EUROPEAN DATA PROTECTION SUPERVISOR

Parecer 4/2015

Rumo a uma nova ética digital:

dados, dignidade e tecnologia

11 de setembro de 2015

A Autoridade Europeia para a Proteção de Dados (AEPD) é uma instituição independente da UE que, nos termos do artigo 41.º, n.º 2, do Regulamento n.º 45/2001 «No que se refere ao tratamento de dados pessoais [...] está encarregada de assegurar que os direitos e liberdades fundamentais das pessoas singulares, especialmente o direito à privacidade, sejam respeitados pelas instituições e órgãos comunitários.», e é responsável «[...] por aconselhar as instituições e órgãos comunitários e as pessoas em causa sobre todas as questões relativas ao tratamento de dados pessoais.». A Autoridade foi nomeada em dezembro de 2014, juntamente com a Autoridade Adjunta, com a missão específica de serem mais construtivas e proativas. Em março de 2015, a AEPD publicou uma estratégia quinquenal em que estabelecia como tencionava executar essa missão e prestar contas pela mesma.

O presente Parecer vem no seguimento do Parecer anterior da AEPD sobre o Regulamento geral sobre a proteção de dados que teve como objetivo ajudar as principais instituições da UE a reunir o consenso adequado acerca de um conjunto de regras viáveis e orientadas para o futuro que reforcem os direitos e liberdades das pessoas. Tal como no Parecer sobre a saúde móvel de inícios de 2015, o presente Parecer aborda o desafio da proteção de dados «entrar na era digital» - o terceiro objetivo da estratégia da AEPD - e «adaptar os princípios da proteção de dados existentes à arena digital global», tendo também em conta os planos da UE para o Mercado Único Digital. É consistente com a abordagem do Grupo de Trabalho do artigo 29.º relativa aos aspetos relacionados com a proteção de dados decorrentes do uso de novas tecnologias, tal como a «Internet das Coisas», para a qual a AEPD contribuiu enquanto membro do grupo.

Dignity	Dignidade
Future-oriented rules and enforcement	Regras orientadas para o futuro e aplicação
Accountable controllers	Responsáveis pelo tratamento suscetíveis de sujeição a escrutínio público
Empowered individuals	Pessoas capacitadas
Innovative privacy engineering	Engenharia de privacidade inovadora
Ethics	Ética

«A dignidade do ser humano é inviolável. Deve ser respeitada e protegida.»

Artigo 1.º, Carta dos Direitos Fundamentais da UE

Os direitos fundamentais à privacidade e à proteção de dados pessoais tornaram-se mais importantes do que nunca para a proteção da dignidade do ser humano. Estes direitos estão consagrados nos Tratados da UE e na Carta dos Direitos Fundamentais da UE. Permitem às pessoas desenvolver as suas próprias personalidades, viver vidas independentes, inovar e exercer outros direitos e liberdades. Os princípios da proteção de dados definidos na Carta da UE (necessidade, proporcionalidade, justiça, minimização dos dados, limitação da finalidade, consentimento e transparência) aplicam-se integralmente ao tratamento de dados, à recolha, bem como à utilização.

A tecnologia não deve ditar valores nem direitos, nem tão-pouco deve a relação entre ambos ser reduzida a uma falsa dicotomia. A revolução digital promete benefícios para a saúde, o ambiente, o desenvolvimento internacional e a eficiência económica. De acordo com os planos da UE para um mercado único digital, a computação em nuvem, a «Internet das Coisas», os megadados e outras tecnologias são consideradas essenciais para a competitividade e o crescimento. Os modelos de negócio estão a explorar novas capacidades para a recolha massiva, transmissão instantânea, combinação e reutilização de informação pessoal para fins não previstos e justificados por políticas de privacidade longas e impenetráveis. Tal colocou os princípios da proteção de dados sob novas tensões, o que exige pensar em termos inovadores acerca do modo como os mesmos são aplicados.

No ambiente digital atual, o respeito pela lei não é suficiente; há que considerar a dimensão ética do tratamento de dados. A moldura regulamentar da UE já concede margem para decisões e salvaguardas flexíveis e casuísticas sempre que se lide com informação pessoal. A reforma da moldura regulamentar será um bom passo em frente. Mas existem questões mais profundas quanto ao impacto das tendências sobre a dignidade, a liberdade individual e o funcionamento da democracia numa sociedade que assenta no acesso a dados.

Estas questões têm implicações filosóficas, jurídicas, morais e de engenharia. O presente Parecer destaca algumas das principais tendências tecnológicas que poderão implicar um tratamento de informação pessoal inaceitável ou que poderão interferir com o direito à privacidade. Delineia um «ecossistema de proteção de megadados» em quatro níveis para responder ao desafio digital: um esforço coletivo, sustentado por considerações de ordem ética.

(1) Regulamentação do tratamento de dados orientada para o futuro e respeito pelos direitos à privacidade e à proteção de dados.

(2) Responsáveis pelo tratamento suscetíveis de sujeição a escrutínio público que decidem acerca do tratamento de informação pessoal.

(3) Engenharia e desenho de produtos e serviços de tratamento de dados respeitadores da privacidade.

(4) Pessoas capacitadas.

A Autoridade Europeia para a Proteção de Dados pretende estimular um debate aberto e informado dentro e fora da UE, envolvendo a sociedade civil, *designers*, empresas,

académicos, autoridades públicas e autoridades reguladoras. O novo comité de ética da proteção de dados da UE que será criado na AEPD contribuirá para a definição de uma nova ética digital, permitindo otimizar os benefícios da tecnologia para a sociedade e a economia de molde a reforçar os direitos e liberdades das pessoas.

ÍNDICE

1. Ubiquidade dos dados: tendências, oportunidades e desafios

Verifica-se um número crescente de informações que estão a ser recolhidas e tratadas de formas cada vez mais opacas e complexas. Com a utilização progressiva de computadores nas empresas e administrações públicas na década de 1980, existia uma perceção generalizada de que as práticas de governos e empresas poderosos no tratamento de dados pessoais estavam a reduzir as pessoas ao estatuto de meros titulares de dados, ameaçando os direitos fundamentais e as liberdades. O que distingue a atual vaga de tecnologias da informação e da comunicação integradas são a sua ubiquidade e poder.

No ano passado constatou-se existirem no planeta mais dispositivos conectados do que pessoas[1]. As melhorias na capacidade dos processadores[2], no armazenamento e na largura de banda de transmissão significa que existem progressivamente menos condicionantes técnicas no tratamento de informações pessoais. Prevê-se que a «Internet das Coisas» e a analítica dos megadados convirjam com a inteligência artificial, o processamento da língua natural e os sistemas biométricos, a fim de reforçar as aplicações com a capacidade de aprendizagem-máquina para inteligência avançada. Os governos e as empresas estão em condições de ultrapassar a «prospeção de dados» e passar para a «prospeção da realidade», a qual penetra na experiência, na comunicação e até mesmo no pensamento do dia-a-dia[3]. À medida que a sociedade se adapta às exigências do mercado digital, estão agora a ser feitos esforços renovados para ensinar programação às crianças pequenas[4]. Aproveitar estas tendências num setor no qual a UE é um consumidor líder, mas que tem ficado para trás no tocante à prestação de serviços, é um tema recorrente na Estratégia para o Mercado Único Digital da Comissão[5].

Estas tendências e muitos dos conceitos utilizados atualmente, apesar da sua adesão, são vagos e sobrepõem-se. Com o propósito de incentivar um debate, pretendemos salientar tendências específicas que, embora não sejam evidentemente exaustivas, no nosso entender suscitam as questões éticas e práticas mais importantes para a aplicação dos princípios em matéria de proteção de dados.

1.1 Megadados

O termo «Megadados» («*Big data*»)[6] refere-se à prática de combinar volumes colossais de informações provenientes de várias fontes e analisá-los, utilizando amiúde algoritmos inteligentes para esclarecer as decisões. Estas informações nem sempre são pessoais: os dados gerados por sensores destinados à monitorização de fenómenos naturais ou atmosféricos como as condições meteorológicas ou a poluição, ou à monitorização de aspetos técnicos de processos de produção, não estão relacionados com uma «pessoa singular identificada ou identificável»[7]. Mas um dos principais valores dos megadados para empresas e governos provém da monitorização do comportamento *humano*, a nível coletivo e individual, e reside no seu potencial preditivo[8].

Um dos resultados é o surgimento de um modelo de rendimento para empresas da Internet que contam com o seguimento da atividade em linha para otimizarem o valor económico das transações para os prestadores de serviços, não apenas em publicidade direcionada como também nas condições e taxas de apólices de seguro, empréstimos e outras relações contratuais. No mercado competitivo destinado à atenção dos utilizadores, a maior parte das pessoas não está consciente da grande dimensão deste seguimento[9]. Esses «megadados» deveriam ser considerados pessoais mesmo nos casos em que tenham sido aplicadas técnicas de anonimização: está a tornar-se cada vez mais fácil inferir a identidade de uma pessoa

mediante a combinação de dados alegadamente «anónimos» com outros conjuntos de dados que incluem informações disponíveis ao público, por exemplo, nas redes sociais[10]. Nos casos em que os dados sejam, em particular, comercializados entre fronteiras e jurisdições, a responsabilização pelo tratamento das informações torna-se opaca e difícil de determinar ou aplicar nos termos da legislação em matéria de proteção de dados, sobretudo na ausência de quaisquer normas internacionais.

1.2 «Internet das Coisas»

Muitos dispositivos ligados à Internet já são já moeda corrente, tais como os telemóveis inteligentes (*smartphones*), os *tablets* e os distribuidores automáticos de numerário e as máquinas para fazer os registos de embarque. Prevê-se que até 2020 a conectividade se torne num elemento normal, com 25 mil milhões de objetos conectados (comparativamente aos 4,8 mil milhões em 2015) que vão desde a telemedicina aos veículos, dos contadores inteligentes a uma vasta gama de novos dispositivos fixos e móveis para viabilizar as cidades inteligentes[11].

Estes sensores vão fornecer informações imediatas e pormenorizadas que atualmente os institutos de estatística e inquéritos não conseguem obter, mas que não são necessariamente mais exatas, existindo mesmo a possibilidade de serem enganosas[12]. Os 1,8 mil milhões de ligações máquina-máquina automotivas estimadas até 2022 poderão reduzir os acidentes e a poluição, aumentar a produtividade e a autonomia dos idosos e portadores de deficiência[13]. As denominadas «tecnologias usáveis» («*wearables*»), tais como vestuário e relógios vão processar informações pessoais similarmente a outros dispositivos conectados. Serão capazes de detetar coágulos de sangue e monitorizar a condição física e a cicatrização de feridas; os tecidos conectados poderão proteger contra ambientes extremos, no combate a incêndios, por exemplo. Estes dispositivos irão carregar dados pessoais diretamente para o armazenamento em nuvem, associado às redes sociais e eventualmente transmitir publicamente, permitindo a identificação de utilizadores e o seguimento do comportamento e movimentos de pessoas e multidões[14].

A forma como estas informações são tratadas poderá afetar a privacidade não apenas dos utilizadores dos dispositivos, incluindo quando utilizados no local de trabalho, mas também os direitos de terceiros que são observados e gravados pelo dispositivo. Apesar de existirem poucas provas de discriminação efetiva, não há dúvidas de que o volume colossal de informações recolhidas pela «Internet das Coisas» tem suscitado uma grande atenção enquanto meio para maximizar os lucros através de uma fixação de preços mais personalizada de acordo com o comportamento que foi objeto de seguimento, designadamente no setor dos seguros de saúde.[15]. Também serão desafiadas outras regras específicas do domínio, por exemplo, nos casos em que os dispositivos que envolvam o tratamento de dados de saúde não se encontrem tecnicamente categorizados como dispositivos médicos, não ficando abrangidos pelo âmbito de aplicação da regulamentação[16].

1.3 Computação ambiente

A **computação ambiente ou invisível** refere-se a uma tecnologia-chave subjacente à «Internet das Coisas». Uma das suas aplicações mais óbvias são as «casas inteligentes» e os «escritórios inteligentes» compostos por dispositivos com capacidade integrada sofisticada de tratamento de informações, que prometem maior eficiência energética e pessoas mais informadas capazes de influenciar o seu consumo remotamente (embora vá depender da

independência do residente relativamente ao senhorio ou administrador do edifício). É necessário ficar claro quem é responsável pela finalidade e pelos meios de tratamento dos dados pessoais envolvidos nas aplicações de computação ambiente, não apenas para proteger os direitos fundamentais das pessoas, como também para uma repartição adequada das responsabilidades de molde a assegurar o cumprimento dos requisitos de segurança do sistema geral.

1.4 Computação em nuvem

A computação em nuvem é conhecida como uma tecnologia facilitadora central tanto para analítica avançada e as capacidades de extração, a recolha e a analítica de megadados e o caudal de dados provenientes da «Internet das Coisas», atualmente utilizada por cerca de um quinto das pessoas e empresas na UE[17]. Permite a concentração de dados a partir da miríade de dispositivos da «Internet das Coisas» e depende da disponibilidade e conectividade de volumes colossais de dados em instalações de armazenamento e tratamento de grande escala espalhadas pelo mundo[18]. A adoção mais generalizada da computação em nuvem[19] por parte dos setores público e privado estima-se que vá acrescentar potencialmente um total de 449 mil milhões de euros ao PIB da UE28 (0,71% do PIB total da UE).

O controlo das informações pessoais é amiúde partilhado entre o cliente e o prestador do serviço em nuvem, sendo que a responsabilidade pelas obrigações de proteção de dados nem sempre é clara. Na prática, tal poderá significar que é prestada proteção insuficiente. Estas obrigações existem independentemente da **localização física do armazenamento de dados**. **Além disso,** embora seja apenas uma tecnologia de base que apoia as aplicações comerciais, a própria infraestrutura de computação em nuvem poderá tornar-se uma infraestrutura crítica e aumentar os desequilíbrios no poder do mercado, com 30% das empresas a afirmarem recentemente ser difícil cancelar a subscrição ou mudar de prestadores[20].

1.5 Modelos de negócio dependentes de dados pessoais

Estas tecnologias permitiram novos modelos de negócio que dependem de informações não apenas geradas pela prestação do serviço, mas também provenientes de outras fontes como a presença nas redes sociais para avaliar o risco e solvabilidade e maximizar os lucros. Hoje em dia, um modelo de negócio proeminente é representado por plataformas que fazem a ponte entre vendedores e compradores, permitindo a partilha e redistribuição de produtos, serviços, competências e ativos. Muitas vezes referidas como plataformas de «economia de partilha», «consumo colaborativo» ou comerciais entre pares em linha e móveis,[21] estas plataformas podem oferecer eficiências económicas clássicas, injetar competitividade nos mercados e diminuir os resíduos. Estima-se que o seu valor global vá quadruplicar de 26 para 110 mil milhões de dólares nos próximos anos[22]. Esses modelos de negócio impulsionados pelos dados estão já a gerar receitas consideráveis na partilha de veículos e no arrendamento para habitação, bem como na tecnologia financeira e nos empréstimos sociais. Os estudos indicam que os consumidores apreciam a sua aparente maior acessibilidade e conveniência[23].

A aceitação geral de tais plataformas prende-se normalmente com a reputação do utilizador, as avaliações pelos pares e a verificação da identidade. Tal pode ser potencialmente encarado como algo que reforça a transparência e a responsabilização, mas não necessariamente em relação ao próprio prestador da plataforma. Os grandes intervenientes destes mercados têm sido criticados por, alegadamente, reterem dados relacionados com a reputação dos utilizadores individuais a quem as informações dizem respeito. Existe um risco enorme de que as pessoas possam ser excluídas dos serviços com base em reputações radicadas em

dados incorretos que não podem contestar ou pedir para apagar. A dependência de dados provenientes de várias fontes também coloca em causa o princípio da minimização dos dados previsto na legislação da UE. O alcance do futuro impacto nas pessoas e na sociedade dos modelos de negócio facilitados pela tecnologia existentes e futuros exige uma reflexão cuidadosa[24].

1.6 Aeronaves não tripuladas e veículos autónomos

Atualmente, as aeronaves não tripuladas, ou aeronaves semiautónomonas, são sobretudo utilizadas para finalidades militares, mas são cada vez mais utilizadas para fins de vigilância, cartografia, transporte, logística e segurança pública, tal como para o combate a incêndios florestais[25]. As fotografias, vídeos e outros dados pessoais recolhidos por aeronaves não tripuladas podem ser trocados em redes de telecomunicações. A sua utilização encerra o risco de uma interferência grave na privacidade e de um efeito dissuasor na liberdade de expressão. Surge a questão sobre de que modo a sua conceção e utilização pode ser eficazmente regulada, para que as pessoas em causa possam exercer os seus direitos de acesso aos dados capturados por estas máquinas.

No solo, os veículos autónomos ou os carros de condução automática vão mudar a forma como a deslocação individual é utilizada e está organizada e poderão esbater a diferença entre os transportes privados e públicos. Estima-se que até 2035 existirão 12 milhões de veículos totalmente autónomos e 18 milhões parcialmente autónomos, com a Europa a figurar entre os primeiros aderentes.[26]. Os algoritmos que dirigem os carros vão reger as decisões que podem dizer diretamente respeito à integridade física ou até mesmo à vida ou morte das pessoas, por exemplo na escolha programada na eventualidade de um impacto inevitável. Além da necessidade óbvia de clareza sobre quem é responsável e deve prestar contas pelo controlo dos dados e pela segurança dos dados, estas aplicações suscitam várias questões éticas.

1.7 Tendências com um impacto potencialmente maior e de mais longo prazo

Está previsto que a breve trecho fique disponível a **bioimpressão em 3D** de itens biológicos, que utiliza cópias de células de pacientes e «ligaduras biológicas» de colagénio (isto é, dados sensíveis nos termos da legislação da UE) para estabelecer linhas sucessivas de células vivas[27]. Facilitará o fornecimento de partes anatómicas personalizadas e será particularmente valiosa nas zonas do mundo mais pobres e de pós-conflito. A bioimpressão levanta questões óbvias de ética médica, da salvaguarda da propriedade intelectual e da proteção do consumidor mas igualmente, dado que assenta no tratamento de dados íntimos e sensíveis relacionados com a saúde das pessoas, da aplicação das regras em matéria de proteção de dados.

A **inteligência artificial**, tal como a robótica, refere-se a um requisito tecnológico para máquinas autónomas tanto fixas quanto móveis. O seu progresso oferecerá um enorme potencial, para além da sua aplicação atual. Os computadores de aprendizagem profunda ensinam a si próprios tarefas através do tratamento de grandes conjuntos de dados, utilizando (entre outras coisas) redes neurais que parecem imitar o cérebro. Os investigadores e as empresas pretendem melhorar a aprendizagem não supervisionada. Já existem algoritmos capazes de compreender e traduzir línguas, reconhecer imagens, escrever artigos de notícias e analisar dados médicos[28]. As redes sociais fornecem grandes quantidades de informações pessoais que foram previamente rotuladas eficazmente pelas próprias pessoas. Esta poderá ser a mais recente numa linha de melhorias cognitivas para aumentar a capacidade do cérebro

humano, tal como o papel ou o ábaco ou integrado em máquinas autónomas, robôs, mas é chegada a altura de considerar as ramificações mais amplas para as pessoas e a sociedade[29].

2. Um ecossistema de proteção dos megadados

A UE tem agora a oportunidade de assumir a liderança na demonstração do modo como os governos, entidades reguladoras, responsáveis pelo tratamento, *designers*, desenvolvedores e pessoas podem atuar melhor em conjunto para reforçar direitos e orientar, não bloquear, a inovação tecnológica. As tendências descritas na secção dois, no entender de um comentador, «aumentaram o fosso entre aquilo que é possível e o que é legalmente permitido»[30]. Contrariamente ao que é alegado por alguns, a privacidade e a proteção de dados são uma plataforma para um ambiente digital sustentável e dinâmico, não um obstáculo. As autoridades independentes de proteção de dados como a AEPD desempenham um papel crucial na dissipação de tais mitos e na resposta aos receios genuínos das pessoas de perderem o controlo das suas informações pessoais[31].

É provável que a próxima geração de dados pessoais esteja ainda menos acessível às pessoas a que dizem respeito. A responsabilidade pela modelação de um mercado digital único sustentável está necessariamente dispersa, mas é também interdependente, à semelhança de um ecossistema, exigindo uma interação eficaz entre desenvolvedores, empresas e entidades reguladoras na defesa dos interesses da pessoa. Nesta secção expomos as linhas gerais do contributo que estes quatro intervenientes essenciais podem dar.

2.1 Regulamentação orientada para o futuro

Recentemente, instámos a UE a agarrar esta oportunidade histórica de implementar regras mais simples quando se lide com informações pessoais que se manterão relevantes para uma geração[32]. As negociações sobre o Regulamento geral sobre a proteção de dados e a Diretiva relativa à proteção de dados nos setores da polícia e judiciário encontram-se na fase final e, em breve, a atenção voltar-se-á para o futuro da Diretiva relativa à proteção da privacidade no setor das comunicações eletrónicas e do Regulamento que rege o modo como as instituições e órgãos da UE executam eles próprios o tratamento de dados pessoais. Dado que o custo económico de recolha e armazenamento de dados é quase insignificante, recairá sobre as autoridades de proteção de dados a aplicação destas regras de forma consistente, a fim de evitar «risco moral» de um tratamento excessivo de dados[33].

A estratégia do Mercado Único Digital reconhece a ligação entre o controlo de grandes volumes de dados e o poder do mercado. Partilha a convicção, expressa no nosso Parecer preliminar sobre «privacidade e competitividade na era dos grandes volumes de dados», da necessidade de uma maior coerência entre as entidades reguladoras. A UE já dispõe dos instrumentos para corrigir os desequilíbrios de poder no mercado digital: por exemplo, os processos antitrust em curso da Comissão constituem um reconhecimento da predominância de dispositivos móveis para aceder à Internet. A moldura jurídica existente permite uma aplicação mais holística, tal como através de uma câmara de compensação da UE para as autoridades de supervisão considerarem se casos individuais podem suscitar questões de conformidade com as regras em matéria de concorrência e proteção de consumidores e de dados. Por exemplo:

- Exigir uma maior transparência do preço - em numerário ou de outro tipo - de um serviço, pode informar e facilitar a análise de processos de concorrência[34], e

- Detetar discriminação de preços injusta com base na qualidade deficiente dos dados e o estabelecimento de perfis e correlações injustas[35].

Um diálogo mais estreito entre as entidades reguladoras de diferentes setores poderia conduzir a uma resposta aos apelos crescentes para parcerias globais que possam criar bens comuns de dados abertos onde os dados e as ideias, tais como estatísticas e mapas, possam circular e estar disponíveis e serem trocados no interesse do público, com menor risco de vigilância, a fim de conferir às pessoas mais influência sobre as decisões que lhes digam respeito.[36].

2.2 Responsáveis pelo tratamento suscetíveis de sujeição a escrutínio público

A sujeição a escrutínio requer a implementação de políticas e sistemas de controlo internos que assegurem a conformidade e apresentem provas, em especial, às autoridades de supervisão independentes.

Defendemos eliminação da burocracia na legislação em matéria de proteção de dados, através da minimização dos requisitos de documentação desnecessária, com o intuito de maximizar a margem de manobra para iniciativas mais responsáveis por parte das empresas, apoiadas por orientações das autoridades de proteção de dados. O princípio de que os dados pessoais apenas devem ser tratados de formas compatíveis com a ou as finalidades específicas para as quais foram recolhidos é fundamental para respeitar as expectativas legítimas das pessoas. Por exemplo, os códigos de conduta, auditorias, certificação, auditorias e uma nova geração de cláusulas contratuais e regras vinculativas para as empresas podem ajudar a criar uma confiança sólida no mercado digital. Os responsáveis pela transmissão de informações pessoais devem ser muito mais dinâmicos e proativos e afastarem-se da tendência denominada «Black Box» (Caixa Negra) de secretismo e opacidade das práticas comerciais, ao mesmo tempo que exige mais transparência aos clientes[37].

2.3 Engenharia respeitadora da privacidade

A inovação humana tem resultado sempre de atividades de grupos sociais específicos e de contextos específicos, que normalmente refletem as normas sociais da época[38]. Contudo, as decisões em matéria de desenho tecnológico não devem ditar as nossas interações sociais e a estrutura das nossas comunidades, devendo, pelo contrário, apoiar os nossos valores e direitos fundamentais.

A UE deveria desenvolver e promover técnicas e metodologias de engenharia que permitam implementar tecnologias de tratamento de dados que respeitem cabalmente a dignidade e direitos das pessoas. Os engenheiros de sistemas e de programas informáticos necessitam de perceber e aplicar melhor os princípios da privacidade desde a conceção nos novos produtos e serviços nas fases e tecnologias de conceção. A sujeição a escrutínio necessita de ser apoiada por uma maior investigação e desenvolvimento de métodos e instrumentos para assegurar auditorias precisas e para determinar a conformidade dos responsáveis pelo tratamento e dos subcontratantes com as regras, tais como «etiquetar» cada unidade de dados pessoais com «metadados» que descrevam os requisitos em matéria de proteção de dados.

As soluções de engenharia devem capacitar as pessoas que pretendam preservar a sua privacidade e liberdade através do anonimato. A UE deve promover a conceção e implementação de algoritmos que ocultem as identidades e os dados agregados, a fim de proteger as pessoas ao mesmo tempo que tiram partido do poder preditivo dos dados[39].

Devemos criar hoje os alicerces para fazer face a estas missões, reunindo desenvolvedores e peritos em proteção de dados de diferentes domínios em redes abrangentes, tais como a Rede de Engenharia de Privacidade para a Internet (Internet Privacy Engineering Network - IPEN), que contribuam para um intercâmbio de ideias e abordagens interdisciplinares profícuos.

2.4 Pessoas capacitadas

Um ambiente de «produtores-consumidores»

As pessoas não são meros objetos passivos que necessitam de proteção da lei contra a exploração. As tendências digitais expostas anteriormente apresentam oportunidades positivas para reforçar o papel das pessoas. Por exemplo, hoje em dia as pessoas produzem e consomem conteúdos e serviços, podendo cada vez mais serem consideradas conjuntamente responsáveis com os prestadores de serviços pelo tratamento de dados pessoais, salvo se se destinar a fins puramente «domésticos»[40] (o conceito de «produtores-consumidores» surgiu para descrever esta evolução[41]). Entretanto, as moedas virtuais oferecem aos utilizadores o anonimato e a possibilidade de contornar a verificação das transações por parte de terceiros e, por conseguinte, menores custos de transação no pagamento por bens e serviços transfronteiriços. Por outro lado, o anonimato e a natureza transjurisdicional (ou, conforme se poderá argumentar, *ajurisdicional*) destas moedas virtuais tornam as pessoas vulneráveis à fraude e aos mercados criminosos difíceis de detetar e investigar. Para além dos deveres das entidades reguladoras, das empresas e dos engenheiros, os cidadãos são também responsáveis por estarem cientes, atentos, de serem críticos e de estarem informados quando fazem escolhas tanto em linha quanto fora de linha[42].

Consentimento

Além disso, contrariamente ao pensamento tradicional, nem todo o comportamento humano pode ser explicado por princípios económicos que assumem que os seres humanos são completamente racionais e sensíveis a incentivos económicos[43]. Tal afigura-se relevante para o futuro papel do consentimento da pessoa ao tratamento de informações pessoais que lhe digam respeito. Nos termos da legislação da UE, o consentimento não constitui a única base legítima para a maior parte do tratamento. Mesmo nos casos em que o consentimento desempenha um papel importante, não exime os responsáveis pelo tratamento da sujeição a escrutínio relativamente ao que fazem com os dados, sobretudo se tiver sido obtido um consentimento generalizado para proceder ao tratamento para uma vasta gama de finalidades.

Controlo e «propriedade» dos dados

As pessoas devem poder contestar erros e ideias preconcebidas injustas decorrentes da lógica utilizada por algoritmos para determinar pressupostos e previsões. A título ilustrativo, nos EUA um estudo de cerca de 3 000 relatórios de crédito pertencentes a 1 000 consumidores concluiu que 26 por cento continham problemas de erros «materiais» suficientemente graves para afetar as classificações de crédito dos consumidores e, portanto, o custo da obtenção de crédito[44].

Os dados são muitas vezes considerados um recurso, à semelhança do petróleo, para ser comercializado, idealmente, por partes da transação igualmente bem informadas[45]. Os clientes não são justamente compensados pelas suas informações pessoais que são comercializadas e alguns defenderam um modelo de propriedade dos dados. Todavia, é difícil garantir um controlo absoluto dos dados pessoais: haverá outras preocupações como o interesse público e os direitos e liberdades de terceiros. O controlo é necessário, mas não

suficiente[46]. No entanto, a dignidade humana está sempre presente e, nos termos da legislação da UE, a analogia de propriedade não pode ser aplicada como tal a informações pessoais, que têm uma ligação intrínseca às personalidades individuais. Não existe nenhuma disposição na legislação da UE em matéria de proteção de dados para que uma pessoa possa renunciar a este direito fundamental.

Um método alternativo para proporcionar às pessoas um melhor controlo dos seus dados, quem pode aceder e para que finalidade, poderia residir na utilização de depósitos de dados pessoais ou «caixas-fortes de dados»[47]. O conceito de um tal «depósito pessoal» requer mecanismos de segurança que assegurem que apenas as entidades autorizadas pela pessoa em causa possam aceder aos dados e apenas às partes para as quais estão autorizadas. Os depósitos de dados pessoais serão mais eficazes se disserem respeito a informações atuais e continuamente atualizadas, tais como dados geoespaciais ou sinais de vida. Para além das salvaguardas técnicas, os utilizadores de dados seriam obrigados a respeitar as regras em matéria de partilha e utilização de dados. A concorrência e a possibilidade de se mudar de serviço utilizado são o único poder mais eficaz dos consumidores para influenciar o mercado de serviços que têm ao dispor. Assegurar a portabilidade das ligações, nomeadamente identificadores e informações de contacto, demonstrou ser um fator-chave para a concorrência e reduziu eficazmente os preços no consumidor, após a liberalização do mercado das telecomunicações. A portabilidade dos dados, que é a possibilidade factual e prática de transferir a maior parte dos dados de uma pessoa de um prestador de serviços para outro, representa um ponto de partida eficaz para criar as condições para um verdadeira escolha do consumidor.

3. A dignidade no âmago da uma nova ética digital

É necessário que um enquadramento ético apoie os pilares de base deste ecossistema digital. A AEPD considera que um melhor respeito e a salvaguarda da dignidade humana poderão servir de contrapeso à vigilância difusa e assimetria de poder com que as pessoas são atualmente confrontadas. Tal deve estar no âmago da uma nova ética digital.

3.1 Dignidade e dados

No seguimento da revolução industrial dos séculos XVIII e XIX, o movimento dos direitos humanos procurou assegurar o bem social mais lato através da redução das barreiras ao respeito pela pessoa. A UE assumiu agora, com a Carta dos Direitos Fundamentais, e na sequência da Declaração Universal dos Direitos Humanos e da Convenção Europeia dos Direitos do Homem, como ponto de partida a inviolabilidade da dignidade do ser humano. A dignidade do ser humano constitui não só um direito fundamental em si mesma, mas também a base para as liberdades e os direitos subsequentes, nomeadamente os direitos à privacidade e à proteção de dados pessoais[48]. As violações da dignidade podem incluir a objetificação, em que uma pessoa é tratada como um instrumento para servir os propósitos de terceiros[49]. A privacidade é parte integrante da dignidade humana e o direito à proteção de dados foi originalmente concebido na década de 1970 e 1980 como forma de compensar o potencial de erosão da privacidade e dignidade através do tratamento de dados pessoais em grande escala. Na Alemanha o direito à «autodeterminação informativa» teve por base os direitos à dignidade pessoal e o livre desenvolvimento da personalidade previstos nos artigos 1.º e 2.º da Constituição alemã[50].

Contudo, no início do século XXI, é cada vez mais solicitado às pessoas que divulguem muitas mais informações pessoais na Internet, a fim de participarem em assuntos sociais,

administrativos e comerciais, o que implica um âmbito cada vez mais restrito para a autoexclusão. Com toda a atividade potencialmente sempre em linha, a noção de consentimento livre e informado é submetida a uma enorme pressão. Vão sendo deixadas «migalhas de pão digitais» a cada minuto que são combinadas para classificarem as pessoas em tempo real e criar perfis múltiplos e, por vezes, contraditórios. Estes perfis podem ser distribuídos em microssegundos sem o conhecimento das pessoas e ser utilizados como a base para decisões importantes que lhes dizem respeito.

A utilização de perfis para prever o comportamento das pessoas acarreta o risco de estigmatização, reforçando os estereótipos existentes, a segregação social e cultural e a exclusão[51], com essa «inteligência coletiva» a subverter a escolha individual e a igualdade de oportunidades. Essas «bolhas de filtro» ou «câmaras de eco pessoais» podem acabar por sufocar a criatividade, inovação e liberdades de expressão e associação que permitiram a expansão das tecnologias digitais.

Entretanto, é utilizado um estado permanente de exceção com base na «segurança» para justificar as múltiplas camadas de técnicas intrusivas para monitorizar a atividade das pessoas[52]. Compreender este «propulsor da vigilância» exige uma perspetiva de longo prazo sobre os efeitos gerais na sociedade e no comportamento.

Juntamente com países terceiros, a UE necessita de ponderar seriamente como assegurar que estes valores não são meramente respeitados no papel, enquanto na prática são neutralizados no ciberespaço. A UE, em especial, tem agora um período decisivo antes da adoção generalizada destas tecnologias para integrar os valores nas estruturas digitais que vão definir a nossa sociedade.[53]. Tal requer uma nova avaliação de se os potenciais benefícios das novas tecnologias dependem realmente da recolha e análise das informações pessoais identificáveis de milhares de milhões de pessoas. Tal avaliação poderá desafiar os desenvolvedores a conceberem produtos que despersonalizem em tempo real volumes colossais de informações desorganizadas, fazendo com que seja mais difícil ou impossível distinguir uma pessoa.

É já reconhecido que certos tratamentos de dados, por exemplo, de dados genéticos, não devem apenas ser regulados, mas também sujeitos à avaliação das preocupações sociais mais latas realizada, por exemplo, por comités de ética. Atendendo à sua natureza, os dados genéticos não dizem apenas respeito à pessoa, mas também à sua ascendência e descendência. Os dados genéticos não servem apenas para identificar laços familiares, os elementos encontrados nos genes de uma pessoa podem também fornecer informações sobre os seus progenitores e filhos e conduzir a decisões por parte dos responsáveis pelo tratamento que influenciam as suas oportunidades na vida antes mesmo do seu nascimento. A potencial concentração de dados pessoais genéticos nas mãos de alguns operadores gigantes do mercado tem implicações para as economias de mercado, bem como para as pessoas em causa. Uma dependência crescente de um sistema global para a recolha e análise de um fluxo constante de dados pode tornar a sociedade e a economia mais vulneráveis a falhas de segurança e ataques maliciosos sem precedentes.

Caso não abordemos o futuro com um pensamento inovador, a moldura existente é suscetível de falhar. Existe uma procura e necessidade crescentes de considerar a pessoa em causa como uma pessoa e não apenas um consumidor ou utilizador. As autoridades de proteção de dados verdadeiramente independentes têm um papel crucial na prevenção de um futuro no qual as pessoas sejam determinadas por algoritmos e as suas contínuas variações. Devem estar equipadas para exercer um «dever de diligência» em relação às pessoas e a sua dignidade em linha. Os conceitos e princípios tradicionais de privacidade e proteção de dados já contêm

cambiantes éticas para a proteção da dignidade, tais como o emprego e a saúde. Mas as tendências atuais abriram um capítulo completamente novo, afigurando-se necessário explorar se os princípios são suficientemente robustos para a era digital[54]. A própria noção de dados pessoais é provável que mude radicalmente, dado que a tecnologia permite cada vez mais que as pessoas sejam reidentificadas a partir de dados supostamente anónimos. Além disso, a aprendizagem automática e a fusão da inteligência humana e artificial vão minar os conceitos dos direitos e responsabilidade das pessoas.

3.2 Um Conselho Consultivo de Ética europeu

Não se trata de traçar um quadro alarmista de distopia. Já estão em curso debates nas esferas jurídica, política, económica, social, científica e até mesmo religiosa[55]. As abordagens simplistas que conferem vantagem unilateral ao lucro económico ou à vigilância para proteção não são provavelmente mais úteis do que a aplicação excessivamente restritiva das leis existentes que obviam à inovação e ao progresso. Por conseguinte, a AEPD propõe uma análise exaustiva, ampla e multidisciplinar para apresentar recomendações e informar o debate social sobre de que modo uma sociedade livre e democrática deve enfrentar o desafio tecnológico.

A Estratégia da AEPD [56] empenhada em desenvolver uma abordagem ética para a proteção de dados que reconheceu que «a exequibilidade, utilidade ou rentabilidade não são sinónimos de sustentabilidade» e que salientou «a supremacia da responsabilização sobre a conformidade mecânica com a letra da lei». Pretendemos um alcance que vá além da comunidade de funcionários, advogados e especialistas informáticos da UE em direção a pessoas eminentes que estão preparadas para aferir as implicações de médio a longo prazo da alteração tecnológica e das respostas regulamentares. Nos próximos meses, vamos criar na nossa instituição independente um grupo consultivo externo sobre a dimensão ética da proteção de dados, para explorar as relações entre os direitos humanos, a tecnologia, os mercados e os modelos de negócio no século XXI.

O nosso Conselho Consultivo de Ética será composto por um grupo de destacadas personalidades dos domínios da ética e filosofia, sociologia, psicologia, tecnologia e economia que contarão, conforme necessário, com o apoio de peritos adicionais com conhecimentos e experiência em domínios como a saúde, os transportes e a energia, a interação social e os meios de comunicação social, a economia e finanças, a governação e democracia e a segurança e o policiamento. Serão convidadas a considerar as implicações éticas mais vastas do modo como os dados pessoais são concebidos e utilizados, sendo dada a máxima transparência às suas deliberações.

4. Conclusão: é chegada a altura de aprofundar o debate

A privacidade e a proteção de dados fazem parte da solução, não do problema. Por ora, a tecnologia é controlada pelos humanos. Não é fácil classificar exatamente estes desenvolvimentos potenciais como bons ou maus, desejáveis ou nocivos, vantajosos ou prejudiciais, muito menos quando um número de tendências potenciais carece de ser contextualizado. Os decisores políticos, os desenvolvedores de tecnologia, os empresários e todos nós temos de considerar seriamente se e de que modo queremos influenciar o desenvolvimento de tecnologia e a sua aplicação. Mas igualmente importante é que a UE considere urgentemente a ética e o papel da dignidade humana nas tecnologias do futuro.

Os princípios da proteção de dados provaram ser capazes de salvaguardar as pessoas e a sua privacidade dos riscos associados ao tratamento de dados irresponsável. Mas as tendências atuais poderão requerer uma abordagem completamente nova. Assim, estamos a iniciar um novo debate sobre até que ponto a aplicação dos princípios tais como a justiça e a legitimidade é suficiente. A comunidade de proteção de dados pode desempenhar um novo papel utilizando ferramentas existentes como verificações e autorizações prévias, porque nenhum outro órgão está equipado para controlar tal tratamento de dados. O desenvolvimento da tecnologia, da inovação global e da conectividade humana a uma velocidade vertiginosa proporcionam uma oportunidade para atrair atenção, suscitar interesse e construir um consenso.

Com o presente Parecer esperamos poder fornecer uma moldura para um debate mais amplo e aprofundado acerca do modo como a UE pode assegurar a integridade dos seus valores ao mesmo tempo que usufrui dos benefícios das novas tecnologias.

Feito em Bruxelas, em 11 de setembro de 2015

(**assinatura)**

Giovanni BUTTARELLI
Autoridade Europeia para a Proteção de Dados

Notas

[1] Fonte: GSMA Intelligence.

[2] A «Lei de Moore» que defende que o número de transístores que podem ser colocados numa micropastilha duplica a cada 18 meses demonstrou estar, de um modo geral, correta; Moore, Gordon E. (1965-04-19). «*Cramming more components onto integrated circuits*», Electronics. 22-08-2011

[3] Nathan Eagle, Alex (Sandy) Pentland, «*Reality mining: sensing complex social systems*», Journal Personal and Ubiquitous Computing Volume 10 4.ª Edição, março de 2006, pp. 255–268. Shoshana Zuboff em «*Big Other: surveillance capitalism and the prospects of an information civilization*», Journal of Information Technology (2015) 30, pp. 75-89, escreve «Como resultado de uma mediação informática difusa, praticamente cada aspeto do mundo é traduzido numa nova dimensão simbólica à medida que os eventos, os objetos, os processos e as pessoas se tornam visíveis, reconhecíveis e partilháveis de uma nova maneira». Zuboff prevê o «surgimento de uma nova arquitetura universal» que designa de «Big Other», «um regime ubíquo de instituições ligadas em rede que regista, modifica e mercantiliza a experiência do dia-a-dia desde torradeiras a corpos, comunicação a pensamento, com o propósito de criar novas vias para a monetização e o lucro»; pp. 77, 81.

[4] «*BBC Micro Bit computer's final design revealed*» 7.7.2015, http://www.bbc.com/news/technology-33409311(acedido em 10.09.2015); «*No assembler required: How to teach computer science in nursery school*», The Economist, 1.8.2015.

[5] Nenhuma das dez principais empresas do setor da tecnologia por capitalização bolsista se encontra sediada na UE (oito nos EUA, uma na China e outra em Taiwan) segundo o relatório das Dez Principais Empresas por Capitalização Bolsista da PWC (Global Top Ten Companies by Market Capitalisation), Atualização de 31 de março de 2015.

[6] «Megadados refere-se ao aumento exponencial da disponibilidade e da utilização automatizada de informações: refere-se a conjuntos de dados digitais gigantescos detidos por empresas, governos e outras organizações de grandes dimensões, que são depois extensivamente analisados (daí o nome "analítica") com recurso a algoritmos informáticos»; Parecer 3/2013 do GT29 sobre a limitação da finalidade. Um relatório da White House em 2014 descreveu os Megadados como «A capacidade tecnológica crescente para capturar, agregar e processar um volume, velocidade e variedade de dados cada vez maiores», ver «*Big Data*: *Seizing Opportunities, Preserving Values,* Gabinete Executivo do Presidente *("Podesta-report")*», maio de 2014.

[7] Nos termos da legislação da UE, os «dados pessoais» são definidos como «qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social», artigo 2.º, alínea a), da Diretiva 95/46/CE. Esta definição é, em larga medida, comparável às adotadas pelo Conselho da Europa na Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (conhecida como a Convenção 108) e pelas Linhas de orientação da OCDE sobre a proteção da privacidade e os fluxos transfronteiras de dados pessoais. Para uma análise aprofundada, consultar o «Parecer 4/2007 sobre o conceito de dados pessoais», WP136 do Grupo de Trabalho do artigo 29.º.

[8] Ver, por exemplo, o discurso da Presidente da Comissão Federal do Comércio dos Estados Unidos, em 2014: «A proliferação dos dispositivos conectados, a queda abrupta dos preços de recolha, armazenamento e tratamento de informações, bem como a capacidade de os corretores de dados e outros profissionais combinarem dados fora de linha e em linha significa que as empresas podem acumular praticamente quantidades ilimitadas de informações sobre consumidores e armazená-las por tempo indefinido. Recorrendo à analítica preditiva, podem ficar a conhecer uma quantidade surpreendente de informações sobre cada um de nós a partir destes elementos;» Declarações iniciais da Presidente da CFC Edith Ramirez, «B*ig Data: A Tool for Inclusion or Exclusion?*», Washington,

DC 15 de setembro de 2014. Segundo Sandy Pentland, «A física social é uma ciência social quantitativa que descreve ligações fiáveis e matemáticas entre as informações e o fluxo de ideias, por um lado, e o comportamento das pessoas, por outro... permite-nos prever a produtividade de pequenos grupos, de departamentos no seio de empresas e até mesmo de cidades completas». Isto «é aquilo de que se necessita para criar melhores sistemas sociais» (pp. 4, 7) e para «permitir aos responsáveis governamentais, gestores das indústrias e cidadãos) utilizarem as ferramentas dos incentivos da rede social para *estabelecer novas normas de comportamento*» (p. 189) (os itálicos são da nossa autoria); Pentland, «*Social Physics: How Good Ideas Spread: The Lessons from a New Science*».

[9] Eurabarómetro Especial 431 sobre a Proteção de Dados, junho de 2015, e Estudo do Painel da Pew Research, de janeiro de 2014, sobre as Perceções Públicas da Privacidade e Segurança na Era pós-Snowden («*Public Perceptions of Privacy and Security in the Post-Snowden Era*»). De acordo com os resultados de um estudo, uma visita normal a um único sítio Web resulta em 56 casos de recolha de dados, segundo Julia Angwin «*Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, 2012).» O relatório de 2014 da White House sobre megadados argumenta que «um poder e sofisticação computacionais... criam uma assimetria de poder entre aqueles que estão na posse dos dados e aqueles que intencional ou inadvertidamente os fornecem»; «alguns dos desafios mais profundos revelados durante esta análise prendem-se com o modo como a analítica dos megadados poderá... criar um ambiente de tomada de decisão tão opaco onde a autonomia individual se perde num conjunto impenetrável de algoritmos».

[10] Utilizando os dados anónimos públicos do recenseamento de 1990, 87% da população dos EUA poderia provavelmente ser identificada pelo respetivo código postal de 5 dígitos combinado com o género e data de nascimento; ver Paul Ohm «*Broken promises of privacy: responding to the surprising failure of anonymisation*», UCLA Law Review 2010 e «*Record linkage and privacy: issues in creating new federal research and statistical info*», abril de 2011. O ADN é único (salvo para os gémeos univitelinos) e estável ao longo da vida. Contém informações sobre a etnia, predisposições para doenças e permite identificar outros membros da família. Em janeiro de 2013, os investigadores conseguiram identificar pessoas e famílias a partir dos dados de ADN de bases de dados genealógicas acessíveis ao público; Gymrek, M., McGuire, A. L., Golan, D., Halperin, E. & Erlich, Y. *Science* 339, 321–324 (2013). Ver igualmente «*Poorly anonymized logs reveal NYC cab drivers' detailed whereabouts*», 23.06.2014 http://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/ (acedido em 10.09.2015). Consultar também o Parecer 04/2007 sobre o conceito de dados pessoais do GT29, o Parecer 03/2013 sobre a limitação da finalidade do GT29; o Parecer 06/2013 sobre os dados abertos e a reutilização de informações do setor público («ISP») do GT29; e o Parecer 05/2014 sobre técnicas de anonimização do GT29.

[11] Fonte: Gartner.

[12] Ver, por exemplo, o debate «*What is the future of official statistics in the Big Data era?*» Royal Statistical Society, Londres 19 de janeiro de 2015; http://www.odi.org/events/4068-future-official-statistics-big-data-era (acedido em 10.09.2015).

[13] «*Ten technologies which could change our lives: potential impacts and policy implications*» (Dez tecnologias que poderiam mudar as nossas vidas: potenciais impactos e implicações políticas), Unidade da Prospetiva Científica, Serviço de Estudos do Parlamento Europeu, janeiro de 2015.

[14] O programa de trabalho para o período compreendido entre 2016 e 2017 do Programa Horizonte 2020 da UE está a apoiar estes desenvolvimentos, incluindo projetos-piloto em grande escala que irão analisar as preocupações em matéria de privacidade e éticas.

[15] O setor dos seguros foi descrito como o «modelo nativo para a Internet das Coisas»; «*From fitness trackers to drones, how the "Internet of Things" is transforming the insurance industry*», Business Insider 11.6.2015. A noção de discriminação dos preços no direito da concorrência, decorrente do artigo 102.º do TFUE, proíbe uma empresa com uma posição dominante no mercado de «impor, de forma direta ou indireta, preços de compra ou de venda ou outras condições de transação não equitativas», é altamente controversa, ver por exemplo Damien Gerardin e Nicolas Petit «*Price*

Discrimination Under EC Competition Law: Another Antitrust Theory in Search of Limiting Principles» (julho de 2005), Global Competition Law Centre Working Paper Series No. 07/05. Em relação aos megadados e ao seu (segundo os autores ainda por concretizar) potencial para acelerar os preços personalizados, ver Gabinete Executivo do Presidente dos Estados Unidos, «*Big Data and Differential Pricing*» (Megadados e Diferenciação de Preços), fevereiro de 2015, e uma análise recente que conclui que os preços personalizados conduzem, normalmente, ao tratamento de dados pessoais e, por conseguinte, devem observar o princípio de transparência previsto na legislação em matéria de proteção de dados que obriga as empresas a informarem as pessoas sobre a finalidade do tratamento dos seus dados pessoais: as empresas devem facultar essa informação se personalizarem os preços. E se as empresas utilizarem um *cookie* para reconhecer alguém, a Diretiva relativa à proteção da privacidade no setor das comunicações eletrónicas exige que a empresa informe a pessoa sobre a finalidade do *cookie*; projeto de trabalho de Frederik Borgesius «*Online Price Discrimination and Data Protection Law*». Disponível em http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2652665 (acedido em 10.09.2015).

[16] Os dispositivos médicos encontram-se definidos na legislação da UE ao abrigo da Diretiva 93/42/CEE do Conselho, relativa aos dispositivos médicos, com a redação que lhe foi dada pela Diretiva 2007/47/CE do Parlamento Europeu e do Conselho, de 5 de setembro de 2007. Em relação às implicações da proteção de dados da «saúde móvel», ver o Parecer 1/2015 da AEPD.

[17] Segundo o Eurostat, 21% das pessoas e 19% das empresas na UE utilizam serviços de armazenamento em nuvem.

[18] «Se a Internet mundial fosse um país, seria o 12.º maior consumidor de eletricidade do mundo, situando-se algures entre Espanha e Itália. Tal representa aproximadamente 1,1 a 1,5 por cento do consumo mundial de eletricidade (em 2010) e gases com efeito de estufa gerados anualmente por 70 a 90 grandes (500 megawatts) centrais elétricas a carvão.» Conselho para a Defesa de Recursos Naturais, Avaliação de Eficiência do Centro de Dados: «*Scaling Up Energy Efficiency Across the Data Centre Industry: Evaluating Key Drivers and Barriers*» 2014.

[19] Relatório do estudo «SMART 2013/0043 - *Uptake of Cloud in Europe*» (Implantação da Computação em Nuvem na Europa).

[20] Fonte: Eurostat.

[21] O termo «economia de partilha» foi criticado como se tratando de enganador: «*The Sharing Economy Isn't About Sharing at All*», Giana M. Eckhardt e Fleura Bardhi, Harvard Business Review, 28.01.2015.

[22] Rachel Botsman e Roo Rogers, «*What's Mine Is Yours: How Collaborative Consumption is Changing the Way We Live*», 2011.

[23] Fórum sobre o Futuro da Privacidade, «*User Reputation: Building Trust and Addressing Privacy Issues in the Sharing Economy*», junho de 2015.

[24] Ver o seminário, de 9 de junho de 2015, da Comissão Federal do Comércio dos Estados Unidos «*Competition, Consumer Protection, and Economic Issues Raised by the Sharing Economy*», https://www.ftc.gov/news-events/events-calendar/2015/06/sharing-economy-issues-facing-platforms-participants-regulators/ (acedido em 10.09.2015).

[25] Em relação às implicações em matéria de proteção de dados das aeronaves não tripuladas ou dos sistemas de aeronaves telepilotadas, ver o parecer da AEPD sobre a Comunicação da Comissão ao Parlamento Europeu e ao Conselho intitulada «Uma nova era para a aviação — Abrir o mercado da aviação à utilização civil de sistemas de aeronaves telepilotadas de forma segura e sustentável», novembro de 2014.

[26] Fonte: Boston Consulting Group.

[27] Gartner.

[28] O algoritmo de reconhecimento facial DeepFace do Facebook indicou 97% de sucesso - superando as pessoas; «*DeepFace: Closing the Gap to Human-Level Performance in Face Verification*», publicado no relatório da Conferência da IEEE sobre Visão Computacional e Reconhecimento de padrões, junho de 2014.

[29] O termo robô tem sido definido como uma «máquina situada no mundo que sente, pensa e atua»; Bekey, G, «*Current trends in robotics: technology and ethics, em Robot Ethics - The ethical and social implications of robotics*», The MIT Press2, 2012, p. 18. Estima-se que entre 2013 e 2016 terão sido vendidos 22 milhões de robôs de serviço; Relatório IRF World Robotics, 2013. Sobre inteligência artificial ver «*Rise of the Machines*», Economist, 09.5.15 e Projeto Internet 2014 do Centro de Investigação Pew. Em 2014, uma empresa de inteligência artificial condicionou a sua aquisição por parte de uma empresa líder de tecnologia à criação de um conselho de ética e segurança e uma proibição de utilizar o trabalho de inteligência artificial para fins militares ou de serviços de informações; Forbes, «*Inside Google's Mysterious Ethics Board*», 03.02.2014.

[30] Pentland, «*Social physics*», p. 147.

[31] Ver nota 9 *supra*. Pentland «*Social Physics*» p. 153: «Os grandes avanços nos cuidados de saúde, nos transportes, na energia e na segurança são todos possíveis...os principais obstáculos à consecução destes objetivos são os receios em matéria de privacidade e o facto de ainda não dispormos de qualquer consenso sobre o equilíbrio entre valores pessoais e sociais». O debate em torno da pandemia do Ébola em 2014 na África Ocidental ilustra bem a forma como está traçada esta falsa dicotomia entre privacidade individual e necessidades sociais. A tendência tem sido fazer o seguimento das doenças e medir o seu ciclo de vida através de inquéritos e censos que facilmente se tornam obsoletos e são difíceis de extrapolar para antecipar onde surgirá o próximo surto. Existem alguns exemplos de utilização de «megadados» para fazer o seguimento de surtos de malária na Namíbia e no Quénia e, em 2009, para fazer o seguimento da eficácia das advertências governamentais relativas à saúde durante a crise da gripe suína no México. Uma fonte de dados são os registos de chamadas móveis que mostram a estação de base que atendeu a chamada e podem facultar em tempo real uma estimativa aproximada da localização das pessoas e para onde se dirigem. A recolha desses registos não é especificamente dirigida, não permitindo fazer a distinção entre os que estão ou não estão infetados com o Ébola. Uma organização sueca sem fins lucrativos fez um levantamento da mobilidade das pessoas na África Ocidental, mas não foi possível utilizar os dados, porque os operadores de comunicações móveis não os facultavam a investigadores externos aprovados, alegando que necessitavam de instruções dos governos que, por sua vez, evocaram preocupações relacionadas com a privacidade que não poderiam estar garantidas nos termos da legislação da UE; http://www.pri.org/stories/2014-10-24/how-big-data-could-help-stop-spread-ebola. (acedido em 10.09.2015)

[32] Parecer 3/2015 da AEPD.

[33] Um pressuposto dos megadados de que «N=all» se refere a olhar para todos os pontos de dados e não apenas uma amostra, Viktor Mayer-Schönberger, e Kenneth Cukier, «*The Rise of Big Data: How it's changing the way we think about the world*», 2013 .O Conselho de Lisboa e o Instituto de Política Progressiva argumentaram que a prosperidade aumentará através da maximização da «densidade digital» - «a quantidade de dados utilizados *per capita* numa economia» http://www.lisboncouncil.net/component/downloads/?id=1178 (acedido em 10.09.2015). O Grupo de Trabalho Internacional relativo à Proteção de Dados nas Telecomunicações (designado «Grupo de Berlim») propôs derrogações aos princípios de proteção de dados relativamente aos megadados; http://www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf. (acedido em 10.09.2015). O Fórum Económico Mundial apelou a uma concentração na utilização e não na recolha e para um afastamento do requisito de consentimento para a recolha de dados pessoais, «*Unlocking the Value of Personal Data: From Collection to Usage*», 2013.

[34] Ver o Parecer preliminar da AEPD sobre privacidade e competitividade na era dos grandes volumes de dados.

[35] O artigo 21.º da Carta dos Direitos Fundamentais proíbe «qualquer discriminação em razão, designadamente, do sexo, raça, cor, origem étnica ou social, características genéticas, língua, religião ou convicções, opiniões políticas ou outras, pertença a uma minoria nacional, riqueza, nascimento, deficiência, idade ou orientação sexual». Muitas destas categorias de dados («que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual» são objeto de proteção reforçada nos termos do artigo 8.º da Diretiva 95/46/CE.

[36] Em relação à ideia de um bem comum digital ver «*Ambition numérique: Pour une politique française et européenne de la transition numérique*», Conselho Digital francês, junho de 2015 p. 276; Bruce Schneier advoga a criação de «espaços públicos sem proprietário» na Internet, tais como parques públicos, «*Data and Goliath*», pp. 188-189; Sandy Pentland defende um «bens comuns de dados públicos», «*Social Physics*», p. 179. Em relação à avaliação da segurança da publicação de conjuntos de dados agregados, ver o Parecer 06/2013 sobre os dados abertos e a reutilização de informações do setor público («ISP») do GT29.

[37] «*Während die Einzelnen immer transparenter werden, agieren viele Unternehmen hochgradig intransparent*» http://crackedlabs.org/studie-kommerzielle-ueberwachung/info. Em relação à transparência qualificada, ver, por exemplo, Frank Pasquale: «*The Black Box Society: The Secret Algorithms that Control Money and Information*».

[38] «*Behind the technology that affects social relations lie the very same social relations*», David Noble, «*Social Choice in Machine Design: The Case of Automatically Controlled Machine Tools*», em *Case Studies in the Labor Process*, ed. Andrew Zimbalist, 1979. Ver igualmente Judy Wacjman, «*Pressed for Time: The Acceleration of Life in Digital Capitalism*», 2014 pp. 89-90; e Zuboff, «*Big Other*» (citado na nota 3 *supra*).

[39] Parecer 05/2014 sobre técnicas de anonimização, adotado em 10 de abril de 2014 (GT 216.)

[40] Em relação a uma isenção objeto de interpretação estrita às regras de proteção para fins exclusivamente pessoais ou domésticos ver o acórdão do TJUE Processo C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů*.

[41] O termo produtor-consumidor foi cunhado por Alvin Toffler em «*The Third Wave*», 1980. Em relação a um debate sobre o «ambiente de produtor-consumidor» e de que modo deveria ser regulado, ver Ian Brown e Chris Marsden, «*Regulating Code*», 2013.

[42] Parecer do Grupo Europeu de Ética para as Ciências e as Novas Tecnologias para a Comissão Europeia: «*Ethics of Security and Surveillance Technologies*» (Ética das Tecnologias de Segurança e Vigilância), Parecer n.º 28, 20.05.2015, p. 74.

[43]Ver, por exemplo, Homer Economicus: «*The Simpsons and Economics*» ed. Joshua Hall, 2014.

[44] Ao abrigo da definição mais conservadora de erro, isto significa que 23 milhões de norte-americanos tinham erros materiais num relatório de consumidor. Cinco por cento dos participantes no estudo tinham erros que, assim que corrigidos, melhoravam a sua classificação de crédito de tal modo que poderiam obter crédito a um preço inferior; Relatório da Comissão Federal do Comércio ao Congresso nos termos da secção 319 da *The Fair And Accurate Credit Transactions Act Of 2003*, dezembro de 2012; Chris Jay Hoofnagle, «*How the Fair Credit Reporting Act Regulates Big Data*» (10 de setembro de 2013). «*Future of Privacy Forum Workshop on Big Data and Privacy: Making Ends Meet*», 2013. Disponível em SSRN: http://ssrn.com/abstract=2432955.

[45] O Fórum Económico Mundial pressupõe os dados como um ativo valioso da pessoa cujos direitos de posse, utilização e eliminação podem ser conferidos a empresas e governos em troca de serviços. Ver também os recentes discursos de entre os quais o do Vice-Presidente da Comissão Andrus Ansip, por exemplo, em 7.9.2015 na reunião anual do grupo de reflexão Bruegel com o título «Produtividade,

inovação e digitalização - quais os desafios políticos globais?»: «Propriedade e gestão dos fluxos de dados, utilização e reutilização de dados. Gestão e armazenamento de dados. Estes apoiam setores emergentes importantes como a computação em nuvem, a Internet das Coisas e os megadados».

[46] «Quem possui então o direito de utilizar as informações e os dados que não pertencem verdadeiramente a uma pessoa? Trata-se de uma questão que transcende fronteiras de comércio, ética e moral, conduzindo a questões de privacidade e à proteção da privacidade; Al-Khouri Nov 2012, http://www.academia.edu/6726887/Data_Ownership_Who_Owns_My_Data_036. Ver igualmente Margaret Jane Radin, «*Incomplete Commodification in the Computerized World*», em The Commodification of Information 3, 17, Niva Elkin-Koren & Neil Weinstock Netanel eds. 2002: «Faz toda a diferença se a privacidade é considerada um direito humano, associado às pessoas por força da sua individualidade, ou um direito de propriedade, algo que pode ser detido e controlado por pessoas. Os direitos humanos são presumivelmente inalienáveis do mercado, ao passo que os direitos de propriedade são presumivelmente alienáveis do mercado».

[47] O projeto Crosscloud do MIT Computer Science and Artificial Intelligence Lab (Laboratório de Inteligência Artificial e de Ciência de Computadores do MIT) apoiado por várias empresas sediadas na UE visa 1) facilitar o desenvolvimento de programas informáticos de multiutilizadores («sociais»), utilizando apenas o desenvolvimento *front-end* e respeitando os direitos e a privacidade dos utilizadores. E 2) permitir aos utilizadores a liberdade de se deslocarem facilmente entre aplicações, plataformas de equipamento e redes sociais, mantendo os seus dados e ligações sociais»; http://openpds.media.mit.edu/#architecture (acedido em 10.09.2015).

[48] Ver Explicação do artigo 1.º da Carta dos Direitos Fundamentais.

[49] Martha Nussbaum, «*Objectification*», em Philopsophy and Public Affairs 24-4-1995.

[50] Acórdão de 15 de dezembro de 1983, BVerfGE 65, 1-71, Volkszählung.

[51] Ver o Parecer sobre ética e vigilância, p. 75, do Grupo Europeu de Ética para as Ciências e as Novas Tecnologias. Um estudo veio sugerir que um algoritmo de direcionamento de anúncios era discriminatório, com as pesquisas a devolverem, em média, anúncios de funções com remuneração superior para os homens comparativamente com as mulheres que visitam páginas Internet de emprego; Universidade Carnegie Mellon e Instituto Internacional das Ciências Informáticas. Em relação à tendência de se dotar por predefinição os assistentes digitais com uma voz feminina, ver, por exemplo, Judy Wajcman, «*Feminist theories of technology*». Cambridge Journal of Economics, 34 (1). pp. 143-152, 2010.

[52] Giorgio Agamben, «*State of Exeption*», *2005.*

[53] Neil Richards, Neil e Jonathan King, «*Big Data Ethics*» (19 de maio de 2014), Wake Forest Law Review, 2014.

[54] BBC, «*Information watchdog investigates "charity data sales"*», 1.9.2015.

[55] Ver carta do Instituto Future of Life. Encíclica Papal *Laudato Si:* «quando os meios de comunicação social e o mundo digital se tornam omnipresentes, não favorecem o desenvolvimento duma capacidade de viver com sabedoria, pensar em profundidade, amar com generosidade. Neste contexto, os grandes sábios do passado correriam o risco de ver sufocada a sua sabedoria no meio do ruído dispersivo da informação. Isto exige de nós um esforço para que esses meios se traduzam num novo desenvolvimento cultural da humanidade, e não numa deterioração da sua riqueza mais profunda. A verdadeira sabedoria, fruto da reflexão, do diálogo e do encontro generoso entre as pessoas, não se adquire com uma mera acumulação de dados, que, numa espécie de poluição mental, acabam por saturar e confundir. Ao mesmo tempo tendem a substituir as relações reais com os outros, com todos os desafios que implicam, por um tipo de comunicação mediada pela Internet. Isto permite selecionar ou eliminar a nosso arbítrio as relações e, deste modo, frequentemente gera-se um novo tipo de emoções artificiais, que têm a ver mais com dispositivos e monitores do que com as

pessoas e a natureza. Os meios atuais permitem-nos comunicar e partilhar conhecimentos e afetos. Mas, às vezes, também nos impedem de tomar contacto direto com a angústia, a trepidação, a alegria do outro e com a complexidade da sua experiência pessoal. Por isso, não deveria surpreender-nos o facto de, a par da oferta sufocante destes produtos, ir crescendo uma profunda e melancólica insatisfação nas relações interpessoais ou um nocivo isolamento.»

[56] Ver a Ação n.º 4 da Estratégia 2015-2020 da AEPD intitulada «Desenvolver uma dimensão ética para a proteção de dados».