operacionais, as DPAs devem considerar como eles podem apoiar ou permitir a inovação e o crescimento econômico para empresas compatíveis, por exemplo, considerando como melhor possível:

☐ incentivar e promover o *compliance*;

☐ melhorar a confiança no *compliance* para os regulados, fornecendo a máxima

certeza;

☐ entender e minimizar impactos econômicos negativos de suas atividades reguladoras; e

☐ minimizar os custos de *compliance* para os regulados.

5. **As Autoridades de Proteção de Dados devem basear suas atividades no risco.**

• As DPAs devem praticar uma abordagem baseada em evidências para determinar os riscos prioritários em sua área de responsabilidade e alocar recursos onde eles seriam mais eficazes para enfrentar esses riscos prioritários.

• As DPAs devem considerar o risco em todas as etapas dos seus processos de tomada de decisão, incluindo a escolha do tipo de intervenção mais apropriado ou o modo de trabalhar com os regulados. A avaliação dos riscos também deve visar o controle do *compliance* e a escolha das ações de execução.

• As DPAs, ao fazerem sua avaliação de risco, devem reconhecer a responsabilidade e o registro de conformidade dos regulados (por exemplo, através do uso de mecanismos de reconhecimento por merecimento) e devem considerar todos os dados disponíveis e relevantes sobre *compliance*, incluindo evidências de verificação externa relevante.

• As DPAs devem rever a eficácia das suas atividades reguladoras escolhidas ao entregar os resultados desejados e fazer os ajustes que se fizerem necessários.

6. **As Autoridades de Proteção de Dados devem assegurar que suas atividades regulatórias são transparente e consistentes e estejam bem coordenadas com as abordagens de outras autoridades.**

• As DPAs devem publicar suas estratégias, planos de trabalho anuais, padrões e

metas, etc., para que os regulados saibam o que podem esperar delas. Isso deve incluir, por exemplo, informações claras sobre:

☐como elas se comunicam com os regulados e como podem ser contatadas;

☐ seu sistema para fornecimento de informações, orientações e recomendações;

☐ os mecanismos de controles de *compliance*, incluindo os detalhes da estrutura de avaliação de risco utilizada para atingir esses controles; e

☐ sua política de execução, explicando como elas reagem ao descumprimento.

• Em uma sociedade digital em que os dados não reconhecem as fronteiras nacionais, as DPAs devem maximizar a eficácia, a consistência e a eficiência em estreita coordenação e cooperação com as DPAs de outras jurisdições.

BIBLIOGRAFIA

Este documento de trabalho se baseou em várias fontes, mas destacamos especialmente as publicações abaixo.

Responsive Regulation – Ian Ayres and John Braithwaite, OUP, 1995.

A Reader on Regulation – Baldwin, Scott & Hood, OUP, 1998.

The Regulatory Craft – Malcolm K. Sparrow, The Brookings Institution, 2000.

The Governance of Privacy – Colin Bennett and Charles Raab, MIT Press, 2006.

Implementing Hampton: From Enforcement to Compliance – UK Better Regulation Executive, 2006.

Really Responsive Regulation – Baldwin & Black – LSE Working Paper, 2007.

Risk and Regulatory Policy - Improving the Governance of Risk – OECD, 2010.

The Governance of Regulators - Best Practice Principles for Regulatory Policy – OECD, 2014.

Law and Corporate Behaviour - Integrating theories of regulation, enforcement, compliance and ethics – Christopher Hodges, Hart Publishing, 2015.

The European Union as Guardian of Internet Privacy – Hielke Hijmans, Springer, 2016.

Regulatory Theory - Foundations and Applications – Peter Drahos, Australian National University, 2017.