APDSI

ASSOCIAÇÃO
PARA A PROMOÇÃO E DESENVOLVIMENTO
DA SOCIEDADE DA INFORMAÇÃO

Ciclo Regulação Digital – Webinar 5: "Transatlantic Data Privacy Framework – Solução ou Problema Adiado?

CONCLUSÕES

30 de junho de 2022

No âmbito do seu Grupo de Missão ''DSA, DMA, e-Privacy'', a APDSI realizou o quinto webinar do Ciclo #RegulaçãoDigital discutindo sobre o ***"Transatlantic Data Privacy Framework (TADPF) – Solução ou Problema adiado?".***

A 30 de junho, Graça Canto Moniz, Sebastião Barros Vale, Shane Murphy e Sofia Riço Calado debruçaram-se sobre o anúncio da Comissão Europeia e da Administração Americana de ***um novo acordo relativamente às transferências de dados pessoais para os Estados Unidos da América****, o Transatlantic Data Privacy Framework.*

As opiniões dos líderes são diversas e entre os oradores também ficaram patentes os diversos pontos de vista e perspetivas futuras sobre esta questão.

Luís Neto Galvão, coordenador do Grupo de Missão ‘’DSA, DMA, e-Privacy’’ da APDSI, foi o moderador deste webinar. Nesta sessão, debateu-se a troca de dados pelo mundo e, em particular, da União Europeia para os Estados Unidos. Foram também mencionados os **desafios que essa “viagem” coloca sempre que não estejam reunidas as condições de segurança para o fazer.**

O webinar teve como ponto de partida o acórdão do Tribunal de Justiça da União Europeia de 2020 que invalidou o anterior mecanismo - o Privacy Shield - que legitimava a transferência de dados pessoais para os Estados Unidos. Anteriormente, o mesmo organismo já tinha invalidado o Safe Harbour. **Esta é já a terceira tentativa de regular dados e a sua transferência para os Estados Unidos.**

Shane Murphy, Privacy Policy Manager EMEA da Meta, lançou a questão: porque são tão importantes para a nossa sociedade as transferências de dados? Shane Murphy responde fazendo uma descrição dos dados como a infraestrutura invisível que “segura” a Internet enquanto a rede que permite o florescer de novos negócios, mas também manter vivas as relações com clientes, amigos e familiares no mundo inteiro.

Quando pensamos em dados, pensamos em tecnologia, mas quando esses dados deixam de ser acessíveis têm um impacto que vai mundo além desta área e que pode afetar todas as nossas relações - até as amorosas. **Os negócios, todavia, têm de começar a preparar-se para eventuais falhas na transmissão de dados para os Estados Unidos se operarem na União Europeia.**

Ainda assim, Shane Murphy prefere olhar para este quadro como uma oportunidade porque nem todos estes fluxos de transmissão de dados envolvem dinheiro. A investigação na área da saúde também está a antecipar o impacto que as restrições na transmissão de dados poderão vir a ter e que já estão a sentir-se, sobretudo nos Estados Unidos. A oportunidade poderá estar para os europeus que pretendem ter acesso a produtos e serviços de dimensão global.

Quem trabalha e estuda o RGPD já definiu esta TADPF como um dos assuntos mais complexos de sempre, o que nos dá uma noção bem clara dos desafios que estão a caminho.

Em que ponto estamos em matéria de transferência de dados entre a União Europeia e os Estados Unidos?

Na verdade, os europeus não estão tão focados na transmissão de dados no contexto das transações comerciais, mas sim na possibilidade de o Governo americano vir a ter acesso aos seus dados pessoais. **"Para muitos milhares de pessoas e empresas este Transatlantic Data Privacy Framework está no bom caminho"**, afirmou o Privacy Policy Manager EMEA, da Meta, que considera que os cidadãos são quem mais vai beneficiar deste mecanismo de proteção quer no reforço das suas relações sociais online, quer em questões humanitárias. Esta reforma tem uma abrangência bastante alargada e profunda e resulta de longas conversações.

A União Europeia e os Estados Unidos encontram-se, neste momento, a finalizar os acertos em pormenor sobre algumas questões para permitir a publicação oficial da totalidade das reformas que se vão aplicar a esta transmissão de dados. Portugal vai ter um papel fulcral na publicação do acordo porque **"um assunto tão delicado como este não pode ficar exclusivamente nas mãos da Comissão Europeia que vai reunir em breve com o Governo português"**, nota Shane Murphy. A discussão deve começar "o quanto antes" e tem de assentar em factos reais e dados concretos, em detrimento de conceitos pré-concebidos.

O futuro desta relação e uma perspetiva global

O fluxo de transmissão de dados precisa, realmente, de um controlo mais sério por parte dos Governos por forma a criar jurisdições mais justas e adequadas aos tempos modernos. À medida que mais e mais países adotam legislação sobre privacidade, surge o risco de que o UE/EUA seja um acordo unilateral, sem consistência internacional. Há várias iniciativas que procuram contornar esse risco: o processo da OCDE que está a "trazer para a mesa" novos princípios sobre o acesso dos Governos a dados pessoais e o Japão que também os está a discutir.

Na UE procura-se uma solução multilateral, até porque já há nalguns países legislação neste contexto com grande respeito pelo cumprimento da lei e dos direitos humanos em normas que têm de ser reforçadas. **"Juntos vamos começar a ter um novo debate**

sobre os fluxos de dados. É uma questão social e política onde se pretende que cidadãos e empresas se sintam bem e confiantes acompanhados por uma filosofia mais global e menos individual ainda que não haja uma solução rápida e totalmente isenta", acrescenta.

A Meta já lançou uma lista de aspetos técnicos com os quais os países têm de estar em conformidade para uma segura transferência de dados além-fronteiras. Será, ainda, necessário haver um acordo do ponto de vista político que reforce o recurso a meios seguros de transferência de dados (os Network Codes on Cybersecurity) que garantam segurança e tranquilidade a todos os intervenientes nestes tempos incertos que atravessamos.

Graça Canto Moniz, Professora de Direito, Universidade Lusófona e Nova School of Law, lembra que toda esta discussão começou em 2000, quando a realidade da Internet só chegava a 7% da população mundial, e não havia nenhuma empresa tecnológica entre as mais bem-sucedidas no mundo. Nos últimos 22 anos, os fluxos de dados entre os Estados Unidos e a União Europeia, têm sido alvo de várias tentativas de regulação, desde quando a Comissão Europeia adotou a ***Decisão Porto Seguro***; em 2013/2014 surgiu ***Edward Snowden*** com a sua revelação de uma série de programas de vigilância dos Estados Unidos que implicavam a vigilância massiva e indiscriminada de cidadãos não americanos; em 2015/2016 o Tribunal de Justiça invalidou a decisão de 2000 e a Comissão Europeia adotou a ***Decisão Escudo de Proteção*** em 2020/2021. A publicação das ***Garantias Essenciais Europeias*** foi feita também nesse ano.

Há 22 anos, a Comissão Europeia considerou que os Estados Unidos eram um país adequado para receber dados da União. Isto foi necessário porque a proteção de dados da UE tem regras para o tratamento de dados pessoais, mas prevê também um regime específico para transferências que tem por objetivo garantir que à medida que os dados pessoais "viajam", a proteção que a União Europeia lhes dá "viaja" com eles.

Este modelo de adequação, que não existe apenas no âmbito da proteção de dados pessoais, é algo **"ambicioso porque a informação é ubíqua e há milhares de milhões de dados a circularem diariamente. Há muitos autores que dizem que reflete um estado**

tecnológico de início de século", afirma Graça Canto Moniz. O regime de transferência de dados pessoais assenta num modelo de avaliação da adequação do direito de um país terceiro, o que implica um exigente exercício de análise do Direito vigente nos Estados Unidos e a conclusão de que dá garantias semelhantes às da União Europeia.

No limite, tudo o que está em discussão neste momento poderá ser uma consequência da importação de soluções normativas – como este modelo de avaliação da adequação – de outras áreas do Direito, nomeadamente do Direito Financeiro. Por outro lado, este modelo de adequação tem um efeito estratégico para UE, que é o facto de influenciar o Direito de outros países de uma forma direta: um país só vai ser considerado adequado se o Direito desse país for equivalente ao padrão de proteção que a União Europeia tem.

Depois de 2013, quando Snowden revelou ao mundo os programas dos Estados Unidos de vigilância em larga escala, a Comissão Europeia tomou algumas precauções e foi constituído um grupo de trabalho que estudou qual a legislação americana que suportava aqueles programas de vigilância. O grupo em questão chegou a várias conclusões, nomeadamente a existência de legislação que suportava aquelas práticas, a ausência de fiscalização (por exemplo por um tribunal) e o facto de os cidadãos estrangeiros não terem mecanismos para se defender de eventuais abusos.

O jovem austríaco Max Schrems também veio a público apontar abusos e falhas nas políticas de privacidade da rede social Facebook com base na legislação europeia, e procurou apresentar alternativas legais que respeitassem os direitos fundamentais dos utilizadores. O seu ativismo está na origem de duas decisões judiciais, os casos Schrems I e II, que colocam em evidência a questão de fundo que se mantém: o "conflito" entre a legislação americana, que suporta os programas de vigilância dos Estados Unidos, e a Carta dos Direitos Fundamentais da União Europeia que já deixou claro aquilo que o Direito Americano deve respeitar se quer, efetivamente, ser considerado adequado: tem de ser claro em relação ao tratamento dos dados, ter respeito pelo princípio da proporcionalidade, fazer supervisão independente e ter vias de recurso eficazes. São estas as quatro garantias essenciais europeias que estão publicadas num documento do Comité Europeu de Proteção de Dados.

Sebastião Barros Vale, EU Policy Counsel no Future of Privacy Forum, mostrou a sua preocupação com o facto de uma eventual nova decisão vir a ser anulada pelo Tribunal de Justiça da União Europeia, tal como aconteceu com as duas anteriores. A 25 de março deste ano as administrações americana e europeia anunciaram um acordo político para um mecanismo que substituirá o *Privacy Shield*. **O objetivo é que se garanta proteção equivalente à europeia do outro lado do Atlântico.**

No comunicado que a Casa Branca publicou na sequência desse anúncio, surge a intenção reforçar as liberdades e garantias individuais no contexto das atividades de vigilância americanas, incluindo um melhoramento das atividades de supervisão das agências americanas. Fica a dúvida se essas revisões serão apenas textuais ou terão reflexo na prática - será que programas autorizados pela lei americana vão ser alterados por forma a cumprirem os requisitos da Carta dos Direitos Fundamentais da União Europeia?

O comunicado da Casa Branca refere que os titulares dos dados europeus terão acesso a recurso efetivo contra atividades de vigilância nos Estados Unidos. Esse mecanismo (o chamado "*Data Protection Review Court*") incluirá membros que não fazem parte do Governo americano e terão autoridade para endereçar as queixas dos cidadãos europeus e impor medidas corretivas. **O Tribunal de Justiça apontou a falta de mecanismos coercivos das medidas impostas pelo anterior Ombudsperson no passado**, pelo que este passo pode representar uma melhoria.

Sobre as obrigações para as organizações americanas que subscrevam os princípios comerciais do novo acordo, tudo indica que as mesmas serão mantidas face às que existiam ao abrigo do *Privacy Shield*. Resta apurar se estes princípios estarão alinhados com o RGPD e a Carta, nomeadamente no que toca aos requisitos de licitude para o tratamento de dados pessoais, direito de acesso dos titulares dos dados e supervisão com uma autoridade independente.

Até à aprovação final da decisão de adequação da Comissão Europeia que substituirá o *Privacy Shield* ainda há algum tempo, porque os Estados Unidos têm de aprovar uma Ordem Executiva para implementar estas reformas na lei americana, que será complementada por um regulamento de implementação do Departamento de Justiça

americano. Só depois dessas leis serem aprovadas nos Estados Unidos, é que a Comissão Europeia publicará uma versão preliminar que está sujeita ao parecer do Comité Europeu de Proteção de Dados (EDPB) e de um voto positivo do Conselho da União Europeia – para além do escrutínio do Parlamento Europeu – , o que se pode traduzir num período que se prolongará até ao primeiro trimestre de 2023.

O Governo americano está, neste momento, a preparar uma ordem executiva presidencial que ainda não foi publicada, aparentemente baseada nas sugestões apresentadas por um grupo de influentes **académicos do Direito da União Europeia e dos Estados Unidos** (ver aqui e aqui).

Terá o já referido Data Protection Review Court independência e poderes suficientes para ser validado pelo Tribunal de Justiça num eventual Acórdão? Pelo menos de acordo com a jurisprudência do Supremo Tribunal dos Estados Unidos refere que tribunais criados através de ordem executiva podem, nalguns casos, agir independentemente do poder Executivo. Adicionalmente, nas recomendações do EDPB sobre Garantias Essenciais Europeias arguiu-se que os titulares dos dados europeus têm, ao abrigo da Carta, direito a recorrer a uma autoridade nacional que não tem, necessariamente, natureza judicial, podendo mesmo ser administrativa.

As empresas devem continuar a usar mecanismos alternativos de transferência de dados (como Cláusulas Contratuais-Tipo) sempre que não exista uma decisão de adequação relativa ao país onde o importador de dados se encontra, identificando potenciais requisitos jurídicos "problemáticos" nos Estados terceiros e medidas mitigadoras (caso existam) no contexto de Análises de Impacto de Transferências, em cumprimento das Recomendações do EDPB. Quanto aos mecanismos de certificação de importadores em países terceiros, as orientações do Comité vão no sentido de que **"para uma entidade num país terceiro (na jurisdição que vai receber dados) estar apta a receber dados da União Europeia, o importador de dados tem de demonstrar que não há legislação problemática na jurisdição onde está estabelecido ou que, existindo, ofereça garantias suplementares de proteção que permitiram receber esses dados"**, explicou **Sebastião Barros Vale**.

A última oradora da sessão foi Sofia Riço Calado, Senior Privacy Counsel da Clouflare, uma empresa de gestão de tráfego de Internet e de soluções de cibersegurança, que deu apoio à Ucrânia na gestão de ataques cibernéticos, com presença no mundo inteiro (em Portugal desde 2019).

Vivemos uma realidade em mutação, de uma fase de conectividade, para aquela que é uma visão mais fragmentada da Internet. O quadro atual obriga a que as empresas digitais tenham uma estratégia internacional de gestão de dados, incorporem diferentes padrões de proteção, antecipem mudanças e percebam que vão aumentar os custos de entrada e permanência em mercados terceiros – até porque as estratégias que incorporam novos padrões também vão mudando ao longo do tempo.

A China e a Rússia são exemplos de países com limitações tecnológicas e com conteúdos de Internet a que os cidadãos têm acesso tão limitados que são muito diferentes daqueles a que nós temos acesso. Na Austrália, por exemplo, os dados de saúde dos cidadãos têm sempre uma cópia alojada em bases de dados locais e na Índia a localização dos dados em território nacional ainda é apenas uma proposta legislativa. Ou seja, neste momento a restrição ainda não existe, mas pode vir a existir.

Quando pensamos em conceitos como *splinternet*, soberania digital e localização de dados, confrontamo-nos com os dados que nos indicam que até 2021 mais do que duplicaram os países que têm legislação que restringe e que localiza os dados – atualmente são 144. “Estamos a passar de uma fase de livre circulação para uma fase com fronteiras, sabemos que as empresas têm que ter uma estratégia internacional de gestão de dados que incorpore as alterações em curso e antecipe mudanças”, afirma **Sofia Riço Calado.**

Ao mesmo tempo que há um movimento para garantir ao nível mundial a livre circulação de dados, temos, também, que lidar com questões como a soberania desses mesmos dados que existe em múltiplos países e que obriga à sua localização na origem.

A Cloudfare tem soluções específicas de localização de dados na Europa, nos Estados Unidos, na Austrália e no Japão (que também tem seguido muito a tendência da União Europeia).

PERGUNTAS E RESPOSTAS

- **Será que a União Europeia foi muito ambiciosa quanto ao regime de transferência de dados perante os Estados Unidos? Continuamos num impasse?**

Sebastião Barros Vale acredita que o standard de proteção não deve mudar na União Europeia.

Graça Canto Moniz admite que a União Europeia possa estar a ser exigente, mas o regime das transferências não foi longe demais: se calhar na solução de adequação a componente aspiracional, como tantas outras no RGPD (como, por exemplo, a proteção das crianças) está representada. Por outro lado, a saga Schrems está a pôr em evidência o problema da vigilância massiva e indiscriminada, nos EUA e noutros países da Europa.

De salientar que empresas maiores, como a Microsoft, por vezes conseguem jogar contra as tendências normativas americanas como exemplificou uma decisão do *S*upreme Court que está na origem do Cloud Act.

- **Tendo o RGPD feito uma abordagem baseada no risco como se encaixa nas empresas que exportam dados para fora da União Europeia?**

Sebastião Barros Vale optou por esclarecer o que quer dizer uma "abordagem baseada no risco" que não significa o risco de sermos apanhados ou termos coimas; significa, isso sim, **que vamos priorizar o cumprimento da lei naquilo que são as atividades de tratamento de dados que representam mais risco para os direitos e liberdades dos titulares dos dados.**

"Estamos um bocado perdidos em relação à abordagem baseada no risco para as transferências de dados, ou seja, ela é possível, mas é muito cara e difícil de implementar". Nesse sentido, a opção mais segura será utilizar soluções com base na Europa e que não transferem dados para fora do Continente quando exista legislação problemática na jurisdição do importador.

Sofia Riço Calado fechou falando sobre a nova abordagem a esta matéria, mais *business friendly*, que vai surgir do Reino Unido que manifestou a intenção de tornar a transferência de dados mais flexível, não colocando tantas restrições à circulação.

SOBRE A APDSI

Criada em 2001, a Associação para a Promoção e Desenvolvimento da Sociedade da Informação (APDSI) tem por objetivo a promoção e desenvolvimento da transformação e inclusão digital em Portugal, reunindo com este interesse comum profissionais, académicos, empresas, organismos públicos e cidadãos em geral.

Na linha destes propósitos a APDSI tem vindo a desenvolver diversas atividades em torno de causas tecnológicas e societais, que se traduzem num conjunto de eventos, recomendações e estudos realizados por grupos de trabalho multidisciplinares em diversas áreas de intervenção, como a Segurança e Privacidade, a Ética no Digital, os Serviços Públicos Digitais, a Saúde, a Cidadania e Inovação Social, o Território Inteligente, as Tecnologias de Inteligência Digital, a Política Digital e Governança, os Futuros da Sociedade da Informação, as Competências digitais e o Ambiente e Energia.

Em todos estes trabalhos a APDSI procura identificar as tendências de evolução e também as interações entre as tecnologias e outras dimensões sociais e económicas, contribuindo com uma visão mais aberta para a discussão e tendo como meta a eficaz perceção e implementação destes conceitos na Sociedade Portuguesa. A APDSI tem o Estatuto de Utilidade Pública e foi em 2008 reconhecida como ONGD.

ASSOCIE-SE

URL | www.apdsi.pt

email | secretariado@apdsi.pt

APDSI

ASSOCIAÇÃO
PARA A PROMOÇÃO E DESENVOLVIMENTO
DA SOCIEDADE DA INFORMAÇÃO

Associação de Utilidade Pública

ONG – Organização Não Governamental

Rua Alexandre Cabral, 2C – Loja A
1600-803 Lisboa – Portugal
URL: www.apdsi.pt

Tel.: (+351) 217 510 762
Fax: (+351) 217 570 516
E-mail: secretariado@apdsi.pt

Patrocinadores Globais da APDSI

Platina

accenture aws Google

Ouro

devoteam Meta